Cisco Prime Infrastructure 3.8 User Guide

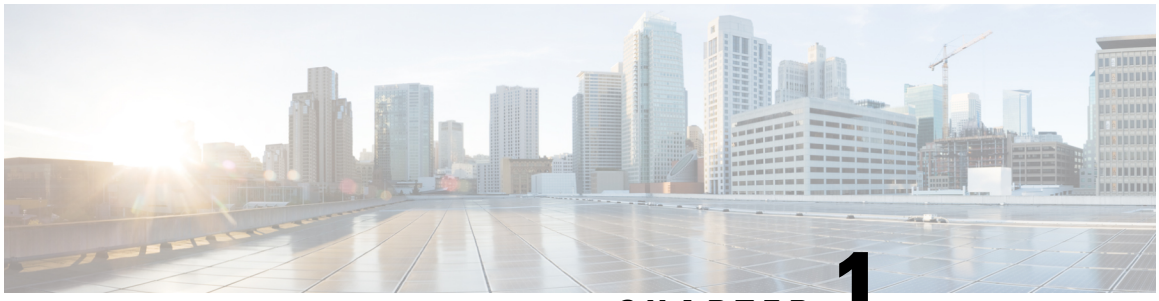
First Published: 2020-03-19

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

PART I

Get Started With Prime Infrastructure



CHAPTER 1

Get Started With Cisco Prime Infrastructure

This section contains the following topics:

Prime Infrastructure Organization

The Prime Infrastructure web interface is organized into a lifecycle workflow that includes the high-level task areas described in the following table. This document follows the same general organization.

Caution You are strongly advised not to enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing Tools > Internetoption and unselecting the Enable third-party browser extensions check box in the Advanced tab.

Table 1: Prime Infrastructure Task Areas

Task Area	Description	Used By
Dashboard	Dashboard gives you a quick view of devices, performance information, and various incidents.	Network Operators and Network Engineers

Task Area	Description	Used By
Monitor	Monitor your network on a daily basis and perform other day-to-day or ad hoc operations related to network device inventory and configuration management. The Monitor tab includes dashboards and tools that you need for day-to-day monitoring, troubleshooting, maintenance, and operations.	Network Engineers, Designers, and Architects
Configuration	Design feature or device patterns, or templates. You create reusable design patterns, such as configuration templates, in the Design area. You may use predefined templates or create your own. Patterns and templates are used in the deployment phase of the lifecycle. You can also design Plug and Play profiles and mobility services.	Network Engineers, Designers, and Architects
Inventory	Perform all device management operations such as adding devices, running discovery, managing software images, configuring device archives, and auditing configuration changes on devices.	Network Engineers, NOC Operators and Service Operators
Maps	View network topology and wireless maps.	Network Engineers, NOC Operators, and Service Operators
Services	Access mobility services, Application Visibility and Control services, and IWAN features.	Network Engineers, NOC Operators and Service Operators
Report	Create reports, view saved report templates, and run scheduled reports.	Network Engineers, NOC Operators, and Service Operators
Administration	Specify system configuration settings and data collection settings, and manage access control. You can view and approve jobs, specify health rules, and manage licenses. You can also perform software updates and configure high availability.	Network Engineers

Setup Tasks to Complete Before Using

Before you can use the features, these tasks should be completed by an administrator:

Table 2: Setup Tasks and References

Tasks to complete before using	For information, see:
Set up and configure the server.	
Add devices to and create device groups to simplify device and network management.	
Enable monitoring for interfaces and technologies used by the network.	
Customize alarm and event behavior for your deployment (for example, alarm and event refresh rates and e-mail and trap receivers).	Set Alarm and Event Management Preferences, on page 266

Log In and Out

To log into the GUI, enter the following in your web browser address field, where server-ip is the IP address of the server:

https://server-ip

Depending on your network configuration, the first time your browser connects to the web server, you may have to update your client browser to trust the server's security certificate. This ensures the security of the connection between your client and the web server.

To log out, click ⚙ at the top right of the window and choose Log Out.

For information on users and the actions they can perform, see:

- How to Transition Between the CLI User Interfaces in , on page 750—Describes all classes of users supported by , including the various CLI user accounts.
- Types of User Groups—Describes the user group mechanism which allows you to control the functions that everyday web GUI users can perform. What you can see and do in the user interface is controlled by your user account privileges. This topic also describes the virtual domain mechanism, which manages Role-Based Access Control (RBAC) for devices.

Change Your Password

You can change your password at any time by clicking ⚙ at the top right of the window and choosing Change Password. Click the ? (help) icon to review the password policy.

(Optional) Click the Generate New Password button to set a secured system-generated password. On clicking this button, a new password will be displayed in the adjacent text box. The same is also displayed in the New Password and Confirm Password text boxes. Click the eye icon in the text box to view or hide the password. You can also copy the password to clipboard by clicking the Copy button.

Click the Reset button to clear the values in the text box.

Use the Main Window Controls

The top left of the title bar provides the following controls.

	Menu button—Toggles the main navigation menu on the left (also called the left sidebar menu)
	Home button—Returns you to the home page (normally the Overview Dashboard)

The right side of the title bar displays your user name and the virtual domain you are working in. A virtual domain is a logical grouping of devices. Virtual domains are used to control who has access to devices and areas of the network. To switch between virtual domains that are assigned to you, see Work In a Different Virtual Domain , on page 18.

	Web GUI global settings button—Log out, change password, view your Cisco.com account profile, adjust your GUI preferences, check a Cisco.com support case, launch online help

When you click  on the right side of the title bar, the window settings menu opens.

Figure 1: Window Settings

Finally, the Alarm Summary gives you a visual indicator of number of alarms in your network. The color indicates the highest severity alarm.

	Alarm Summary—Provides a visual count of alarms in the categories you specify. Clicking this area opens the Alarm Summary popup window.

Change Your Default Home Page

You can specify which page you want to display when you perform either of the following tasks:

- You click from the left side of the web GUI title bar.
- You log in to the web GUI.

This setting is saved on a per-user basis. You can change it at any time without affecting other users.

Step 1 While you have the page you want displayed, click at the top right of the web GUI.

Step 2 Choose Set Current Page as Home.

Set Up and Use the Dashboards

Dashboards provide at-a-glance views of the most important data in your network. They provide status as well as alerts, monitoring, performance, and reporting information. You can customize these dashboards so they contain only the information that is important to you. It may be helpful to set the Network Summary dashboard as your default home page. By doing so, this dashboard is displayed after you log in and you can quickly check overall network health before you do anything else. To set any dashboard as your default home page, see Change Your Default Home Page, on page 6.

Use the following dashboards to monitor and manage your network:

- Network Summary dashboard—To check the health of the entire network. .

Users with administrator privileges can also use the following dashboards:

- Licensing dashboard—See
- Jobs dashboard—See Manage Jobs Using the Jobs Dashboard, on page 19.

Note the following:

- For an explanation of the parts of the dashboard window and how to use dashboard filters, see How to Use the Dashboards, on page 6.

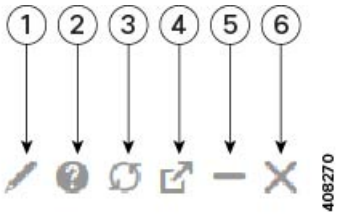
How to Use the Dashboards

The following figure illustrates the key parts of a dashboard window and the controls you can use to adjust them.

Table 3: Dashboard Elements

1	Dashboard filters—Filters all dashlets in the dashboard according to the selection. In this example, a time-based filter is used. The filters displayed depend on the dashboard type. For example, in the performance dashboards, you must select a specific interface, device, circuit, or VC.
2	Metric dashlets—Provides quick metrics for alarms, available devices, and so forth.
3	Dashboard settings and controls: • Dashboard icons—Allows you to launch online help, refresh the entire dashboard, and open the Dock window. • Dashboard Settings menu—Allows you to add or rename a dashboard tab, add new dashlets (both standard and metric), adjust the dashboard's layout, reset all dashboards to their default settings, and export data from the selected dashlets. **Note** The newly added or a renamed dashboard tab can be viewed only in the Tab view.This change is not reflected in the Dashboard menu.
4	Standard dashlets—Provides at-a-glance data that is relevant to the dashboard.

In the top right corner of each dashlet are icons that are activated when you use that dashlet. The dashlet type determines the icons that are available. The most common icons are displayed in the following figure:



See these topics for additional information on dashboards:

- Types of Dashboards, on page 8
- Add Dashlets to Dashboards, on page 10
- Add a New Dashboard, on page 13

Customize the Dock Window

Use the Dock window for quick navigation to frequently used web GUI pages and pop-up windows (such as the 360 view for a particular device). From here, you can also access links to the 15 most recently visited pages and training materials. To open this window, click the Dock icon (located in the top right area of the page).

Complete the following procedure to update the links provided in the Dock window:

Step 1 Add a web GUI page link to the Favorites tab (Dock icon > Links Visited > Favorites):

a) Open the web GUI page you want to add.
b) Click its star (Favorite) icon, which is located in the top left area of the page.

Step 2 Add a pop-up window link to the Docked Items area (Dock icon > Docked Items):

a) Open the pop-up window you want to add, then open its 360 view.

b) From the top right corner of the pop-up window, click the Add to Dock icon.

Types of Dashboards

Check the Health of the Entire Network Using the Network Summary Dashboard

The Network Summary dashboard alerts you to the most important network issues. It provides alarm, status, and usage information for all devices and interfaces in the network, including wireless devices like controllers and APs. You can also display a small network topology dashlet on this dashboard.

To understand the types of information provided by the Metrics dashlets at the top of the dashboard, hover your mouse cursor over a Metrics dashlet and when the popup help button (?) appears, click it to open the dashlet help. For descriptions of the other dashlets on the page, click the popup help button shown with the dashlet controls in the upper right corner of each dashlet.

To open and customize the Network Summary dashboard:

Step 1 Choose Dashboard > Network Summary, then click:

- The Overview tab to check all devices.

  Note Users will now be able to view the description of ports by hovering over the interface names for the Top N Interface Utilization and Top N WAN Interfaces by Utilization interface dashlets.

- The Incidents tab to focus on alarms and events, including syslogs.
- The Site Summary tab to check all devices at particular sites.
- The Network Health tab to check network health against a set of health rules.

Step 2 Adjust the dashboard as needed. You can drag dashlets to different locations on the dashboard, or use the Settings menu to add new dashlets, change the dashboard style, and so forth. If you want to add dashlets to the dashboard, see Add a Predefined Dashlet To a Dashboard, on page 10.

Step 3 Select the time frame you want to view from the Filters Time Frame drop-down list, then click Apply. Selected time frame will be updated in all dashlets.

Check the Health of All Devices or All Interfaces Using the Overview Dashboard

The Overview dashboard helps you maintain the health of your network by providing summarized and aggregated data on the health of all network devices, interfaces, clients, and application services, including their availability, status, utilization, and the alarms and events affecting them.

To understand the types of information provided by the Metrics dashlets at the top of the dashboard, hover your mouse cursor over a Metrics dashlet and when the popup help button (?) appears, click it to open the dashlet help. For descriptions of the other dashlets on the page, click the popup help button shown with the dashlet controls in the upper right corner of each dashlet.

To open and customize the Overview dashboard:

Step 1 Choose Dashboard > Overview, then click:

- The General tab to check on the health of all devices and interfaces, including coverage areas, which devices are reachable, and top users of CPU and memory.
- The Incidents tab to focus on alarms and events, including sites with the most alarms, device reachability, types of alarms, and syslog details.
- The Client tab to focus on the health of network clients. This tab hosts a variety of client-oriented dashlets, including a troubleshooting tool, distribution and speed graphs for wired and wireless clients, and client posture.
- The Network Devices tab to check device availability, CPU and memory use, and temperature issues.
- The Network Interfaces tab to check interface availability, status, CPU and memory use, and interfaces with the most errors and discards.
- The Service Assurance tab to check on identified network services and the applications, servers, and Netflow-monitored resources that support them, as well as the clients consuming them.

Note Users will now be able to view the description of ports by hovering over the interface names for the Top N Interface Utilization, Top N WAN Interfaces by Utilization, and Top N Interface Errors and Discards interface dashlets.

Step 2 Adjust the dashboard as needed. You can drag dashlets to different locations on the dashboard, or use the Settings menu to add new dashlets, change the dashboard style, and so forth. If you want to add dashlets, see Add a Predefined Dashlet To a Dashboard, on page 10.

Step 3 Select the time frame you want to view from the Filters Time Frame drop-down list, then click Apply.

Check the Health of Wireless Networks Using the Wireless Dashboard

The Wireless dashboard helps you maintain the health of your wireless network by providing aggregated data on network security status and attacks, mesh network efficiency, air quality, interferers, and so on.

To understand the types of information provided by the Metrics dashlets at the top of the dashboard, hover your mouse cursor over a Metrics dashlet and when the popup help button (?) appears, click it to open the dashlet help. For descriptions of the other dashlets on the page, click the popup help button shown with the dashlet controls in the upper right corner of each dashlet.

To open and customize the Wireless dashboard:

Step 1 Choose Dashboard > Wireless, then click:

- The Security tab to check on top security issues, detected rogues of all types, CleanAir security, and rogue containment, and Cisco Adaptive Wireless Intrusion Prevention (wIPS) data.
- The Mesh tab to focus on mesh network alarms, and links with the worst SNR, number of node hops and packet errors.
- The CleanAir tab to focus on non-802.11 interference sources, including the total count of and worst interferers, CAS interferer notifications, and general air quality.

- The ContextAware tab to focus on Cisco Context-Aware Mobility data supported by Mobility Service Engines, including MSE tracking counts, location-assisted client troubleshooting, and detected rogue elements.

Step 2 Adjust the dashboard as needed. You can drag dashlets to different locations on the dashboard, or use the Settings menu to add new dashlets, change the dashboard style, and so forth. If you want to add dashlets, see Add a Predefined Dashlet To a Dashboard, on page 10.

Step 3 Select the time frame you want to view from the Filters Time Frame drop-down list, then click Apply.

Step 1 Adjust the dashboard as needed. You can drag dashlets to different locations on the dashboard, or use the Settings menu to add new dashlets, change the dashboard style, and so forth. If you want to add dashlets, see Add Dashlets to Dashboards, on page 10.

Step 2 Select the time frame you want to view from the Filters Time Frame drop-down list, then click Go.

Add Dashlets to Dashboards

- Prepackaged dashlets that are provided with —Some of the dashlets are displayed on dashboards by default; others are listed in the Settings menu, and you can add them as needed. These dashlets provide information you will likely monitor (for example, device CPU utilization, interface errors and discards, and traffic statistics). See Add a Predefined Dashlet To a Dashboard, on page 10.
- Customized dashlets that you create to monitor device performance—These dashlet types can only be added to the Device Trends dashboard. See Add a Customized Dashlet to the Device Trends Dashboard.

Add a Predefined Dashlet To a Dashboard

provides a predefined set of dashlets that will provide you with commonly-sought network data. By default, a subset of these dashlets is already included in the dashboards, to help you get started. Complete the following procedure to add another of these predefined dashlets to your dashboards.

Note To edit or remove a dashlet, click the appropriate icon from the top right corner of that dashlet. (See How to Use the Dashboards.)

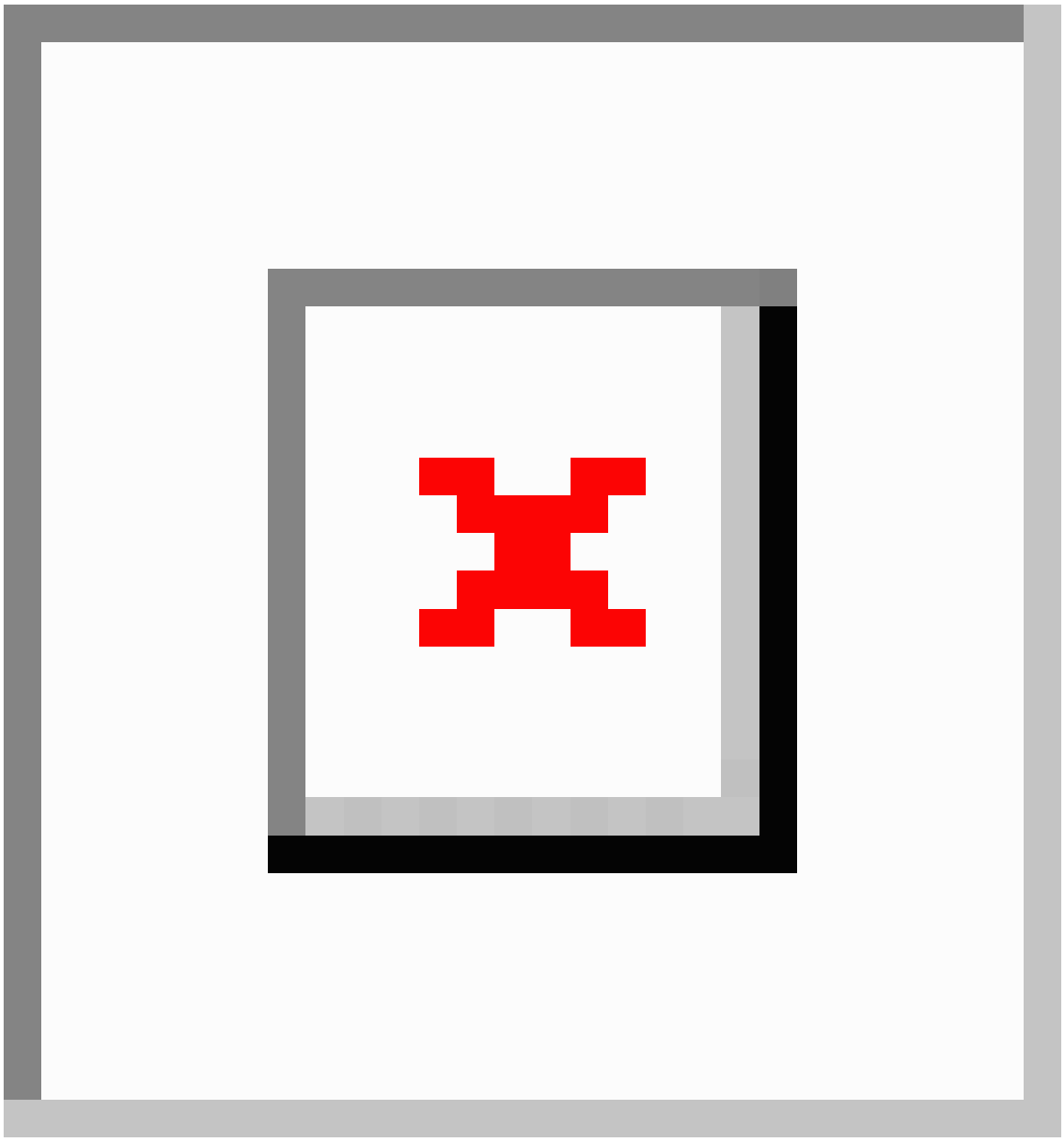
Step 1 From the sidebar menu, choose Dashboard, then select the dashboard you want to add a dashlet to.

For example, to add a Device Memory Utilization dashlet to the Device Trends dashboard, choose Dashboard > Device Trends > Device.

Step 2 Identify the dashlet you want to add, then add it:

a) From the top right corner of the dashboard, click Settings and then click Add Dashlet(s). lists the dashlets that can be added to that dashboard.

b) To open a pop-up window that provides an overview of a particular dashlet, hover your cursor over dashlet's name. The pop-up window also lists the sources for the data the dashlet provides and the filters you can apply to the dashlet, as shown in the following illustration.



c) Click Add to add the selected dashlet to the dashboard.

Step 3 Verify that the dashlet is populated with data.

If it is not, check whether the required monitoring policy is enabled. (Only the Device Health monitoring policy is enabled by default. It checks device availability, CPU and memory pool utilization, and environmental temperature.)

a) From the top right corner of the dashlet, click its ? (Help) icon to open the dashlet's pop-up window.

b) Check the information provided in the Data Sources area. If it lists a monitoring policy, check whether the policy is activated. See Check What Is Monitoring, on page 250.

Add a Customized Dashlet to the Device Trends Dashboard

If none of the dashlets in the Device Trends dashboard provide the device performance information you need, you can add a dashlet that uses a customized template to poll devices for their SNMP MIB attributes. Complete the following procedure to add this dashlet to the dashboard.

Before you begin

Check the available monitoring policies to determine which policy collects the information you need. You will have to specify a policy during the dashlet creation process. If none of the policies meet your needs, you can create a policy that polls new parameters. See Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 258.

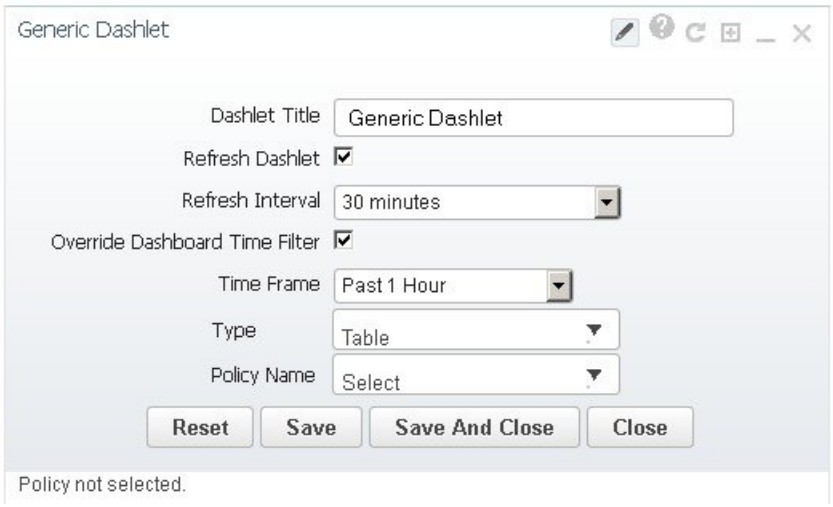
Step 1 Choose Dashboard > Device Trends > Device.

Step 2 From the top right corner of the dashboard, click Settings and then click Add Dashlet(s).

Step 3 Expand the Device Dashlets list.

Step 4 Locate Generic Dashlet, then click Add.

adds a blank generic dashlet to the Device Trends dashboard.



Step 5 Configure the new dashlet as needed.

At a minimum, you should:

- Enter a meaningful title in the Dashlet Title field.
- Check the Override Dashboard Time Filter check box if you do not want to apply the time filters to all of the dashlets in the dashboard.
- In the Type drop-down list, choose whether the dashlet will display its data as a table or line chart. (Regardless of your choice, will display a toggle at the bottom of the dashlet that allows you to change the format.)

- In the Policy Name drop-down list, choose the monitoring policy that will collect the data for this dashlet.

Step 6 Click Save And Close.

Add a New Dashboard

Use this procedure to create a new dashboard. Your new dashboard will appear as a new tab under one of the dashboards listed in Types of Dashboards, on page 8.

Step 1 Open the relevant existing dashboard.

For example, if you want to create a new tab under the Performance dashboard, click any tab under Dashboard > Performance.

Step 2 Click the + (Add New Dashboard) tab.

The Settings menu opens.

Step 3 Enter a name for the new dashboard, then click Apply.

Step 4 Click the new dashboard tab, then add dashlets as described in Add a Predefined Dashlet To a Dashboard, on page 10.

Troubleshoot Network Health Using Dashboards

Prime Infrastructure provides a quick way to view the health of your network and sites by choosing Dashboard > Network Summary > Nework Health. You must create location groups and then add devices to the locations. Prime Infrastructure displays a map indicating the overall health of all the sites. The Network Health page allows you to toggle the view between wired and wireless devices. By default, all locations and a maximum of 500 APs per location group are displayed. If you choose Wired view, the Network Health page shows the WAN Inteface Utilizatoin details and a map indicating the overall health status of the wired devices of all the locations. If you choose Wireless view, the Network Health page shows the Wireless Client Count details and a map indicating the overall health status of the wireless devices of all the sites. In the Wireless view, click the Executive View expand icon to choose any one of the client, access points, environment (clean air), and application dashboards. The Network Health page displays the dashlets corresponding to the selected dashoard. You can click the settings icon to add more dashlets. Click more to cross launch the Dashboard.

Related Topics

Define Health Rules, on page 14
Network Health Map Features, on page 15
Network Health Summary, on page 16
Define QoS and Interface Settings, on page 14
QoS Metrics, on page 16
Traffic Conversation, on page 17
Create Location Groups, on page 50

Define Health Rules

You can specify rules and threshold values for your sites. The rules you specify determine the notifications that appear in Dashboard > Network Summary > Network Health.

Step 1 Choose Services > Application Visibility & Control > Health Rule. There are 3 tabs where you can specify health rules:

- Service Health—Define health rules for services such as Jitter, MOS score, Network Time, Packet Loss, Traffic Rate, etc.
- Infrastructure Health—Define health rules for wired devices.
- Wireless Health—Define health rules for wireless devices.

Note The default critical and warning threshold set for client count is 40 and 36 respectively. The maximum critical threshold for client count can be set as 1000.

Step 2 To add a new health rule, click the plus icon, then specify the location, metric, and threshold. You can add new Infrastructure Health and Wireless Health rules only.

Step 3 To edit an existing health rule, select the health rule you want to modify, then click Edit.

Step 4 Enter the details for the health rule, then click Save.

The values you enter apply to all devices and interfaces in the location group for which the health rule applies.

Related Topics

Network Health Map Features, on page 15
Network Health Summary, on page 16
Create Location Groups, on page 50

Define QoS and Interface Settings

The Health Rule page allows you the define the QoS and Interface settings for the heatmap displayed in the Network Health page.

Step 1 Choose Services > Application Visibility & Control > Health Rule.

Alternately, click the Launch Health Rules link in the Network Health page.

Step 2 Click the Infrastructure Health tab.

Step 3 Check the QoS Settings check boxes which you want to exclude from the heatmap. By default, the Exclude Scavenger check box will be checked and not shown in the heatmap.

Step 4 Uncheck the Exclude Admin Down Interface if you want to include the Admin down interfaces in the heatmap. By default, the Exclude Admin Down Interface will be checked and not shown in the heatmap.

Step 5 Click Save.
The QoS and Interface settings will get immediately applied to the heatmap in the Network Health page. The corresponding health rule job will get updated after 30 minutes.

Network Health Map Features

When you choose Dashboard > Network Summary > Network Health, the map displays all the location groups with geographic attributes that you previously added. By default, a maximum of 500 APs per location group are displayed.

The location groups are colored according to the overall health of the location:

- Red—indicates there are critical issues in the specified location.
- Yellow—indicates there are warnings in the specified location.
- Green—indicates there are no errors or warnings.
- Gray—indicates there are no devices or data in the specified location.

In addition to the color indicating the health, the icon can be:

- Solid—indicates a parent site, meaning there are children locations associated with the site.
- Outlined—indicates there are no children associated with this location.

Hover your mouse over any location on the map to view a popup window that lists the sites in that location and the corresponding errors or warnings, by device type, in each location.

Click on a site name to view in a zoomed-in map of the site.

Related Topics

Define Health Rules, on page 14
Network Health Display Options, on page 15
Network Health Summary, on page 16
Create Location Groups, on page 50

Network Health Display Options

When you choose Dashboard > Network Summary > Network Health, display options appear on the right side of the page as show in the below figure.

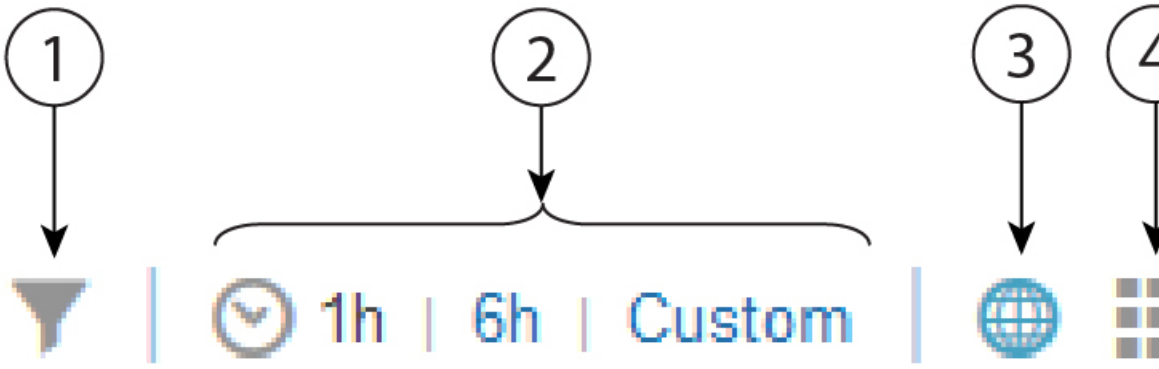


Table 4: Network Health Display

1	Filter options. The options you select affect what is displayed in the map and the Health Summary pane. Click Clear > Selection to remove all filters.

2	Time frame. By default, information from the last 6 hours is displayed in the Site Visibility map and Health Summary pane.
3	Displays the map in the left pane.
4	Displays the Network Health summary details in the Health Index view.
5	Displays the Network Health summary details in a table format.
6	Shows or hides the Health Summary pane on the right.

Related Topics

Define Health Rules, on page 14
Network Health Map Features, on page 15
Network Health Summary, on page 16
Create Location Groups, on page 50

Network Health Summary

The Health Summary pane displays errors and threshold violations for all devices across all locations. Prime Infrastructure aggregates health data from the devices and services to the site summary every 15 minutes. Click on any of the sites or devices listed in the Health Summary pane to view more information. For example, click on the site(s) listed under Service Health Issues. A new pane opens listing the sites with service health issues where you can easily see in which area(s) the errors or warnings are occurring.

: Displays the areas in which service health related errors or warnings are occurring.

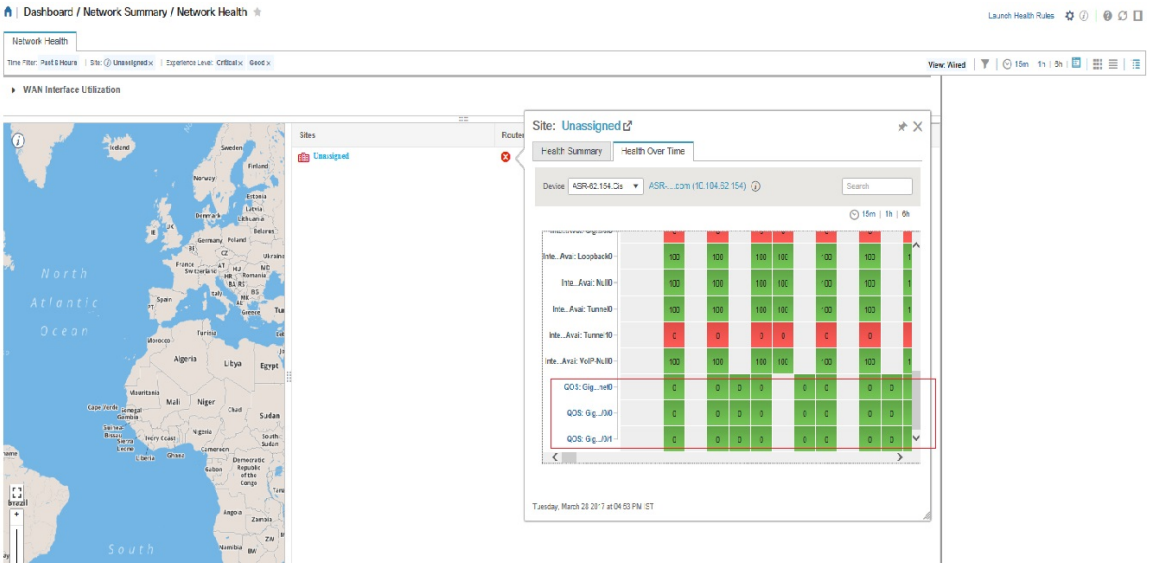
Click on a site name to have the map zoom in on that particular site and display additional information specific to that site. You can edit the health rule settings of a site by clicking the settings icon next to the site name. The modified health rule settings will get automatically updated in the Health Rules page. If a site doesn't have assinged health rules, then the health rules displayed for that site represent the health rules of its parent site.

Related Topics

Define Health Rules, on page 14
Network Health Map Features, on page 15
Create Location Groups, on page 50

QoS Metrics

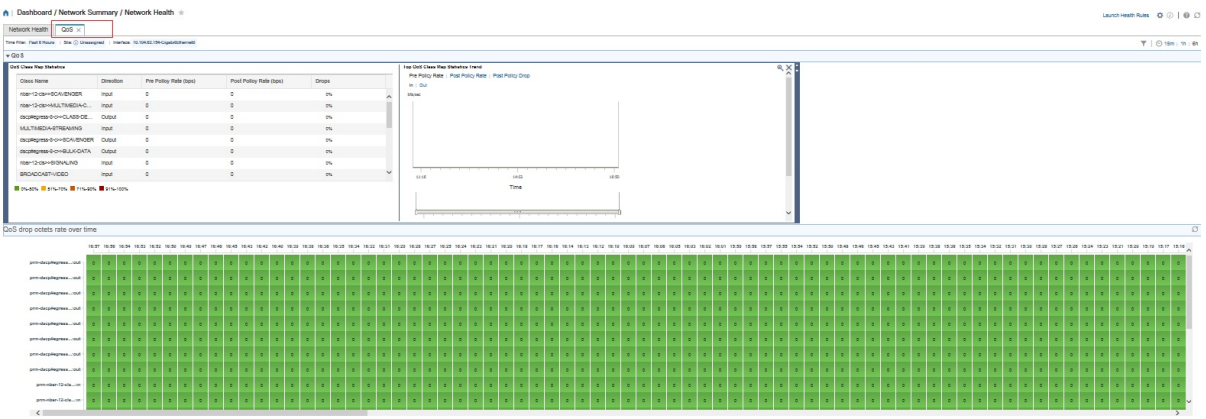
The Network Health page shows the QoS metrics for routers and switches. You can launch the QoS tab for routers, switches and interfaces in the Network Health page by clicking the QoS hyperlink in the heatmap, the Health summary view, Health index view, and Table view. The heatmap for routers and switches, shows the aggregated QoS data per interface level and the average of dropOctetsRate across all QoS classes and all directions for each interface.



Click the QoS tab in the Network Health page to view more granular data per class map for the chosen interface. The QoS tab shows the following details:

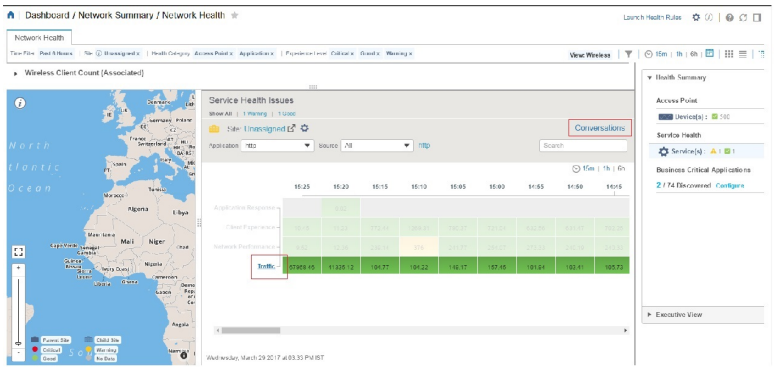
- QoS class Map Statistics
- Top QoS class Map statistics Trend
- QoS drop Octets rate over time

The QoS tab shows more granular and is shown per class map for a given interface.



Traffic Conversation

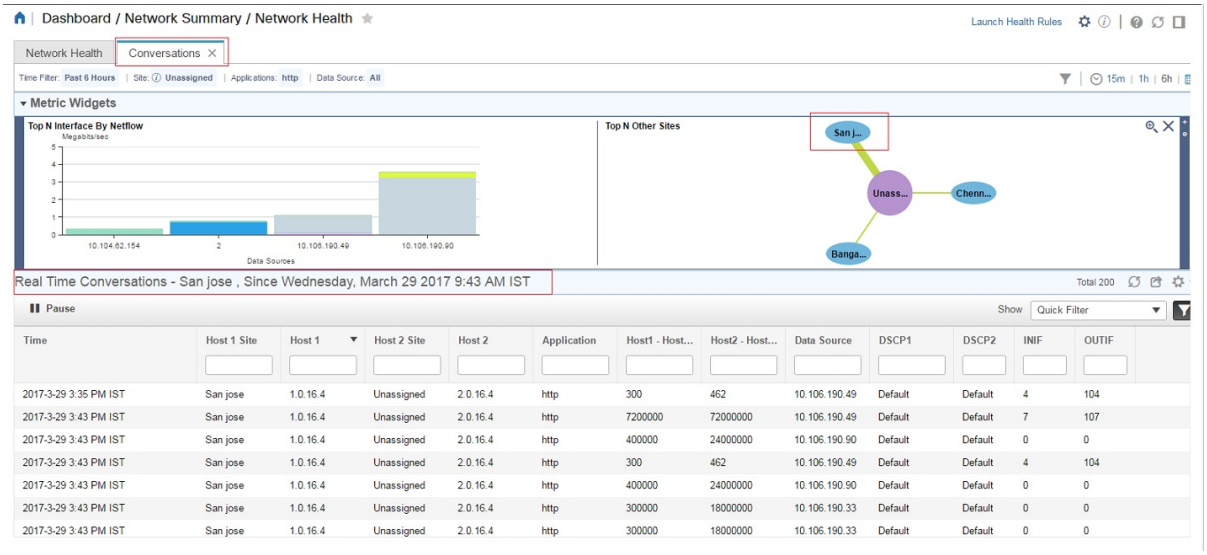
You can launch the Conversation tab in the Network Health page by clicking the traffic hyperlink in the heatmap or the Conversations hyperlink as shows in the below image.



The conversation tab shows the following details:

- Top N Interface By Netflow chart
- Top N Other Sites graph
- Real Time Conversation table

The Real Time Conversation table shows the conversations based on the global filters (Site, Application Data Source, and Time filter). If you want to view the real time conversations of a particular site or an interface, click the site in the Top N Other Sites graph or the interface in the Top N Interface By Netflow chart. You can view up to 4000 records in the Real Time Conversation table and the records get automatically refreshed every minute.



Time	Host 1 Site	Host 1	Host 2 Site	Host 2	Application	Host1 - Host...	Host2 - Host...	Data Source	DSCP1	DSCP2	INIF	OUTIF
2017-3-29 3:35 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	300	462	10.106.190.49	Default	Default	4	104
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	7200000	72000000	10.106.190.49	Default	Default	7	107
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	400000	24000000	10.106.190.90	Default	Default	0	0
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	300	462	10.106.190.49	Default	Default	4	104
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	400000	24000000	10.106.190.90	Default	Default	0	0
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	300000	18000000	10.106.190.33	Default	Default	0	0
2017-3-29 3:43 PM IST	San jose	1.0.16.4	Unassigned	2.0.16.4	http	300000	18000000	10.106.190.33	Default	Default	0	0

Work In a Different Virtual Domain

Virtual domains are logical groupings of devices and are used to control your access to specific sites and devices. Virtual domains can be based on physical sites, device types, user communities, or any other designation the administer chooses. All devices belong to ROOT-DOMAIN, which is the parent domain for all new virtual domains. For more information about virtual domains, see .

If you are allowed access to more than one virtual domain, you can switch to a different domain by completing the following procedure:

Step 1 Click ⚙ from the right side of the title bar.

Step 2 Choose Virtual Domain: current-domain.

Step 3 From the Virtual Domain drop-down list, choose a different domain.

immediately changes your working domain.

Manage Jobs Using the Jobs Dashboard

If you have the appropriate user account privileges, you can manage jobs using the Jobs dashboard. To view the Jobs dashboard, choose Administration > Dashboards > Job Dashboard. From here, you can quickly see if a job was successful, partially successful, or failed.

If too many jobs are already running, will hold other jobs in the queue until resources are available. If this delays a scheduled job past its normal starting time, the job will not run. You will have to run it manually.

Some jobs may require approval. If this is the case, sends an email to users with Administrator privileges notifying them that a job was scheduled and needs approval. The job will only run after it is approved.

The following table describes the buttons displayed in the Jobs dashboard.

Table 5: Jobs Dashboard Buttons

Button	Description
Delete Job	Removes a job from the Jobs dashboard.
Edit Job	Edit the settings configured for the selected job.
Edit Schedule	Displays the series schedule and lets you edit it (start time, interval, and end time). **Note** Editing the schedule of an already-scheduled job will change the status of that job to Pending for Approval since each edit requires an approval from the user who created the job.
Run	Runs a new instance of the selected job. Use this to rerun partially successful or failed jobs; the job will only run for the failed or partially successful components.
Abort	Stops a currently-running job, but allows you to rerun it later. Not all jobs can be aborted; will indicate when this is the case.
Cancel Series	Stops a currently-running job and does not allow anyone to rerun it. If the job is part of a series, future runs are not affected.
Pause Series	Pauses a scheduled job series. When a series is paused, you cannot run any instances of that series (using Run).
Resume Series	Resumes a scheduled job series that has been paused.

Note The Delete Job, Abort, and Cancel Series buttons are not available for system and poller jobs.

To view the details of a job, follow these steps:

Step 1 Choose Administration > Dashboards > Job Dashboard.

Step 2 From the Jobs pane, choose a job series to get basic information (such as job type, status, job duration, and next start time).

Step 3 To view the job interval, click a job instance hyperlink.

At the top of the job page, the Recurrence field indicates how often the job recurs. Job interval details will be added for every jobs that triggers.

Step 4 To get details about a failed or partially successful job, click the job instance hyperlink and expand the entries provided on the resulting page.

This is especially helpful for inventory-related jobs. For example, if a user imported devices using a CSV file (a bulk import), the job will be listed in the Jobs sidebar menu under User Jobs > Device Bulk Import. The job details will list the devices that were successfully added and the devices that were not.

Example

To troubleshoot a failed software image import job:

1. Choose User Jobs > Software Image Import from the Jobs sidebar menu.
2. Locate the failed job in the table and then click its hyperlink.
3. Expand the job's details (if not already expanded) to view the list of devices associated with the job and the status of the image import for each device.
4. To view the import details for a specific device, click that device's i (information) icon in the Status column. This opens an Image Management Job Results pop-up window.
5. Examine each step and its status. For example, the Collecting image with Protocol: SFTP column might report that SFTP is not supported on the device.

Extend Functions

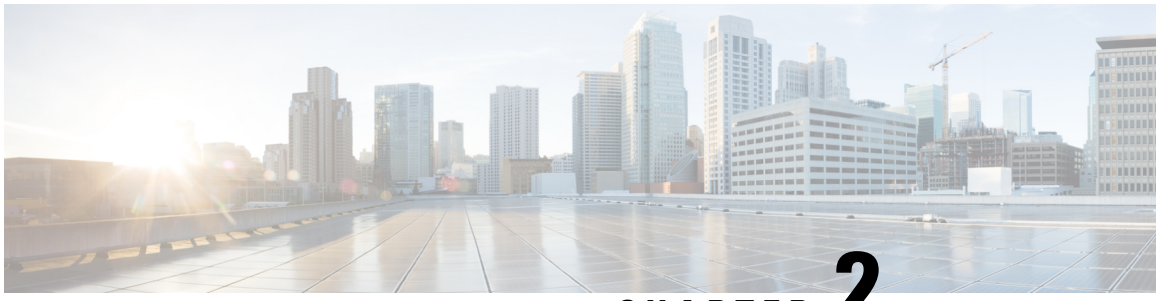
Advanced users can extend functions and manage administrative options using the REST API.

To get information about this tool, click ⚙ at the top right of the web GUI, and then choose Help > REST APIs. You can also download the Cisco Prime Infrastructure API Reference Guide directly from Cisco.com.

Check Cisco.com for the Latest Documentation

Refer to for information about and links to all of the documentation that is provided with .

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.



CHAPTER 2

Change Prime Infrastructure User Settings

Set User Preferences

Prime Infrastructure provides user preference settings that allows you to modify how information is displayed.

- Change Your User Preferences
- Change Your Idle-User Timeout
- Change List Length

Change Your User Preferences

To change your user preferences, click the Settings icon (the gear icon on the right side of the menu bar) and choose My Preferences and change the settings shown on the My Preferences page.

Related Topics

Change Your Idle-User Timeout, on page 23
Change List Length, on page 25
Set Up Your Alarm and Event Display Preferences, on page 267
Prime Infrastructure Organization, on page 1

Change Your Idle-User Timeout

Prime Infrastructure provides two settings that control when and how idle users are automatically logged out:

- User Idle Timeout—You can disable or configure this setting, which ends your user session automatically when you exceed the timeout. It is enabled by default and is set to 10 minutes. The User Idle Timeout value must be lesser or equal to the Global Idle Timeout vlaue.

- Global Idle Timeout—The Global Idle Timeout is enabled by default and is set to 10 minutes. Only users with administrative privileges can disable the Global Idle Timeout setting or change its time limit.

Note Prime Infrastructure will log out the idle user based on the lesser Timeout value.

You may find it useful to disable the user idle timeout feature if, for example, you are an Operations Center user experiencing sudden log-offs, due to idle sessions, with one or more Prime Infrastructure instances managed by Operations Center. For details, see the section Disable Idle User Timeouts for Operations Center in the chapter Set Up the Prime Infrastructure Server in the Cisco Prime Infrastructure Administrator Guide. .

To change the timeout settings, follow these steps:

Step 1 Click the Settings icon and choose My Preferences.

Step 2 Under User Idle Timeout:

- Change the check status of the check box next to Logout idle user to enable or disable your idle timeout.
- From the Logout idle user after drop-down list, choose one of the idle timeout limits.

Step 3 Click Save. You will need to log out and log back in for this change to take effect.

For details, see the section Disable Idle User Timeouts for Operations Center in the chapter Set Up the Prime Infrastructure Server in the Cisco Prime Infrastructure Administrator Guide. .

Related Topics

Change Your User Preferences, on page 23

Disable Idle User Timeout

By default, client sessions are disabled and users are automatically logged out after certain period of inactivity. This is a global setting that applies to all users. To avoid being logged out during the installation, it is recommended to disable automatic logout of idle users in the system settings using the following procedure.

Note The Global Idle Timeout setting overrides the User Idle Timeout setting. To configure Global Idle Timeout settings, see CiscoPrime Infrastructure Administrator Guide.

Step 1 Choose Administration > Settings > System Settings, then choose General > Server.

Step 2 In the Global Idle Timeout area, uncheck the Logout all idle users check box and click Save.

Step 3 Click ⚙ at the top right of web GUI window and choose My Preferences.

Step 4 In the User Idle Timeout area, uncheck the Logout idle user check box and click Save.

If you need to change the idle timeout value, then select Logout idle user check box and from the Logout idle user after drop-down list, choose one of the idle timeout limits. (But this cannot exceed the value set in the Global Idle Timeout settings.)

Step 5 Click Save. You will need to log out and log back in for this change to take effect.

Change List Length

Prime Infrastructure lets you change the default number of entries displayed in some lists. The Items Per List setting affects the number of entries displayed on the monitoring pages for:

- APs
- Controllers
- Site Maps
- Mesh
- CleanAir

The Items Per List setting does not apply to Network Devices, alarms and events, configuration archive, software image management, or configuration.

An average of 50 items will be shown on a given page.

Step 1 Click the Settings icon and choose My Preferences.

Step 2 Change the setting in the Items Per List Page drop down.

Step 3 Click Save.

Related Topics

Change Your User Preferences, on page 23

Configure the Global Timeout for Idle Users

provides two settings that control when and how idle users are automatically logged out:

- User Idle Timeout—You can disable or configure this setting, which ends your user session automatically when you exceed the timeout. It is enabled by default and is set to 15 minutes.
- Global Idle Timeout—The Global Idle Timeout setting overrides the User Idle Timeout setting. The Global Idle Timeout is enabled by default and is set to 15 minutes. Only users with administrative privileges can disable the Global Idle Timeout setting or change its time limit.

By default, client sessions are disabled and users are automatically logged out after 15 minutes of inactivity. This is a global setting that applies to all users. For security purposes, you should not disable this mechanism, but you can adjust the timeout value using the following procedure. To disable/change the timeout for an idle user, see Disable Idle User Timeout, on page 24

Step 1 Choose Administration > Settings > System Settings, then choose General > Server.

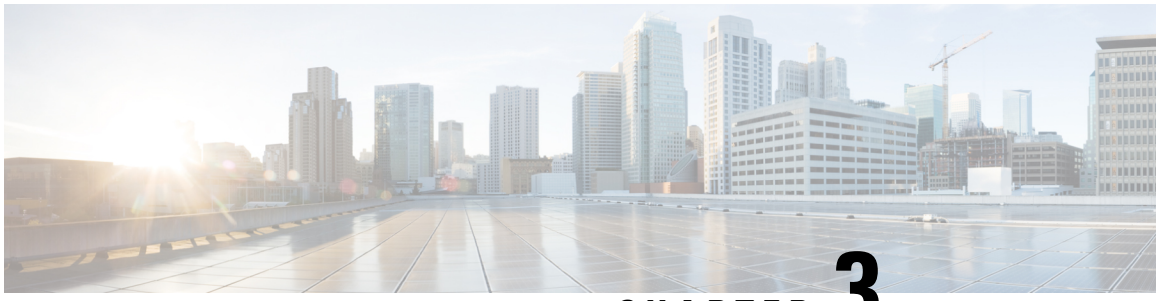
Step 2 In the Global Idle Timeout area, make sure the Logout all idle users check box is selected (this means the mechanism is enabled).

Step 3 Configure the timeout by choosing a value from the Logout all idle users after drop-down list.

Step 4 Click Save. You will need to log out and log back in for this change to take effect.

PART II

Manage the Inventory



CHAPTER 3

Add and Organize Devices

This chapter contains the following topics:

Add Devices to

uses device, location, and port groups to organize elements in the network. When you view devices in a table or on a map (network topology), the devices are organized in terms of the groups they belong to. When a device is added to , it is assigned to a group named Unassigned Group. You can then move the device into the desired groups as described in Create Groups of Devices for Easier Management and Configuration, on page 46.

Table 6: Methods for Adding Devices

Supported Methods for Adding Devices	See:
Add multiple devices by discovering the neighbors of a seed device using:	Add Devices Using Discovery, on page 30.
• Ping sweep and SNMP polling (Quick Discovery)	• Run Quick Discovery, on page 31
• Customized protocol, credential, and filter settings (useful when you will be repeating the discovery job)	• Run Discovery with Customized Discovery Settings, on page 32
Add multiple devices using the settings specified in a CSV file	

Supported Methods for Adding Devices	See:
Add a single device (for example, for a new device type)	Add Devices Manually (New Device Type or Series), on page 35

Understand the Discovery Process

Prime Infrastructure performs the following steps during the discovery process:

1. Using ICMP ping, determine if each device is reachable. If Prime Infrastructure is unable to reach the device, the device Reachability status is Unreachable.
2. Verify the SNMP credentials. If the device is reachable by ICMP, but the SNMP credentials are not valid, the device Reachability status is Ping Reachable.

   If the device is reachable by both ICMP and SNMP, the device Reachability status is Reachable .
3. Verify Telnet and SSH credentials.
4. Modify the device configuration(s) to add a trap receiver in order for Prime Infrastructure to receive the necessary notifications.
5. Start the inventory collection process to gather all device information.
6. Add the devices to the Inventory > Network Devices page.

After running discovery, choose Inventory > Device Management > Network Devices to verify that discovery is complete.

Add Devices Using Discovery

supports two discovery methods:

- Ping sweep from a seed device (Quick Discovery). The device name, SNMP community, seed IP address and subnet mask are required. See Run Quick Discovery, on page 31
- Using customized discovery methods (Discovery Settings)—This method is recommended if you want to specify settings and rerun discovery in the future. See Run Discovery with Customized Discovery Settings, on page 32.

Note

- If a discovery job rediscovers an existing device and the device's last inventory collection status is Completed, does not overwrite the existing credentials with those specified in the Discovery Settings. For all other statuses (on existing devices), overwrites the device credentials with those specified in the Discovery Settings.
- Service discovery might take longer than usual when a large number of devices is added during database maintenance windows. Therefore, we recommend that you avoid large-scale operations during the night and on weekends.
- Autonomous APs are filtered out of the discovery process to optimize the discovery time. You need to manually add Autonomous APs using Import Devices or Credential Profile.

The discovery process of a device is carried out in the sequence of steps listed below. As performs discovery, it sets the reachability state of a device, which is: Reachable, Ping Reachable, or Unreachable. A description of the states is provided in Device Reachability and Admin States, on page 40.

1. determines if a device is reachable using ICMP ping. If a device is not reachable, its reachability state is set to Unreachable.
2. Server checks if SNMP communication is possible or not.
   - If a device is reachable by ICMP but its SNMP communication is not possible, its reachability state is set to Ping Reachable.
   - If a device is reachable by both ICMP and SNMP, its reachability state is Reachable.
3. Verifies the device's Telnet and SSH credentials. If the credentials fail, details about the failure are provided in the Network Devices table in the Last Inventory Collection Status column (for example, Wrong CLI Credentials). The reachability state is not changed.
4. Modifies the device configuration to add a trap receiver so that can receive the necessary notifications (using SNMP).
5. Starts the inventory collection process to gather all device information.
6. Displays all information in the web GUI, including whether discovery was fully or partially successful.

Note When verifies a device's SNMP read-write credentials, the device log is updated to indicate that a configuration change has been made by (identified by its IP address).

Specify the Management IP Address Type (IPv4/IPv6) for Discovered Devices

For discovered dual-home (IPv4/IPv6) devices, specify whether you want to use IPv4 or IPv6 addresses for management IP addresses.

Step 1 Choose Administration > Settings > System Settings, then choose Inventory > Discovery.

Step 2 From the IPv4/IPv6 Preference for Management Address drop-down list, choose either v4 or v6.

Step 3 Click Save.

Run Quick Discovery

Use this method when you want to perform a ping sweep using a single seed device. Only the device name, SNMP community, seed IP address and subnet mask are required. If you plan to use the configuration management features, you must provide the protocol, user name, password, and enable password.

Step 1 Choose Inventory > Device Management > Discovery, then click the Quick Discovery link at the top right of the window.

Step 2 At a minimum, enter the name, SNMP community, seed IP address, and subnet mask.

Step 3 Click Run Now.

What to do next

Click the job hyperlink in the Discovery Job Instances area to view the results.

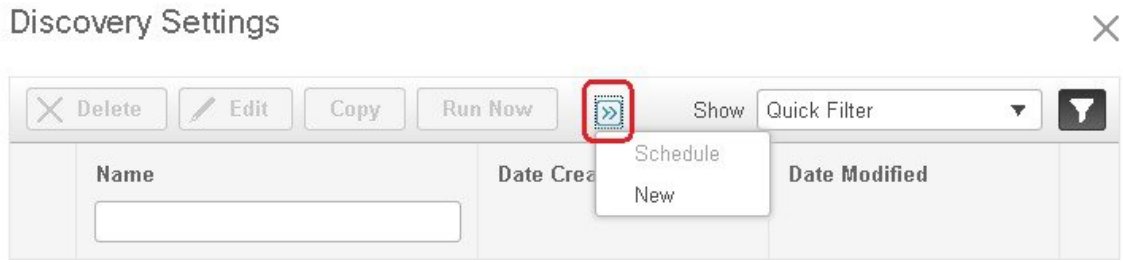
Run Discovery with Customized Discovery Settings

can discover network devices using discovery profiles. A discovery profile contains a collection of settings that instructs how to find network elements, connect to them, and collect their inventory. For example, you can instruct to use CDP, LLDP, OSPF to discover devices, or just perform a simple ping sweep (an example of the results of a ping sweep is provided in Sample IPv4 IP Addresses for Ping Sweep, on page 32.) You can also create filters to fine-tune the collection, specify credential sets, and configure other discovery settings. You can create as many profiles as you need.

After you create a profile, create and run a discovery job that uses the profile. You can check the results of the discovery job on the Discovery page. You can also schedule the job to run again at regular intervals.

Step 1 Choose Inventory > Device Management > Discovery, then click the Discovery Settings link at the top right of the window. (If you do not see a Discovery Settings link, click the arrow icon next to the Quick Discovery link.)

Step 2 In the Discovery Settings pop-up, click New.



Step 3 Enter the settings in the Discovery Settings window. Click "?" next to a setting to get information about that setting. For example, if you click "?" next to SNMPv2 Credential, the help pop-up provides a description of the protocol and any required attributes.

Step 4 Click Run Now to run the job immediately, or Save to save your settings and schedule the discovery to run later.

Sample IPv4 IP Addresses for Ping Sweep

The following table provides an example of the results of a ping sweep.

Subnet Range	Number of Bits	Number of IP Addresses	Sample Seed IP Address	Start IP Address	End IP Address
255.255.240.0	20	4094	205.169.62.11	205.169.48.1	205.169.63.254
255.255.248.0	21	2046	205.169.62.11	205.169.56.1	205.169.63.254
255.255.252.0	22	1022	205.169.62.11	205.169.60.1	205.169.63.254

255.255.254.0	23	510	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.0	24	254	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.128	25	126	205.169.62.11	205.169.62.1	205.169.63.127
255.255.255.192	26	62	205.169.62.11	205.169.62.1	205.169.63.62
255.255.255.224	27	30	205.169.62.11	205.169.62.1	205.169.63.30
255.255.255.240	28	14	205.169.62.11	205.169.62.1	205.169.63.14
255.255.255.248	29	6	205.169.62.11	205.169.62.9	205.169.63.14
255.255.255.252	30	2	205.169.62.11	205.169.62.9	205.169.63.10
255.255.255.254	31	0	205.169.62.11		
255.255.255.255	32	1	205.169.62.11	205.169.62.11	205.169.62.11

Verify Discovery

When discovery is completed, you can verify if the process was successful.

To verify successful discovery, follow these steps:

Step 1 Choose Inventory > Device Management > Discovery.

Step 2 Choose the discovery job for which you want to view details.

Step 3 Choose User Jobs > Discovery from the left navigation pane and select the specific job.

Step 4 Under Discovery Job Instances, expand the arrow to view details about the devices that were discovered.

If devices are missing:

- Change your discovery settings, then rerun the discovery.
- Add devices manually. See Add Devices Manually (New Device Type or Series), on page 35 for more information.

The Discovery Job Instances section now displays Export and Refresh buttons. You can export the job information as both PDF and CSV.

Import Devices from Another Source

If you have another management system from which you want to import your devices, or if you want to import a spreadsheet that lists all of your devices and their attributes, you can add device information into by importing a bulk device file. You must ensure that the CSV file you plan to import is complete and properly formatted, as explained in Create Device Import CSV Files, on page 34.

Step 1 Choose Inventory > Device Management > Network Devices, click the + icon above the Network Devices table and then click Bulk Import.

Step 2 From the Operation drop-down list, choose Device.

Step 3 Next to Select CSV File, click Browse to navigate to and select the CSV file that contains the devices that you want to import.

Step 4 Click Import.

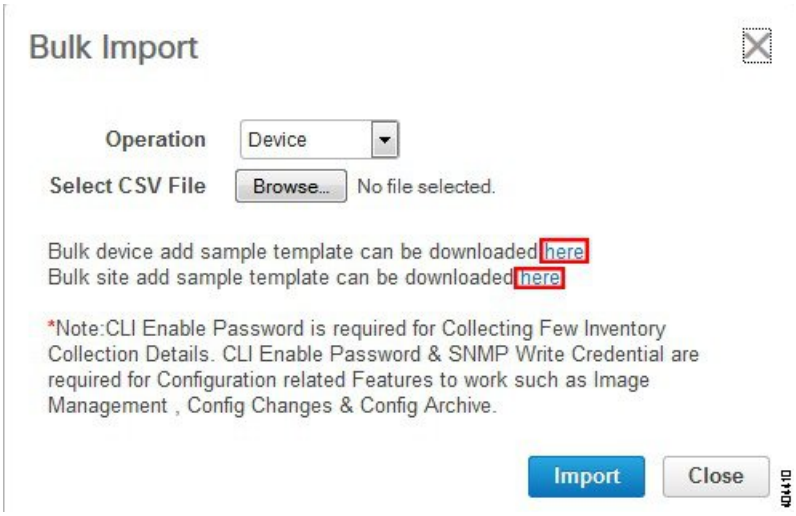
Step 5 Check the status of the import by choosing Administration > Dashboards > Job Dashboard > UserJobs > Device Bulk Import.

Step 6 Click the arrow to expand the job details and view the details and history for the import job.

Create Device Import CSV Files

If you want to use a CSV file to import your devices from another source into , you should prepare the CSV file using the device template, which you can download from as follows:

1. Choose Inventory > Device Management > Network Devices Inventory > Device Management >. Then click Bulk Import.
2. Click the here link next to "Bulk device add sample template can be downloaded" (as highlighted in the figure below). The template contains all of the fields and descriptions for the information that must be contained in the CSV device file you plan to import.



Please note that when you add devices by importing a CSV file, the extent to which can manage these devices will depend on the information you provide in the CSV file. For example: If you do not provide values for the CLI username, CLI password, CLI enable password, and CLI timeout value fields for a device in the CSV file, will be unable to modify that device's configurations, update device software images, or perform other useful functions.

This will also affect collection of complete device inventory. For partial inventory collection in , you must provide values for at least the following fields in the CSV file:

- Device IP address
- SNMP version
- SNMP read-only community strings
- SNMP write community strings
- SNMP retry value
- SNMP timeout value

For full inventory collection in Prime Infrastructure, you must also provide a value for the Protocol field, as well as values for the fields that correspond to the protocol you specify. For example: If you specify a value of **SNMPv3** in the Protocol field, you must also specify values for the SNMPv3 fields in the sample CSV file (such as the SNMPv3 username and authorization password).

You can specify the credential profile in the CSV file to apply the credentials to a set of devices. If you specify the credential profile and also enter the values manually in the CSV file, the device will be managed based on a combination of the manually entered credentials and the credential profile, with the manually entered credentials taking higher priority. For example, if the CSV file contains a credential profile with SNMP and Telnet credentials in addition to manually entered SNMP credentials, then the device is managed based on the manually entered SNMP credentials and the Telnet credentials in the credential profile.

If the CSV file you plan to import contains any User Defined Field (UDF) parameters, you must ensure that you add these UDF parameters before importing the CSV file. You can do this by selecting Administration > Settings > System Settings > Inventory > User Defined Fields and then adding each of the UDF parameters. The UDF column in your CSV file must be begin with **UDF:**, as indicated in the CSV template. Do not use the special characters : ; and # for UDF field parameters.

Note During bulk import, the CSV file must contain only the IP Address and Credential Profile Name information.

Add Devices Manually (New Device Type or Series)

Use this procedure to add a new device type and to test your settings before applying them to a group of devices.

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Click the + icon above the Network Devices table, then choose Add Device.

Step 3 In the Add Device dialog box, complete the required fields. Click the "?" next to a field for a description of that field.

Note Telnet/SSH information is mandatory for devices .

Step 4 (Optional) Click Verify Credentials to validate the credentials before adding the device.

Step 5 Click Add to add the device with the settings you specified.

Note For NCS 2000 devices, the "Enable Single Session TL1" setting takes effect only for devices running release 11.0 onwards.

Note , by default, does not accept UCS with self-signed certification. User can enable it manually by adding the following lines in the /opt/CSCOlumos/xmp_inventory/xde-home/inventoryDefaults/ncsCIMC.def file.

```
<default attribute="HTTPS_TRUST_CONDITION">always</default>

<default attribute="HTTPS_HOSTNAME_VERIFICATION_STRATEGY">allow_all</default>
```

Add a Virtual Device Context Device

In , Cisco NX-OS software supports Virtual Device Contexts (VDCs), which partition a single physical device into multiple logical devices that provide fault isolation, management isolation, address allocation isolation, service differentiation domains, and adaptive resource management. A VDC allows a switch to be virtualized at the device level. It runs as a separate logical entity within the switch that maintains its own set of running software processes, has its own configuration, and is managed by an administrator. VDC1 is the default (Admin) VDC and has a special role: It allows you to configure child VDCs and allocate resources.

manages all Cisco Nexus switch features (including VDCs) on devices running Cisco NX-OS software release 6.2(12) or later.

To add the device with the default VDC, complete the following procedure:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 From the Add Device drop-down list, choose Add Device.

Step 3 Specify the required settings in the various tabs.

To view a description of a particular parameter, place your cursor over its ? icon.

Step 4 (Optional) Click Verify Credentials to confirm that the credentials you entered are valid before adding the device.

Step 5 Click Add to add the device with the settings you specified.

After successful inventory collection, the device with the default VDC is added. Subsequently, child VDCs are added automatically and the configuration is stored in the database.

Add a Meraki Device to Prime Infrastructure

You can monitor all Meraki Access Point, Meraki Security Appliances and Meraki switches in Cisco Prime Infrastructure. Cisco Prime Infrastructure uses SNMP protocol to extract information about the Meraki devices, from Cloud, for both monitoring and inventory purposes.

Integrating Cisco Meraki into Cisco Prime Infrastructure requires the following;

- Enable SNMP on the Dashboard
- Add the Meraki Dashboard to the Cisco Prime Infrastructure Server
- Verify Connectivity

To add a Meraki device to Prime Infrastructure, perform the following steps :

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Click the + icon above the Network Devices table, then choose Add Device.

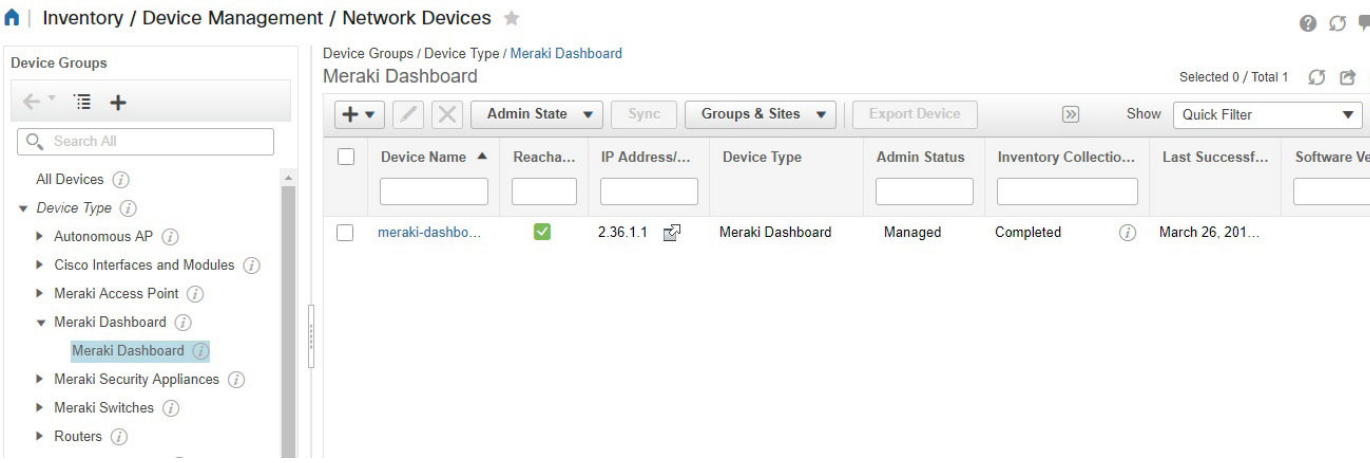
Step 3 Enter the IP Address or DNS Name of the Meraki Dashboard.

Step 4 Enter the SNMP v2/v3 credentials in the Add Device screen.

Step 5 (Optional) Click Verify Credentials to validate the credentials before adding the device.

Step 6 Click Add to add the devices with the settings you specified. The device details will be displayed in the right pane. Some of which include:

- Device Name
- Reachability/Status
- IP address/DNS name
- Device Type or Model
- MAC address
- Client Count
- Serial Number
- Mesh Status
- Network Name.



The Meraki Dashboard remains the single point of configuration for Meraki devices. Cisco Prime makes it very easy to get to any specific device by including a device link next to the IP Address of the device. These links will launch a browser window that will bring the administrator right to the device in the Meraki Dashboard which helps you to extract comprehensive information about a particular device.

Note You must select an appropriate device group from the group selector/object selector in the Network Devices page to view the required the Access Points, Switches, and Security Appliances.

Prerequisites for Adding Wireless Controllers

Note the following information when adding wireless devices to Prime Infrastructure:

- When you remove a wireless controller from Prime Infrastructure, a warning message appears to confirm whether the access points associated with that controller also need to be removed.
- If you are adding a controller across a GRE link using IPSec or a lower MTU link with multiple fragments, you may need to adjust the values of Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU. If these values are too high, the controller might not be added to Prime Infrastructure.

  To adjust the Maximum VarBinds per Get PDU or Maximum VarBinds per Set PDU values: Stop the Prime Infrastructure server, choose Administration > Settings > Network and Device > SNMP, and edit the Maximum VarBinds per Get PDU and Maximum VarBinds per Set PDU values to 50 or lower.
- If you are adding a wireless controller and receive the error message "Sparse table not supported", verify that you are running compatible versions of both Prime Infrastructure and WLC before retrying. For information on compatible versions of the two products, see the Cisco Wireless Solutions Software Compatibility Matrix entry for Prime Infrastructure, on Cisco.com.
- Prime Infrastructure acts as a trap receiver for controllers you add. The following traps are enabled on the controller: 802.11 Disassociation, 802.11 Deauthentication, and 802.11 Authenticated.
- When you add a new controller, the Reachability of the controller will be listed as "Unknown" while Prime Infrastructure attempts to communicate with the new controller. The controller's Reachability changes to "Reachable" or "Ping Reachable" once the communication with the controller is successful.
- When Compliance is enabled, the WLC can go to partial inventory collection state due to the following reasons:
  - CLI credential does not have read-write privilege.
  - WLC closes the connection during synchronization.
  - WLC does not respond in the configured time out period.
- To update the credentials of multiple controllers in bulk, choose Inventory > Network Devices > Wireless Controllers. Then select the controllers you need to update and click the Edit icon. Finally, select the credential profile and click Update or Update & Sync.
- You can also update the credentials of multiple controllers in bulk by creating a CSV file that contains a list of controllers to be updated. Make sure there is one controller per line, with each line a comma-separated list of the controller attributes you want updated.
  - Choose Inventory > Network Devices > Wireless Controllers.
  - Click the + icon above the table.
  - Choose Bulk Import and browse to the CSV file.

Validate Added Devices and Troubleshoot Problems

To monitor the discovery process, follow these steps:

Step 1 To check the discovery process, choose Inventory > Device Management > Discovery.

Step 2 Expand the job instance to view its details, then click each of the following tabs to view details about that device's discovery:

- Reachable—Devices that were reached using ICMP. Devices may be reachable, but not modeled, this may happen due to various reasons as discussed in Add Devices Using Discovery, on page 30. Check the information in this tab for any failures.
- Filtered—Devices that were filtered out according to the customized discovery settings.
- Ping Reachable—Devices that were reachable by ICMP ping but could not be communicated using SNMP. This might be due to multiple reasons: invalid SNMP credentials, SNMP not enabled in device, network dropping SNMP packets, etc.
- Unreachable—Devices that did not respond to ICMP ping, with the failure reason.
- Unknown— cannot connect to the device by ICMP or SNMP.

Note For devices that use the TL1 protocol, make sure that node names do not contain spaces. Otherwise, you will see a connectivity failure.

Step 3 To verify that devices were successfully added to , choose Inventory > Device Management > Network Devices. Then:

- Verify that the devices you have added appear in the list. Click a device name to view the device configurations and the software images that collected from the devices.
- View details about the information that was collected from the device by hovering your mouse cursor over the Inventory Collection Status field and clicking the icon that appears.
- Check the device's Reachability and Admin Status columns. See Device Reachability and Admin States, on page 40.

Check a Device's Reachability State and Admin Status

Use this procedure to determine whether can communicate with a device (reachability state) and whether it is managing that device (admin status). The admin status also provides information on whether the device is being successfully managed by .

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Locate your device in the Network Devices table.

a) From the Show drop-down list (at the top right of the table), choose Quick Filter.
b) Enter the device name (or part of it) in the text box under the Device Name column.

Step 3 Check the information in the Reachability and Admin Status columns. See Device Reachability and Admin States, on page 40 for descriptions of these states.

Device Reachability and Admin States

Device Reachability State—Indicates whether can communicate with the device using all configured protocols.

Table 7: Device Reachability State

Icon	Device Reachability State	Description	Troubleshooting
	Reachable	can reach the device using SNMP, or the NCS 2K device using ICMP.	—
	Ping reachable	can reach the device using Ping, but not via SNMP.	Although ICMP ping is successful, check for all possible reasons why SNMP communication is failing. Check that device SNMP credentials are the same in both the device and in , whether SNMP is enabled on the device, or whether the transport network is dropping SNMP packets due to reasons such as mis-configuration, etc. .
	Unreachable	cannot reach the device using Ping.	Verify that the physical device is operational and connected to the network.
	Unknown	cannot connect to the device.	Check the device.

Device Admin State—Indicates the configured state of the device (for example, if an administrator has manually shut down a device, as opposed to a device being down because it is not reachable by Ping).

Table 8: Device Admin State

Device Admin State	Description	Troubleshooting
Managed	is actively monitoring the device.	Not Applicable.
Maintenance	is checking the device for reachability but is not processing traps, syslogs, or TL1 messages.	To move a device back to Managed state, see Move a Device To and From Maintenance State, on page 41.

Unmanaged	is not monitoring the device.	In the Network Devices table, locate the device and click the "i" icon next to the data in the Last Inventory Collection Status column. The popup window will provide details and troubleshooting tips. Typical reasons for collection problems are: • Device SNMP credentials are incorrect. • The deployment has exceeded the number of devices allowed by its license. • A device is enabled for switch path tracing only. If a device type is not supported, its Device Type will be Unknown. You can check if support for that device type is available from Cisco.com by choosing Administration > Licenses and Software Updates > Software Update and then clicking Check for Updates.
Unknown	cannot connect to the device.	Check the device.

Move a Device To and From Maintenance State

When a device's admin status is changed to Maintenance, will neither poll the device for inventory changes, nor will it process any traps or syslogs that are generated by the device. However, will continue to maintain existing links and check the device for reachability.

See Device Reachability and Admin States, on page 40 for a list of all admin states and their icons.

Step 1 From the Network Devices table, choose Admin State > Set to Maintenance State.

Step 2 To return the device to the fully managed state, choose Admin State > Set to Managed State.

Edit Device Parameters

You can edit the device parameters of a single device or multiple devices by choosing Inventory > Device Management > Network Devices.

To edit device parameters, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Select a single device or multiple devices and then click the Edit icon.

Editing more than 9 devices triggers a job in the Job Dashboard page. The status of the bulk edit is displayed in that page.

Step 3 Update the required parameters.

Step 4 Click Update to update the parameters of all of the selected devices or Update & Sync to update and synchronize the devices with the updated parameters.

Synchronize Devices

To synchronize the Prime Infrastructure database with the configuration running on a device, you can force an inventory collection.

To synchronize devices, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Select the device whose configuration you want synchronized with the configuration stored in the Prime Infrastructure database.

Step 3 Click Sync.

Note If the synchronized device is a default/Admin VDC, then all the configuration of all the child VDCs are synchronized automatically and the configuration is updated in the Prime Infrastructure database. Admin VDC sync will also add the newly added VDC in hardware to the user interface or delete the deleted VDC in hardware from the user interface.

Smart Inventory

Smart Inventory allows only limited features to be collected if the commit id on the device is not changed. Otherwise, full collection of features will happen. Smart Inventory aims to reduce the amount of data transferred between Prime Infrastructure and the device in a smart way. Prime Infrastructure will do a major inventory collection and full config archive only when there is a change in the configuration of the device. If there is no change in the running configuration of the device, only the physical information like images, flash, files, interface status, etc will be collected from the device. If there is no change in the running config of the device, config archive will not be triggered.

To enable Smart Inventory:

Step 1 Choose Administration > System Settings > Inventory > Smart Inventory.

Step 2 Select the Enable Smart Inventory Globally check box. All the supported devices will be listed.

Note You can also enable/disable Smart Inventory for the individual devices. Select the required devices and click Enable or Disable button.

Add NAM HTTP/HTTPS Credentials

If you are using Cisco Network Analysis Modules (NAMs) to monitor your network, you must add HTTPS credentials so that Prime Infrastructure can retrieve data from them. This is especially important for users who have licensed Assurance features, as most Assurance features depend on NAM data to work.

Prime Infrastructure polls NAMs directly via HTTP (or HTTPS) to collect their data. This type of polling requires Prime Infrastructure to store each NAMs' HTTP credentials. Unlike with SNMP community strings

and Telnet/SSH credentials, you cannot enter NAM HTTP credentials during the discovery process. You can only specify NAM HTTP credentials after the modules are discovered or added to inventory.

Follow these steps to add HTTP credentials for a single NAM. You can repeat this task for all NAMs from which you want Prime Infrastructure to collect data.

Step 1 Choose Inventory > Device Management > Network Devices > Device Type > Cisco Interfaces and Modules > Network Analysis Modules.

Step 2 Select one of the NAMs and click Edit.

Step 3 In the Edit Device window, under Http Parameters:

- Protocol—Select the HTTP protocol, HTTP or HTTPS. The TCP Port will change automatically to the default port for the protocol that you have selected.
- TCP Port—Enter a different TCP Port if you want to override the default.
- Username—Enter the name of a user who can access the NAM via HTTP or HTTPS.
- Password—Enter the password for the username that you entered.
- Confirm Password—Enter the password a second time to confirm.

Step 4 Choose Update.

Export Device Information to a CSV File

When you export the device list to a file, all device information is exported into a CSV file. The file is then compressed and encrypted using a password you select. The exported file contains information about the device's SNMP credentials, CLI settings, and geographical coordinates. The exported file includes device credentials but does not include credential profiles.

Caution Exercise caution while using the CSV file as it lists all credentials for the exported devices. You should ensure that only users with special privileges can perform a device export.

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Select the devices that you want to export, then click Export Device (or click  and choose Export Device).

Step 3 In the Export Device dialog box, enter a password that will be used to encrypt the exported CSV file. Users will need to supply this password to open the exported file.

Step 4 Enter the password, confirm password, or export file name and click Export. Depending on your browser configuration, you can save or open the compressed file.

Apply Device Credentials Consistently Using Credential Profiles

Credential profiles are collections of device credentials for SNMP, Telnet/SSH, HTTP, and TL1. When you add devices, you can specify the credential profile the devices should use. This lets you apply credential settings consistently across devices.

If you need to make a credential change, such as changing a device password, you can edit the profile so that the settings are updated across all devices that use that profile.

To view the existing profiles, choose Inventory > Device Management > Credential Profiles.

Create a New Credential Profile

Use this procedure to create a new credential profile. You can then use the profile to apply credentials consistently across products, or when you add new devices.

Step 1 Select Inventory > Device Management > Credential Profiles.

Step 2 If an existing credential profile has most of the settings you need, select it and click Copy. Otherwise, click Add.

Step 3 Enter a profile name and description. If you have many credential profiles, make the name and description as informative as possible because that information will be displayed on the Credential Profiles page.

Step 4 Enter the credentials for the profile. When a device is added or updated using this profile, the content you specify here is applied to the device.

The SNMP read community string is required.

Step 5 Click Save Changes.

Apply a New or Changed Profile to Existing Devices

Use this procedure to perform a bulk edit of devices and change the credential profile the devices are associated with. This operation overwrites any existing association between a device and a credential profile. You can also use this operation to synchronize device configurations with the new settings.

Note Make sure the profile's credential settings are correct before following this procedure and selecting Update and Sync. That operation will synchronize the devices with the new profile.

Step 1 Configure the credential profile using one of these methods:

- Create a new credential profile by choosing Inventory > Device Management > Credential Profiles, and clicking Add.
- Edit an existing profile by choosing Inventory > Device Management > Credential Profiles, selecting the profile, and clicking Edit.

Step 2 When you are satisfied with the profile, choose Inventory > Device Management > Network Devices.

Step 3 Filter and select all of the devices you want to change (bulk edit).

Step 4 Click Edit, and select the new credential profile from the Credential Profile drop-down list.

Step 5 Save your changes:

- Update saves your changes to the database.
- Update and Sync saves your changes to the database, collects the device's physical and logical inventory, and saves all inventory changes to the database.

Delete a Credential Profile

This procedure deletes a credential profile from . If the profile is currently associated with any devices, you must disassociate them from the profile.

Step 1 Check whether any devices are using the profile.

a) Go to Inventory > Device Management > Credential Profiles.
b) Select the credential profile to be deleted.
c) Click Edit, and check if any devices are listed on the Device List page. If any devices are listed, make note of them.

Step 2 If required, disassociate devices from the profile.

a) Go to Inventory > Device Management > Network Devices.
b) Filter and select all of the devices you want to change (bulk edit).
c) Click Edit, and choose --Select-- from the Credential Profile drop-down list.
d) Disassociate the devices from the old profile by clicking OK in the warning dialog box.

Step 3 Delete the credential profile by choosing Inventory > Device Management > Credential Profiles, selecting the profile, and clicking Delete.

Export and Import a Credential Profile

You can export and import the credentials profile from device management using the following steps:

Step 1 Choose Inventory > Device Management > Credential Profiles

Step 2 Select the credential profile that you want to export, click Export Profile.

Step 3 Enter the following credentials in the Export Profile pop-up window:

- Password
- Confirm Password
- Export File Name

Step 4 Click Export to save the zip file which contains Profile and Profile associated with devices csv files.

Step 5 To import the credential profile, use the following steps:

Step 6 Login to the Prime Infrastructure Server.

Step 7 Choose Inventory > Device Management > Credential Profiles.

Step 8 Click Bulk Import.

Step 9 In the Bulk Import pop-up, browse the credential profile .csv file and Click Import.

Caution You should not import Profile_associated_devices .csv files during bulk import.

Step 10 Once the import is completed, the credential profile bulk import job is created. You can navigate to Administration > Dashboard > Job Dashboard > User Jobs > Credential Profile Bulk Import to check the job.

Create Groups of Devices for Easier Management and Configuration

Organizing your devices into logical groupings simplifies device management, monitoring, and configuration. As you can apply operations to groups, grouping saves time and ensures that configuration settings are applied consistently across your network. In smaller deployments where all devices can be configured with the same settings, you may only need to create one general device group. The grouping mechanism also supports subgroups. You will see these groups in many of the GUI windows.

When a device is added to , it is assigned to a location group named Unassigned. If you are managing a large number of devices, be sure to move devices into other groups so that the Unassigned Group membership does not become too large.

How Groups Work

For information on how elements are added to groups, see How Elements Are Added to Groups: Dynamic, Manual, and Mixed Groups, on page 48.

Network Device Groups

The following table lists the supported types of network device groups. The device groups can be accessed from the Inventory.

Network Device Group Type	Membership Criteria	Can Be Created or Edited By Users?
Device Type	Devices are grouped by family (for example, Routers, Switches and Hubs, and so forth). Under each device family, devices are further grouped by series. New devices are automatically assigned to the appropriate family and series groups. For example, a Cisco ASR 9006 would belong to Routers (family) and Cisco ASR 9000 Series Aggregation Services Routers (series). Note the following: • You cannot create a device type group; these are dynamic groups that are system-defined. Instead, use device criteria to create a user-defined group and give it an appropriate device name. • Device type groups are not displayed in Network Topology maps. • Unsupported devices discovered by are automatically assigned the Unsupported Cisco Device device type and are listed under Device Type > Unsupported Cisco Device Family.	No
Location	Location groups allow you to group devices by location. You can create a hierarchy of location groups(such as theater, country, region, campus, building, and floor) by adding devices manually or by adding devices dynamically. A device should appear in one location group only, though a higher level "parent" group will also contain that device. For example, a device that belongs to a building location group might also indirectly belong to the parent campus group. By default, the top location of the hierarchy is the All Locations group. All devices that have not been assigned to a location appear under the Unassigned group under All Locations.	Yes
User Defined	Devices are grouped by a customizable combination of device and location criteria. You can customize group names and use whatever device and location criteria you need.	Yes

Port Groups

The following table lists the supported types of port groups.

Port Group Type	Membership Criteria	Can be created or edited by users?
Port Type	Grouped by port type, speed, name, or description. Ports on new devices are automatically assigned to the appropriate port group. You cannot create Port Type groups. Instead, use device criteria to create a user-defined group, and create subgroups under the user-defined group.	No; instead create a User Defined Group

System Defined	Grouped by port usage or state. Ports on new devices are automatically assigned to the appropriate port group. Link Ports—Ports that are connected to another Cisco device or other network devices and are operating on "VLAN" mode and are assigned to a VLAN. Trunk Ports—Ports that are connected to a Cisco device or other network devices (Switch/Router/Firewall/Third party devices) and operating on "Trunk" mode in which they carry traffic for all VLANs. If the status of a port goes down, it is automatically added to Unconnected Port group. You cannot delete the ports in this group, and you cannot re-create this group as a sub group of any other group. You cannot create System Defined Port groups. Instead, use device criteria to create a user-defined group, and create subgroups under the user-defined group. **Note** As the WAN Interfaces is a static group, automatic port addition is not applicable. Hence, you must add the ports manually to the group.	No; instead create a User Defined Group
User Defined	Grouped by a customizable combination of port criteria, and you can name the group. If the group is dynamic and a port matches the criteria, it is added to the group.	Yes

Data Center Groups

The following table lists the supported types of data center groups.

Table 9: Data Center Group Supported Types

Data Center Group Type	Membership Criteria	Can be created or edited by users?
System Defined	Grouped by type (Data Center, Cluster, Virtual Machine (VM), Host). You cannot create System Defined Data Center Groups. Instead, use device criteria to create a user-defined Data Center group, and create subgroups under the user-defined group.	No. Can create User Defined Groups for VMs and Hosts
User Defined	Grouped by customizable combination of device and location criteria. You can customize group names and use whatever device criteria you need.	Yes

How Elements Are Added to Groups: Dynamic, Manual, and Mixed Groups

How elements are added to a group depends on whether the group is dynamic, manual, or mixed.

Method for Adding Devices	Description
Dynamic	automatically adds a new element to the group if the element meets the group criteria. While there is no limit to the number of rules that you can specify, the performance for updates may be negatively impacted as you add more rules.
Manual	Users add the elements manually when creating the group or by editing the group.
Mixed	Elements are added through a combination of dynamic rules and manual additions.

The device inheritance in parent-child user defined and location groups are as follows:

- User Defined Group—When you create a child group:
  - If the parent and child groups are both dynamic, the child group can only access devices that are in the parent group.
  - If the parent group is static and the child group is dynamic, the child group can access devices that are outside of the parent group.
  - If the parent and child groups are dynamic and static, the child group "inherits" devices from the parent device group.
- Location Group—The parent group inherits the child group devices.

Groups and Virtual Domains

While groups are logical containers for elements, access to the elements is controlled by virtual domains. This example shows the relationship between groups and virtual domains.

- A group named SanJoseDevices contains 100 devices.
- A virtual domain named NorthernCalifornia contains 400 devices. Those devices are from various groups and include 20 devices from the SanJoseDevices group.

Users with access to the NorthernCalifornia virtual domain will be able to access the 20 devices from the SanJoseDevices group, but not the other 80 devices in the group. For more details, see Create Virtual Domains to Control User Access to Devices.

Create User-Defined Device Groups

To create a new device type group, use the user-defined group mechanism. You must use this mechanism because device type groups are a special category used throughout . The groups you create will appear in the User Defined category.

To create a new group, complete the following procedure:

Step 1 Choose Inventory > Group Management > Network Device Groups.

Step 2 In the Device Groups pane, click the + (Add) icon and then choose Create User Defined Group.

Step 3 Enter the group's name and description. If other user-defined device type groups already exist, you can set one as the parent group by choosing it from the Parent Group drop-down list. If you do not select a parent group, the new group will reside in the User-Defined folder (by default).

Step 4 Add devices to the new group:

If you want to add devices that meet your criteria automatically, enter the criteria in the Add Devices Dynamically area. To group devices that fall within a specific range of IP addresses, enter that range in square brackets. For example, you can specify the following:

- IPv4-10.[101-155].[1-255].[1-255] and 10.126.170.[1-180]
- IPv6-2014::5217:[0000-ffff]:fe22:[1e40-1f41]

Note While there is no limit on the number of rules you can specify for a dynamic group, group update performance could become slower as the number of rules increases.

If you want to add devices manually, do the following:

a. Expand the Add Devices Manually area and then click Add.

b. In the Add Devices dialog box, check the check boxes for the devices you want to add, then click Add.

Step 5 Click the Preview tab to see the members of your group.

Step 6 Click Save.

The new device group appears in the folder you selected in Step 3.

View All Groups to Which a Device Belongs

To view the list of device groups to which a device belongs, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups.

Step 2 Enter an IP address or device name in the Search field in the Device Group pane on the left, to view the list of all groups to which the device belongs.

You can also search the group by entering the group name in the search field.

Create Location Groups

Step 1 Choose Inventory > Group Management > Network Device Groups.

Step 2 In the Device Groups pane on the left, click the Add icon, then choose Create Location Group.

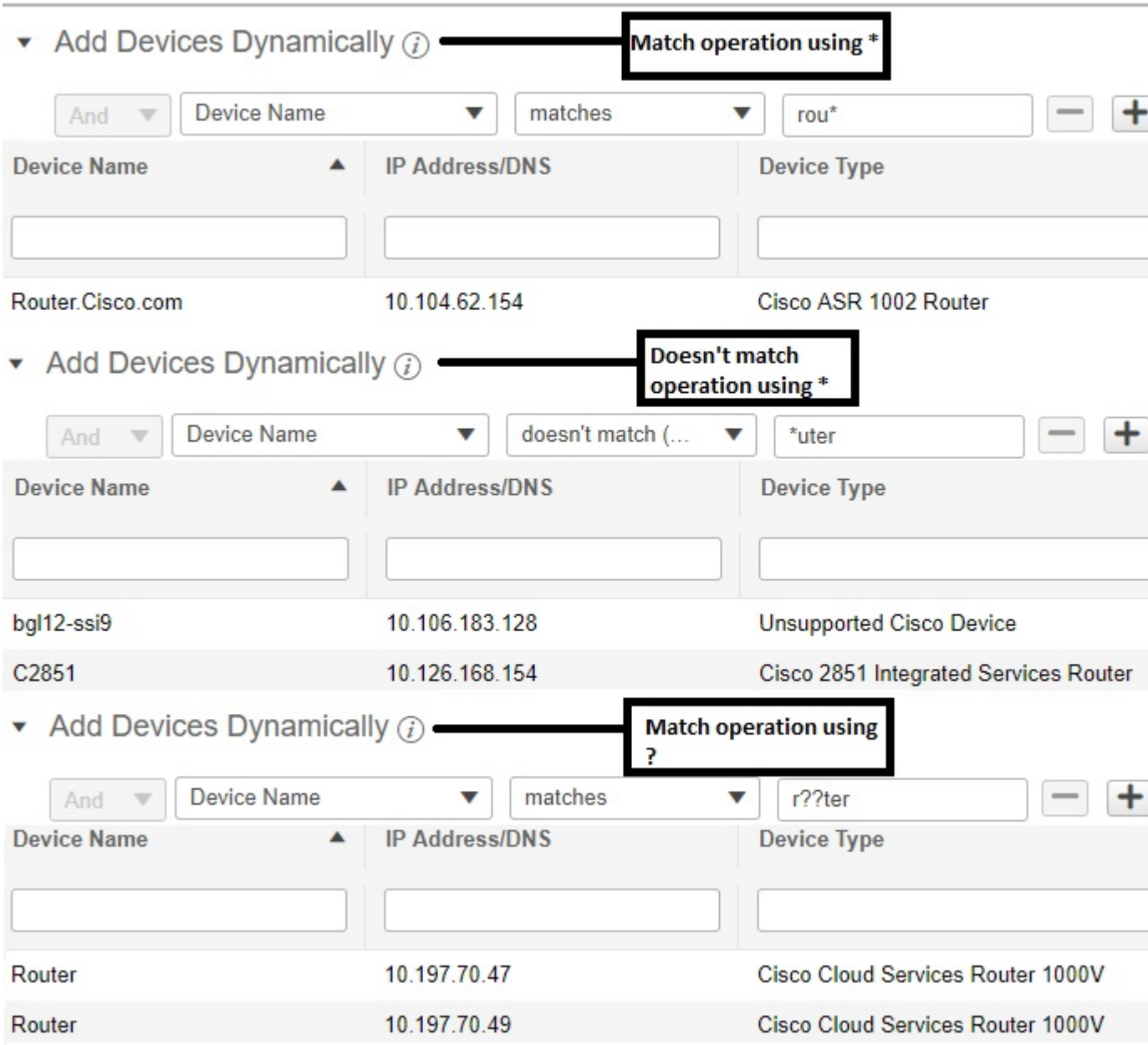
Step 3 Enter the name and description, and choose a group from the Parent Group drop-down list. By default, the group will be an All Locations subgroup (that is, displayed under the All Locations folder).

Step 4 If you are creating a device group based on geographical location, for example, all devices located in a building at a specific address, select the Geographical Location check box and specify the GPS coordinates of the group or click the

View Map link and click on the required location in the map. The GPS coordinates will be populated automatically in this case. Note that location groups defined with a geographic location are represented by a group icon in the geo map. The devices you add to the group will inherit the GPS coordinates of the group. Note that if geographical location is the primary reason for grouping a set of devices, it is recommended that the devices you add to the group do not have their own GPS coordinates that are different from the group's.

If you want to specify Civic Location, select the location from the drop-down list, by manually entering the search key word.

Step 5 If you want devices to be added automatically if they meet certain criteria, enter the criteria in the Add Device Dynamically area. Otherwise, leave this area blank.



While there is no limit on the number of rules that you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.

Step 6 If you want to add devices manually:

a) Under Add Devices Manually, click Add.

b) In the Add Devices dialog box, locate devices you want to add, then click Add.

Step 7 Click the Preview tab to see the group members.

Step 8 Click Save, and the new location group appears under the folder you selected in Step 3 (All Locations, by default).

When you edit a location group, you may change the group type if the following conditions are met:

- The group type is Default.
- The group does not have any subgroups.

Create Groups Using CSV Files

To import a group using a CSV file that lists all attributes of the group that you want to add into Prime Infrastructure, follow these steps.

Step 1 Choose Inventory > Group Management > Network Device Groups, then click Import Groups.

Step 2 Click the here link to download the sample template for the CSV file.

Make sure that you retain the required information in the CSV file as mentioned in the Template.

Step 3 Click Choose File in the Import Groups dialog box, and select the CSV file that contains the group that you want to import.

Step 4 Click Import.

Step 5 Choose Administration > Dashboards > Job Dashboard, then click Import Groups to view the status of the job.

Export Groups to CSV Files

To export group information as a CSV file, follow these steps.

Step 1 Choose Inventory > Group Management > Network Device Groups.

Step 2 Select PI or APIC-EM.

Step 3 Click Export Groups to download the CSV file including the details of all location groups, into your local system.

Add APs to Device Groups and Location Groups

SUMMARY STEPS

1. Choose Inventory > Group Management > Network Device Groups.
2. In the Device Groups pane on the left, hover the mouse over the expand icon next to User Defined or Location and click Add SubGroup.
3. Enter the name, description, and parent group (if any).
4. Add APs in one of the following ways:
5. Click Preview to view the APs that are automatically added to the group based on the specified rule and the manually added APs.
6. Click Save.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Choose Inventory > Group Management > Network Device Groups.	
Step 2	In the Device Groups pane on the left, hover the mouse over the expand icon next to User Defined or Location and click Add SubGroup.	
Step 3	Enter the name, description, and parent group (if any).	
Step 4	Add APs in one of the following ways:	• Manually—Click Add under Add Devices Manually and select the APs you want to add to the group. • Dynamically—Specify rules to which APs must comply before they are added to this port group. You do not add APs to dynamic groups. Prime Infrastructure adds APs that match the specified rules to the dynamic group. If you select any type of Location group other than Default, the APs will not be added dynamically.
Step 5	Click Preview to view the APs that are automatically added to the group based on the specified rule and the manually added APs.	
Step 6	Click Save.	If the group has Unified AP or Third Party AP as a member, a new tab is added in the right hand table in the Device Work Center, to display the APs.

Create Port Groups

To create a port group, follow these steps:

Step 1 Choose Inventory > Group Management > Port Groups.

Step 2 From Port Groups > User Defined, hover your cursor over the "i" icon next to User Defined and click Add SubGroup from the popup window.

Step 3 Enter the name and description, and choose a group from the Parent Group drop-down list. By default, the port group will be under the User Defined folder.

Step 4 Choose the devices a port must belong to in order to be added to the group. From the Device Selection drop-down list, you can select:

- Device—To choose devices from a flat list of all devices.
- Device Group—To choose device groups (Device Type, Location, and User Defined groups are listed).

Step 5 If you want ports to be added automatically if they meet your criteria, enter the criteria in the Add Ports Dynamically area. Otherwise, leave this area blank.

While there is no limit on the number of rules that you can specify for a dynamic group, the group update performance could become slower as the number of rules increases.

Step 6 If you want to add devices manually:

a) Under Add Ports Manually, click Add.
b) In the Add Ports dialog box, locate devices you want to add, then click Add.

Step 7 Click the Preview tab to see the group members.

Step 8 Click Save, and the new port group appears under the folder you selected in Step 3 (User Defined, by default).

Create User-Defined Data Center Groups

In addition to the out-of-box data center and cluster groups, you can create user-defined groups for VMs and hosts. To create a user-defined group, complete the following procedure:

Step 1 Choose Inventory > Device Management > Compute Devices.

Step 2 From the Compute Resources pane, locate User Defined Hosts and VMs and place your cursor over its i (information) icon.

Step 3 From the Actions area, click Add Subgroup.

The Add Device Subgroup page opens.

Step 4 Enter the group's name and description, and then choose the folder the group will reside in from the Parent Group down-down list.

Step 5 Add devices to the location group:

- If you want to add devices that meet your criteria automatically, enter the criteria in the Add Devices Dynamically area.

  Note While there is no limit on the number of rules you can specify for a dynamic group, group update performance could become slower as the number of rules increases.

- If you want to add devices manually, do the following:

  a. Expand the Add Devices Manually area and then click Add.

  b. In the Add Devices dialog box, check the check boxes for the devices you want to add, then click Add.

Step 6 Click the Preview tab to see the devices that will belong to the group.

Step 7 Click Save. The new group appears in the folder you selected in Step 4.

Edit User-Defined Groups

You can change the parent group, add devices, and modify device rules using the edit option.

Procedure

	Command or Action	Purpose
Step 1	Choose Inventory > Group Management > Network Device Groups.	
Step 2	In the Device Groups pane on the left, click the name of the group you want to edit.	
Step 3	Click Edit and modify the details.	When you are editing a location group, you can change the group type to Campus, if: • The group type is Default. • The group does not have any subgroups.
Step 4	Click Preview to view the updated device details.	
Step 5	Click Save to save the updated device details.	

Make Copies of Groups

When you create a duplicate of a group, names the group CopyOfgroup-name by default. You can change the name, if required.

To duplicate a group follow these steps:

Step 1 Choose Inventory > Group Management > Network Device Groups.

Step 2 Choose the group from the Device Groups pane on the left.

Step 3 Locate the device group you want to copy, then click the "i" icon next to it to open the pop-up window.

Step 4 Click Duplicate Group (do not make any changes yet) and click Save. creates a new group called CopyOfgroup-name.

Step 5 Configure your group as described in Create User-Defined Device Groups, on page 49 and Create Location Groups, on page 50.

Step 6 Verify your group settings by clicking the Preview tab and examining the group members.

Step 7 Click Save to save the group.

Copy User-Defined and Location Groups

You can duplicate any user-defined or location group using the Duplicate Group option. The duplicated group will contain all of the values from the original group, which you can modify. The populated group name will have a prefix of "CopyOf" by default. You can change the name, if required.

If you duplicate a child group, a copy of the child group is created under the same parent group.

If you duplicate a parent group, a copy of the respective child groups are created.

Procedure

	Command or Action	Purpose
Step 1	Choose Inventory > Group Management > Network Device Groups.	
Step 2	In the Device Groups pane on the left, locate the device group you want to duplicate. Then click the "i"icon next to the name of the group to display the popup menu.	
Step 3	Click Duplicate Group and update the group details.	
Step 4	Click Preview to view the duplicate group details.	
Step 5	Click Save to save the duplicate group.	

Hide Groups That Do Not Have Any Members

By default, will display a group in the web GUI even if the group has no members. Users with Administrator privileges can change this setting so that empty groups are hidden—that is, they are not displayed in the web GUI. (Hidden groups are not deleted from .)

Step 1 Choose Administration > Settings > System Settings, then choose Inventory > Grouping.

Step 2 Uncheck Display groups with no members, and click Save.

We recommend that you leave the Display groups with no members check box selected if you have a large number of groups and devices. Unselecting it can slow system performance.

Delete Groups

Make sure the group you want to delete has no members, otherwise will not allow the operation to proceed.

Step 1 Choose Inventory > Group Management > Network Device Groups.

Step 2 Locate the device group you want to delete in the Device Groups pane on the left, then click the "i" icon next to it to open the pop-up window.

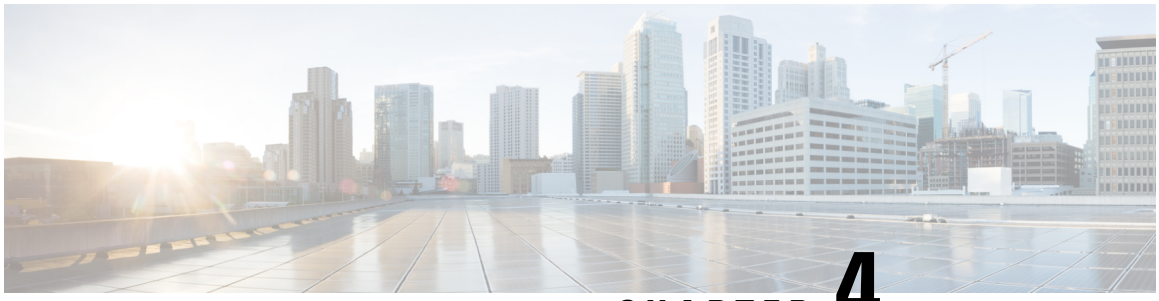
Step 3 Click Delete Group and click OK.

Create Compute Resource Groups

In addition to out-of-box groups for Compute Services devices such as Data Centers and clusters, you can create user-defined groups for UCS servers, hosts and VMs.

Procedure

	Command or Action	Purpose
Step 1	Choose Inventory > Compute Device Groups	
Step 2	In the Compute Resources at left, hover the mouse over the expand icon next to User Defined UCS or User Defined Hosts and VMs and click Add SubGroup.	
Step 3	Enter the group name and description, and select a parent group, if applicable.	
Step 4	In the Add Devices Dynamically pane, specify the rules that you want to apply to the devices in the group.	
Step 5	In the Add Devices Manually pane, choose the compute resources that you want to assign to the group.	
Step 6	Click Preview to view the devices that are automatically added to the group based on the specified rule and the manually added devices.	
Step 7	Click Save to add the compute resource group with the settings that you specified.	



CHAPTER 4

View Devices

View Network Devices

From the Network Devices page (Inventory > Device Management > Network Devices) or (Monitor > Managed Elements > Network Devices), you can view device inventory and device configuration information. This page contains the general administrative functions and configuration functions described in the following table.

Table 10: Network Devices Tasks

Task	Description	Location in the Network Devices Page
Manage devices	You can add, edit, delete, sync, and export devices, set the admin state for devices, add and delete devices from groups and sites, and perform a bulk import.	These features are available in the toolbar located at the top of the page. For more details, see Add Devices Manually (New Device Type or Series), Export Device Information to a CSV File, and Import Devices from Another Source.
	You can add, edit, delete, sync, and export the default and child VDCs.	For more information about VDCs, see Add Devices Manually (New Device Type or Series).
View basic device information and collection status	View information such as reachability status, IP address, device type, and collection status. **Note** Additionally, you can view the IP Address/DNS, Software Type, Location, Creation Timestamp, Device Role, Product Family, Serial Number, and Model Number details of the devices in the Network Devices screen. Click the settings icon at the top right corner, expand the Columns menu and select the desired option to make that particular information appear in the Network Devices screen.	From the IP Address column, click the i (information) icon to open the 360° view for that device . From the Last Inventory Collection column, place your cursor over the i (information) icon to open a pop-up window that lists the inventory collection errors that have occurred.

Task	Description	Location in the Network Devices Page
Manage device groups	By default, creates dynamic device groups and assigns devices to the appropriate Device Type folder. You can create new device groups that reside under the User Defined folder.	Device groups are displayed in the Device Groups pane. A new radio button, RMI+RP, is added apart from the existing RP radio button. Two new text boxes, Chassis 1 IP and Chassis 2 IP and a check box, Gateway Failure, check box are newly added. This check box appears only after you configure a device.
Add devices to site groups	After you set up a site group, you can add devices to it from the Network Devices page. To add devices to a site map, choose Maps > Site Map. **Note** A device can only belong to one site group hierarchy.	• From the Groups & Sites drop-down list, choose Add to Group. • From the Add Device drop-down list, choose Add Device and then choose the appropriate group from the Add to Group drop-down list.. • With a device selected, click Edit Device and the choose the appropriate group from the Add to Group drop-down list. • From the Add Device drop-down list, choose Bulk Import to import devices using a CSV file.
View device details	View device details such as memory, port, environment, chassis view, and interface information.	Click a device name hyperlink to open the Device Details page for that device.
	View device information and status, associated modules, alarms, neighbors, and interfaces, managed VDCs, and VDC details.	From the IP Address column, click the device's i (information) icon to open its 360° View.
Create and deploy configuration templates	You can configure device features on the selected device. You can also view the list of applied and scheduled feature templates that were deployed to the device. **Note** You may not be able to configure a few controller features from the Network Devices page. In this case, create a new template in the Features & Technologies page (Configuration > Templates > Features & Technologies) and deploy it to the device.	Click a device name hyperlink, then click the Configuration tab.
View device configurations	View archived configurations, schedule configuration rollbacks, and schedule archive collections.	Click a device name hyperlink, then click the Configuration Archive tab.

Task	Description	Location in the Network Devices Page
View software images	You can view the recommended software image for a single device and then import or distribute that image. .	1. Click a device name hyperlink, then click the Image tab. 2. Expand the Recommended Images area to view the recommended image for the device you selected. gathers the recommended images from both Cisco.com and the local repository. You can either import the recommended image or distribute it.
View and modify TrustSec configuration	You can view and modify the TrustSec configuration of a TrustSec-based device.	1. Click a device name hyperlink, then click the Configuration tab. 2. Choose Security > TrustSec > Wired 802_1x.
Chassis View	You can view a graphical representation of the front or back panel of a device.	Click a device name hyperlink to open the Device Details page for that device, which displays its Chassis View. **Note** The following devices support the Chassis View: • All AireOS Wireless LAN Controllers • The Cisco 5760 LAN controller • The Catalyst 3850 Switch • The Catalyst 3650 – 28 Port, 52 Port line card only • The Catalyst 4500 – 48 Port line card only • The Catalyst 9300 • The Catalyst 9400 • The Catalyst 9500 • The Catalyst 9600 • The Catalyst 4000 Switch **Note** For Cat 9k devices, only the standard PIDs are supported and there is no support for the combination of port modules. **Note** You can view the Chassis image in the Summary screen which provides details on port utilization and status of it.
View VDC details	You can view a VDC summary, VDC resources, top 3 VDCs for CPU utilization and allocated CPU, and VDCs managed.	Click a device name hyperlink, then click the VDC tab. **Note** The 360° View is not supported for the child vdc in the VDC tab.

Related Topics

View Compute Devices, on page 62

View Compute Devices

The Compute Devices page provides a consolidated view of all the devices that provide compute capability in your data center. To open this page, do one of the following:

- Choose Inventory > Device Management > Compute Devices.
- Choose Monitor > Managed Elements > Compute Devices.

Note The Compute Devices functionality is deplored starting from Cisco Prime Infrastructure version 3.5.

From here, you can view device inventory information for the physical devices (such as Cisco UCS B-series, C-series and E-series devices that support data center virtualization) and the data center components described in the following table.

Table 11: Compute Devices Tasks

Task	List View	Detailed View
View Data Centers	Shows the number of clusters, hosts, and VMs, VM status, discovery source, and monitoring status of the data center.	Click a data center name hyperlink to open its detailed view. This view displays 4 tabs: • Clusters tab—Shows the number of clusters available in this data center. • General tab—Shows the properties of the selected data center. • Hosts tab—Shows details of the hosts available in the selected data center and additional information on installed operating systems. • Virtual Machines tab—Shows details of the virtual machines available in the selected data center, as well as additional information on the memory granted and disk rate.

Task	List View	Detailed View
View Clusters	Shows the host count, number of VMs, VM power status, power on/off status of VMs and discovery sources.	Click a cluster name hyperlink to open its detailed view. This view displays 4 tabs: • General tab—Shows the properties of the selected cluster. • Alarms tab—Shows the alarms that have been generated for the cluster. • Hosts and Virtual Machines tab—Show the operational status, CPU usage, and memory usage of the hosts and VMs associated with the cluster.
View Hosts	Shows the name, status, IP address, hypervisor type, total number of VMs, VM status, and monitoring status of the host. You can configure this page to display additional information, such as a host's discovery source and alarm count. To do so, click the Settings icon and choose the column you want to add from the Columns list. **Note** If the host is installed on a Cisco UCS blade server managed by , the Physical Server column shows the blade server's name and the Physical Device Name column shows the name of the Cisco UCS chassis the blade server resides in.	Click a host name hyperlink to open its detailed view. From here, you can view the performance metrics of the host and its parent cluster. The performance metrics show a graphical representation of CPU utilization, memory usage, and network performance. The detailed view also provides 4 tabs: • General tab—Shows the properties of the selected host. • Virtual Machine tab—Shows the operational status, CPU usage, and memory usage of VMs that belong to the host. • Alarms tab—Shows the alarms that have been generated for the host. • User Defined Fields tab—From here, you can update any user-defined values that have been configured for the host.

Task	List View	Detailed View
View Virtual Machines	Shows the name, operational status, IP address, host name, operating system, and monitoring status of the selected VM. You can configure this page to display additional information, such as a VM's discovery source and alarm count. To do so, click the Settings icon and choose the column you want to add from the Columns list.	Click a VM name hyperlink to open its detailed view. From here, you can view the performance metrics for the VM as well as its parent host and cluster. The VM metrics show a graphical representation of CPU, memory, disk and network usage. The parent host metrics show a graphical representation of CPU, memory, and network usage. The parent cluster metrics show a graphical representation of CPU and memory usage. The detailed view also provides 4 tabs: • Virtual Machine General tab—Shows the properties of the selected VM. • Host General tab—Shows the properties for the physical server if the host is installed on a Cisco UCS blade server. • Alarms tab—Shows the alarms that have been generated for the VM. • User Defined Fields tab—From here, you can update any user-defined attributes that store additional information about devices, such as device location attributes.
View Physical Servers	Shows Cisco UCS blade server information such as ID, device name, IP address, operational status, cores, and memory. This page also shows the IP address, name, and OS for the host associated with the server.	From the Server ID column, click a server's ID hyperlink to open its detailed view and access tabs that provide information on server components such as CPU, memory, and adapters.
View Compute Services	Shows the name of a compute service, its operational status, IP address, type, the latest alarm generated for the service, and the total alarm count.	To be added....

Task	List View	Detailed View
View Cisco UCS Servers	Shows basic device information such as name, type, IP address, reachability status, and alarm count. From here, you can select a server and either add it to or remove it from a group.	From the Device Name column, click a server name hyperlink to open a schematic that illustrates the interconnection between Cisco UCS chassis and blade servers and their operational status.
View Discovery Sources	Shows the name of a discovery source, its reachability status, discovery job status, and virtual inventory collection status. From here, you can add a new device, edit or delete an existing device, and sync the selected device.	To be added....
View User-Defined UCS Servers	allows you to create groups that are populated automatically with the devices that meet the criteria you specify. To create a Cisco UCS server group, do the following: 1. From the Compute Resources pane, place your cursor over the i (information) icon to open a pop-up window. 2. From the Actions area, click Add Subgroup. 3. Complete Steps 3 through 6 of the procedure described in Create User-Defined Device Groups.	To be added....

Task	List View	Detailed View
View User-Defined Hosts and VMs	allows you to create groups that are populated automatically with the devices and VMs that meet the criteria you specify. To create a Host and VM group, do the following: 1. From the Compute Resources pane, place your cursor over the i (information) icon to open a pop-up window. 2. From the Actions area, click Add Subgroup. 3. Complete Steps 3 through 6 of the procedure described in Create User-Defined Device Groups.	To be added....

Related Topics

Create User Defined UCS Groups, on page 66
Create User Defined Hosts and VMs, on page 66

Create User Defined UCS Groups

In addition to viewing the compute device details, you can also create user defined UCS sub-groups. Hover your mouse over the expand icon next to User Defined UCS and click Add SubGroup. See Creating Device Groups in Related Topics. However, these User Defined UCS group is not reflected in Monitor > Monitoring Tools > Alarms and Events.

Related Topics

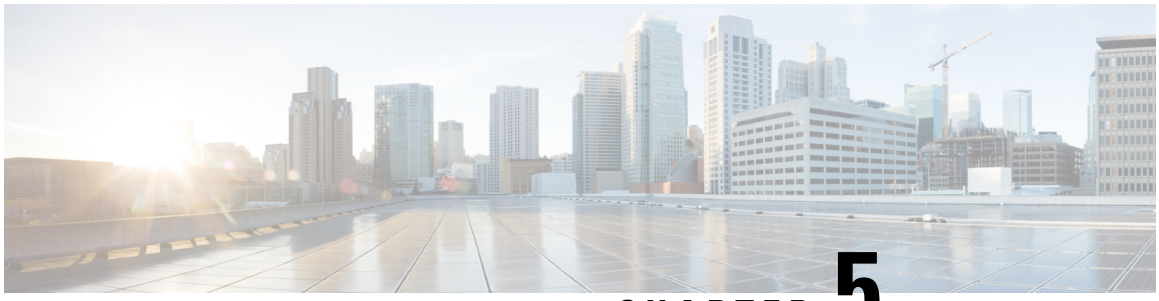
Create User Defined Hosts and VMs, on page 66

Create User Defined Hosts and VMs

You can create user defined Hosts and VMs Sub-groups similar to device groups. Hover your mouse over the expand icon next to User Defined Hosts and VMs and click Add SubGroup. However, these User Defined Hosts and VMs group are reflected in Monitor > Monitoring Tools > Alarms and Events to monitor the alarms or events from any member of this group.

Related Topics

Create User Defined UCS Groups, on page 66



CHAPTER 5

Manage Compute Resources

Manage VMware Vcenter Server

You can add, delete, edit, sync, and bulk import VMware Vcenter servers and also view the complete inventory of compute resources like data center, cluster, hosts and virtual machines (VMs).

Related Topics

Add a VMware vCenter Server, on page 67

CSV File Requirements for Importing Vcenter, on page 68

Add a VMware vCenter Server

Complete the following procedure to manually add a VMware vCenter server in order to manage it.

Before you Begin

You must install a Data Center Hypervisor license to collect vCenter server inventory information. For instructions on how to add this license, see .

Step 1 Choose Inventory > Device Management > Compute Devices.

Step 2 From the Compute Resources pane, click Discovery Sources.

Step 3 From the Add Device drop-down list, choose Add Device.

Step 4 Specify the following parameters in the Add Discovery Source dialog box:

a. Protocol—Choose HTTP or HTTPS.

b. Server—Enter the hostname or IP address of the vCenter server.

c. Port—Enter 80 for HTTP or 443 for HTTPS.

d. Username and Password—Enter the credentials required to log into the vCenter server.

You will need to enter the password a second time in order to confirm it.

Step 5 (Optional) Click Verify Credentials to confirm the credentials you entered are valid before adding the vCenter server.

Step 6 Click Add.

Step 7 From the Discovery Sources page, locate the vCenter server you just added and view its value in the Virtual Inventory Collection Status column.

If No License is displayed, you need to install a Data Center Hypervisor license. This license is required to collect the server's inventory information.

Related Topics

CSV File Requirements for Importing Vcenter, on page 68

CSV File Requirements for Importing Vcenter

To import a VMware vCenter server from another source into using a CSV file, download a sample template by doing the following:

1. Choose Inventory > Device Management > Compute Devices.
2. From the Compute Resources pane, click Discovery Sources.
3. From the Add Device drop-down list, choose Bulk Import.

   The Bulk Import dialog box opens.
4. Click the here link to download a bulk virtual discovery sample template.

To enable full inventory collection in , you must provide values for the following parameters in the CSV file for the discovery source:

- IP address or hostname
- Password
- Port number
- Username
- Protocol

Related Topics

Add a VMware vCenter Server, on page 67

Monitor Compute Resource Performance

monitors the managed compute resources by periodically polling the devices.

supports periodic polling of a predefined set of key performance indicators (KPIs) related to CPU, memory, disk and network for monitoring the health of the virtual elements. does not poll the VM directly, but it gets the data periodically from the Vcenter via the application programming interfaces (APIs). The default polling interval is 5 minutes. You can change the polling interval as described below.

Related Topics

Set the Polling Interval for Data Center Devices, on page 69
Set Up Cluster Monitoring, on page 69

Set the Polling Interval for Data Center Devices

Polling can be enabled on a data center, cluster, and host. When you do so, polling is automatically enabled on the children of the entity you select for polling. For example, if you enable polling on a cluster, pollilng is also enabled on all of the hosts and VMs that belong to that cluster.

To set the polling interval:

Step 1 Choose Administration > Settings > System Settings, then choose Inventory > Datacenter Settings.

Step 2 Choose the polling interval from the drop-down list.

5 mins is the default value.

Step 3 Click Save.

Related Topics

Set Up Cluster Monitoring, on page 69

Set Up Cluster Monitoring

Complete the following procedure to monitor a cluster:

Step 1 Choose Inventory > Device Management > Compute Devices.

Step 2 From the Compute Resources pane, click Clusters.

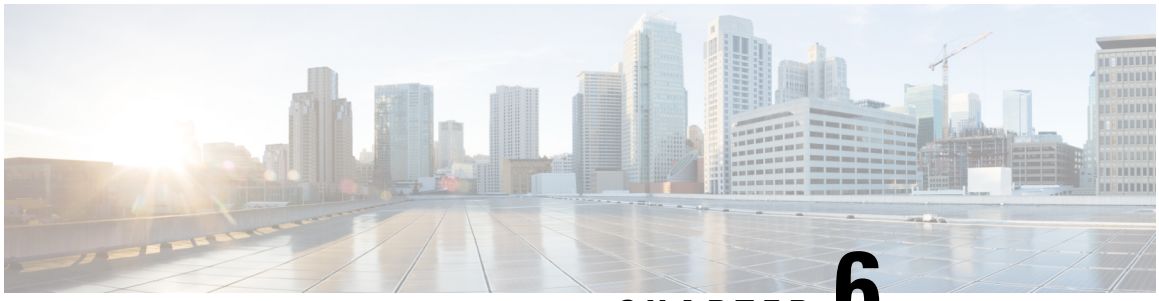
Step 3 Check the check box for the cluster you want to monitor and then click Start Monitoring.

Note the following:

- To stop monitoring a cluster, complete this procedure but click Stop Monitoring in Step 3 instead.
- You cannot stop the monitoring of a parent data center or cluster from its child host or cluster. However, you can stop the monitoring of a child host or cluster from its parent data center or cluster.

Related Topics

Set the Polling Interval for Data Center Devices, on page 69



CHAPTER 6

Manage Device Configuration Files

This chapter contains the following topics:

Set Up Device Configuration File Management

Control How Archiving is Triggered

By default, saves device configuration files to the archive when:

- A new device is added to
- When a device change notification is received

- Archive collection is not carried out in case of full or granular sync.

Note If there is an event occurrence, archive data is collected after the period of configured hold off timer.

Users with Administrator privileges can change these settings.

Step 1 Choose Administration > Settings > System Settings, then choose Inventory > Configuration Archive.

Step 2 Adjust the archiving settings depending on the following criteria.

Check this check box:	To archive files:
Archive configuration out-of-box?	When a new device is added (enabled by default)
Archive configuration on receiving configuration change events?	When a configuration change notification is sent (enabled by default); see Set Up Event-Triggered Archiving, on page 72

Step 3 To schedule regular archiving for groups of devices (or single devices):

a) Choose Inventory > Device Management > Configuration Archive.
b) Under the Devices tab, select the devices or device groups that you want to archive on a regular basis.
c) Click Schedule Archive and complete the schedule settings in the Recurrence area. If the operation will be performed on a large number of devices, schedule the archiving for a time that is least likely to impact production.
d) Click the Backup to Repository button to transfer device configuration periodically to external repository. You can configure or create the repository using CLI commands and the supported repositories are FTP, SSH FTP (SFTP) and Network File System (NFS).

Set Up Event-Triggered Archiving

By default, backs up a device's configuration file whenever it receives a change notification event. This function will work only if devices are configured properly; . For example, for devices running Cisco IOS XR and Cisco IOS XE, the following setting must be configured:

```
logging server-IP
```

When receives a configuration change event, it waits 10 minutes (by default) before archiving in case more configuration change events are received. This prevents multiple collection processes from running at the same time. To check or change this setting, choose Administration > Settings > System Settings, then choose Inventory > Configuration Archive and adjust the Hold Off Timer.

To turn off event-triggered archiving, choose Administration > Settings > System Settings, then choose Inventory > Configuration Archive and uncheck the Archive configuration on receiving configuration change events? check box.

Specify Items to be Excluded When Configuration Files Are Checked for Changes

Some lines in device configuration files should be excluded when compares different versions to identify changes. excludes some lines by default, such as clock settings for routers and switches. If you have Administrator privileges, you can check which lines are excluded, and add more lines to be excluded.

Step 1 Choose Administration > Settings > System Settings, then choose Inventory > Configuration Archive.

Step 2 Click the Advanced tab.

Step 3 In the Product Family list, choose the devices or groups to which you want to apply the command exclusions.

Step 4 In the Command Exclude List, enter a comma-separated list of configuration commands you want to exclude for that selection. These are the parameters will ignore when checking devices for configuration changes.

Step 5 Click Save.

Control the Timeouts for Configuration Archive Operations

The Configuration Archive task uses the Device CLI Timeout value for each fetch activity. A single Configuration Archive task entails 1 to 5 files. Consequently, the overall job timeout value is determined using the following logic:Overall job timeout = Number of files*Device CLI Timeout

To configure a CLI timeout value, choose Inventory > Device Management > Network Devices, click the edit device icon, select the Telnet/SSH option, and then enter a value in the Timeout field.

Note You must increase the Device CLI timeout value if the Configuration Archive task fails due to CLI timeout.

Control How Often the Archive Summary Is Updated

When you choose Inventory > Device Management > Configuration Archive, lists the configuration archives that it has collected. This summary data is updated whenever a new archive is collected. It is also updated by default at least every 30 minutes according to a summary refresh timer. You can change the time setting by choosing Administration > Settings > System Settings, then choose Inventory > Configuration Archive and adjust the Summary refresh hold-off timeSummary refresh Hold off timer.

Control How Many Files Can Be Archived In Parallel

uses 10 thread pools for copying configuration files to the archive. A larger number may be helpful when archiving of changes involving more than 1,000 devices; however, making the number too large can negatively impact system performance. To change this number, choose Administration > Settings > System Settings, then choose Inventory > Configuration Archive and adjust the Thread Pool Count value.

Control Whether Configuration File Content Is Masked During Exports

supports exporting startup and running configuration files to a local file system. By default, the contents of these files are masked when they are exported. To export configuration files, .

Download Configuration Files

You can download the Startup and Running configuration files of up to a maximum of 1000 devices at a time, to your local system.

Step 1 Choose Inventory > Device Management > Configuration Archive.

Step 2 From the Export Latest Configdrop-down list, select one of the following options to download the configuration files:

a. Sanitized—The device credential password will be masked in the downloaded file.

b. Unsanitized—The device credential password will be visible in the downloaded file.

This option downloads all supported configuration from the device as a csv file. To specifically download only the Startup or the Running configuration from the device, use the alternate steps below.

The Unsanitized option appears based on the user permission set in Role Based Access Control (RBAC).

You can also download the configuration files by doing the following:

- Click the device for which you want to download configuration files in the Inventory > Device Management > Configuration Archive page or Click the device for which you want to download configuration files in the Inventory > Device Management > Network Devices page and click Configuration Archive tab.
- Use the expand icon to display the required configuration details from the archive.
- Click Details.
- Select Sanitized or Unsanitized from the Export drop-down list.

Remember Before you upload this config file to your WLC, you need to add a keyword, config at the beginning of each line.

Control When Device Configuration Files are Purged from the Database

Device configuration files cannot be automatically deleted from the database (you can manually delete the files); they can be periodically purged by based on your settings. Users with Administrator privileges can adjust when configuration files are purged as follows. If you do not want any configuration files purged, follow this procedure but leave both fields blank.

Step 1 Choose Administration > Settings > System Settings, then choose Inventory > Configuration Archive.

Step 2 Adjust the archiving settings depending on the following criteria.

Use this field:	To purge files when:
Max. configuration archive	The number of a device's configuration files exceeds this setting (5 by default).

Use this field:	To purge files when:
Max. days retained	A configuration file's age exceeds this setting (7 days by default).

How Do I Find Out the Last Time Files Were Archived?

Step 1 To find out the most recent date when device running configuration files were backed up to the archive, choose Inventory > Device Management > Configuration Archive and click the Devices tab. The Latest Archive column lists the archiving time stamp for each device with the most recent archive listed first. The Created By column displays the archive trigger (for example, a syslog).

Step 2 To view the contents of a device's most recently-archived running configuration file, click the time stamp hyperlink. The Running Configuration window displays the contents of the file.

Step 3 To view the changes that were made between archives for a device, see Compare or Delete Device Configuration Files, on page 79.

Back Up Device Configuration Files to the Archive

What Is Backed Up to the Database?

The configuration archive maintains copies of device configuration files, storing them in the database. Most configuration files are stored in readable format as received from the device and can be compared with earlier versions. Device configurations can be restored to earlier states using the files saved in the archive.

If the running and startup configurations on a device are the same, copies only the running configuration to the database. This is why in some cases, when you view the image repository, you will only see an archive for the running configuration.

If a configuration file has not changed since its last backup, does not archive the file. will report that the job was successful and the job result will display Already Exists.

collects and archives the following device configuration files.

Device/Device OS	What is Backed Up
Cisco IOS and Cisco IOS XE	Latest startup, running, and VLAN configuration.

Device/Device OS	What is Backed Up
Cisco IOS XR	• Latest running configuration; includes active packages. Devices must be managed with system user because copy command is not available in command-line interface (CLI) for non-system users. • Database configuration (binary file) **Note** For Cisco NCS 4000 devices, the database is backed up as a .tgz file to a file system on your local machine.

Back Up (Archive) Configuration Files

When a configuration file is backed up, fetches a copy of the configuration file from the device and copies (backs it up) to the configuration archive (database). Before saving a copy to the archive, compares the fetched file with the last version in the archive (of the same type—running with running, startup with startup). archives the file only if the two files are different. If the number of archived versions exceeds the maximum (5, by default), the oldest archive is purged.

For devices that support both running and startup configurations, identifies out-of-sync (unsynchronized) devices during the backup process by comparing the latest version of the startup configuration with the latest version of the running configuration file. For more information on out-of-sync devices, see Synchronize Running and Startup Device Configurations, on page 78.

The following table describes the supported backup methods and how they are triggered. To check or adjust the default settings, see Control How Archiving is Triggered, on page 71.

Table 12: Backup Method

Backup Method	Description	Notes
On-demand manual backup	Choose Inventory > Device Management > Configuration Archive, choose devices, and click Schedule Archive (run the job immediately or at a later time).	N/A
Regular scheduled backups	Choose Inventory > Device Management > Configuration Archive, choose devices, and click Schedule Archive . In the scheduler, specify a Recurrence.	N/A
New device backups	automatically performs backup for new devices.	Enabled by default
Event-triggered backups (device change notifications)	automatically performs backup when it receives a syslog from a managed device.	Enabled by default

View the Device Configuration Files That Are Saved in the Archive

- View All Archived Files, on page 77

• View Archived Files for a Specific Device, on page 77

View All Archived Files

To view the configuration files that are saved in the database, choose Inventory > Device Management > Configuration Archive. Click the Archives or Devices tabs depending on where you want to start:

- Archives tab—A list of configuration files that have been archived, with the most recent archives listed first. The Out of Band column indicates whether the change was made by an application other than . Use the Groups list on the left to view archives by device types and families. From here you can:
  - Roll Back a Device's Configuration To an Archived Version, on page 80
  - Overwrite a Startup Configuration with a Running Configuration, on page 80
  - Label Important Configuration Files With Tags, on page 78
- Devices tab—A flat list of devices with their archived configurations. From here you can:
  - Schedule backups to the archive (see Back Up Device Configuration Files to the Archive, on page 75).
  - View the archived file for a specific device by clicking the device name hyperlink (see View Archived Files for a Specific Device, on page 77).

By default, saves up to 5 versions of a file, and deletes any files that are older than 7 days; device configuration files cannot be manually deleted from the database. (To check the current purging settings, see Control When Device Configuration Files are Purged from the Database, on page 74.)

View Archived Files for a Specific Device

Note If you only see a running configuration file and not a startup file, that is because the two files are the same. only backs up the startup configuration when it is different from the running configuration.

Step 1 Choose Inventory > Device Management > Configuration Archive, then click the Devices tab.

Step 2 Click a device name hyperlink. lists archived files according to their timestamps.

View the Raw Content of an Archived Configuration File

Use this procedure to view the startup, running, and (if supported) VLAN, database, and admin configuration files that have been saved to the configuration archive. You can choose versions according to timestamps and then compare them with other versions.

To view the contents of a running configuration file stored in the configuration archive:

Step 1 Choose Inventory > Device Management > Configuration Archive, then click the Devices tab.

Step 2 Click a device name hyperlink. lists archived files according to their timestamps.

Step 3 Expand a timestamp to view the files that were archived at that time. You will see the details for Running Configuration, Startup Configuration, Admin Configuration, VLAN Configuration, and Database Configuration. Click the Details hyperlink under these categories, to see more information.

Note If you only see a running configuration file and not a startup file, that is because the two files are the same. only backs up the startup configuration when it is different from the running configuration.

Step 4 Click a file under Configuration Type to view its raw data. The Raw Configuration tab lists the file contents, top to bottom.

Step 5 To compare it with another file, click any of the hyperlinks under the Compare With column. The choices depend on the device type and number of configuration files that have been backed up to the archive. Color codes indicate what was updated, deleted, or added.

Label Important Configuration Files With Tags

Assigning tags to configuration files is a clear method for identifying important configurations and convey critical information. The tag is displayed with the list of files on the Configuration Archive page. Tags can also be edited and deleted using the following procedure.

Step 1 Choose Inventory > Device Management > Configuration Archive.

Step 2 Under the Archives tab, locate the configuration file you want to label, and click Edit Tag.

Step 3 Enter your content in the Edit Tag dialog box (or edit or delete existing tags) and click Save.

Synchronize Running and Startup Device Configurations

Devices that have startup configuration files and running configuration files may become out-of-sync (unsynchronized). A device is considered out-of-sync if its startup file (which is loaded when a device is restarted) is different from its running configuration. Unless a modified running configuration is also saved as the startup configuration, if the device is restarted, the modifications in the running configuration will be lost. The overwrite operation synchronizes the files by overwriting the device's startup configuration with its current running configuration.

Note This device configuration file synchronize operation is different from the Sync operation which performs an immediate inventory collection for a device.

Step 1 Identify the devices that are out-of-sync:

a) Choose Inventory > Device Management > Configuration Archive.
b) Under the Devices tab, check the Startup/Running Mismatch field .
c) If any devices list Yes, make note of the devices.

Step 2 To synchronize the devices:

a) Under the Devices tab, select the out-of-sync devices, and click Overwrite . (See Overwrite a Startup Configuration with a Running Configuration, on page 80 for more information about the overwrite operation.)

Step 3 To check the job details, choose to view details about the overwrite jobs.

Compare or Delete Device Configuration Files

The comparison feature displays two configuration files side by side with additions, deletions, and excluded values indicated by different colors. You can use this feature to view the differences between startup and running configuration files for out-of-sync devices, or to find out if similar devices are configured differently. You can then delete the configuration archives from the database.

excludes a small set of commands by default, such as the NTP clock rate (which constantly changes on a managed network element but is not considered a configuration change). You can change the excluded commands list as described in Specify Items to be Excluded When Configuration Files Are Checked for Changes, on page 73.

Step 1 Choose Inventory > Device Management > Configuration Archive.

Step 2 To delete the device configuration archive, under the Devices tab, locate the device with the configuration you want to delete and click the X delete button.

Step 3 To compare device configuration archives:

a) Under the Devices tab, locate the device with the configuration you want to compare and click its device name hyperlink.

b) Expand a time stamp to view the files that were archived at that time.

c) Launch a comparison window by clicking any of the hyperlinks under the Compare With column. The choices depend on the device type and number of configuration files that have been backed up to the archive. Color codes indicate what was updated, deleted, or added.

In the Configuration Comparison window, you can peruse the configuration by looking at the raw files or by looking at certain portions of the files (configlets). Use the color codes at the bottom window to find what was updated, deleted, or added.

Deploy an External Configuration File to a Device

The Schedule Deploy operation updates a device's configuration file with an external file. The difference between Rollback and Schedule deploy is that the Rollback uses an existing file from the archive, while Schedule Deploy uses an external file.

Depending on the type of device, you can specify the following settings for the deploy job:

- Overwrite the current startup configuration with the new version and optionally reboot the device after the deploy.
- Merge the new file with the current running configuration and optionally archive the file as the new startup configuration.

- Schedule the deploy of database configuration files in .tgz format.

Make sure you have the location of the file on your local machine.

Step 1 Open the device's Device Details page, from which you will execute the deploy operation.
a) Choose Inventory > Device Management > Network Devices.
b) Click the device name hyperlink to open the Device Details page.

Step 2 Open the device's Configuration Archive page by clicking the Configuration Archive tab.

Step 3 Click Schedule Deploy to open the deploy job dialog box.

Step 4 Choose the file you want to deploy by clicking Browse, navigating to the file's location, and choosing the file.

Step 5 Configure the job parameters, depending on the type of file you are deploying:

- Startup configuration—Choose Overwrite Startup Configuration. If you want to reboot the device after the deploy operation, check the Reboot check box.
- Running configuration—Choose Merge with Running Configuration. If you want to also save the file on the device as the startup configuration, check the Save to Startup check box.

Step 6 Schedule the deploy job to run immediately or at a future time, and click Submit.

Step 7 Choose to view details about the job.

Overwrite a Startup Configuration with a Running Configuration

The overwrite operation copies a device's running configuration to its startup configuration. If you make changes to a device's running configuration without overwriting its startup configuration, when the device restarts, your changes will be lost.

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Click the device name hyperlink to open the device's details page, then click the Configuration Archive tab.

Step 3 Click Schedule Overwrite and set the job to run immediately or at a future time, then click Submit.

Step 4 Choose

Roll Back a Device's Configuration To an Archived Version

The rollback operation copies files from the archive to devices, making the new files the current configuration. You can roll back running, startup, and VLAN configurations. By default, the operation is performed by merging the files. If you are rolling back a running configuration, you have the option to perform it using overwrite rather than merge. To roll back a configuration file to a previous version.

Step 1 Choose Inventory > Device Management > Configuration Archive.

Step 2 Click the Archives tab and check the device that has the configuration file you want to roll back, and click Rollback .

Step 3 Choose the file types you want to roll back. In the Schedule Configuration Rollback dialog box:

a) Expand the Rollback Options area.

b) From the Files to Rollback drop-down list, choose the file type. Choosing All applies the operation to startup, running, and VLAN configuration files.

Note For Cisco IOS XR 64-bit devices, if you select Admin Configuration, enter the Device VM Admin Password.

Step 4 Click the specific configuration file version that you want to roll back to.

Step 5 Click Schedule Rollback and complete the following:

Table 13: Roll Back Device Configuration

Area	Option	Description
Rollback	Files to rollback	Select Database Configuration, Running Configuration, or Admin Configuration.
	Reboot	(Startup only) After rolling back the startup configuration, reboot the device so the startup configuration becomes the running configuration.
	Save to startup	(Running only) After rolling back the running configuration, save it to the startup configuration.
	Archive before rollback	Back up the selected file(s) before beginning the rollback operation.
	Overwrite configurations	Overwrite (rather than merge) the old running configuration with the new one.
	Continue rollback on archive failure	(If Archive before rollback is selected) Continue the rollback even if the selected files are not successfully backed up to the database.
	VRF Name	Select the applicable VRF name from the drop down list. The VRF name is validated on submission.
Schedule	(see web GUI)	Specify whether to perform the rollback immediately or at a later scheduled time.

Step 6 Click Submit.

Download Configuration Files

You can download the Startup and Running configuration files of up to a maximum of 1000 devices at a time, to your local system.

Step 1 Choose Inventory > Device Management > Configuration Archive.

Step 2 From the Export Latest Configdrop-down list, select one of the following options to download the configuration files:

a. Sanitized—The device credential password will be masked in the downloaded file.

b. Unsanitized—The device credential password will be visible in the downloaded file.

This option downloads all supported configuration from the device as a csv file. To specifically download only the Startup or the Running configuration from the device, use the alternate steps below.

The Unsanitized option appears based on the user permission set in Role Based Access Control (RBAC).

You can also download the configuration files by doing the following:

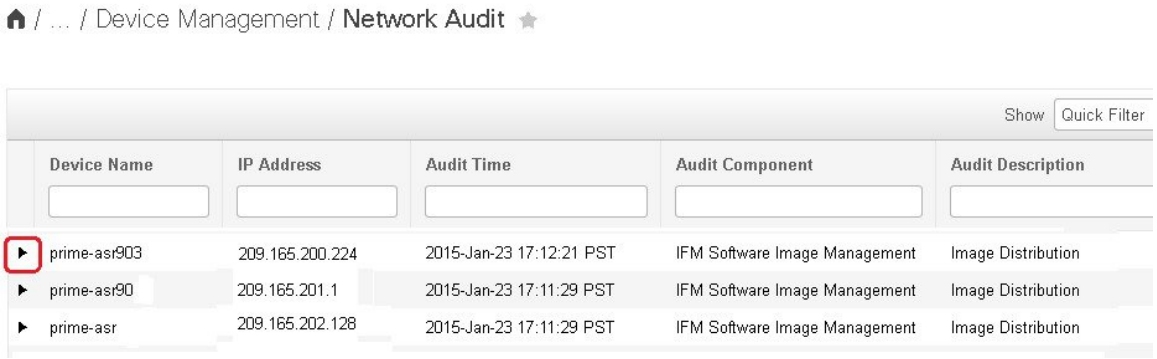
- Click the device for which you want to download configuration files in the Inventory > Device Management > Configuration Archive page or Click the device for which you want to download configuration files in the Inventory > Device Management > Network Devices page and click Configuration Archive tab.
- Use the expand icon to display the required configuration details from the archive.
- Click Details.
- Select Sanitized or Unsanitized from the Export drop-down list.

Remember Before you upload this config file to your WLC, you need to add a keyword, config at the beginning of each line.

Check the Network Audit for Configuration Archive Operations

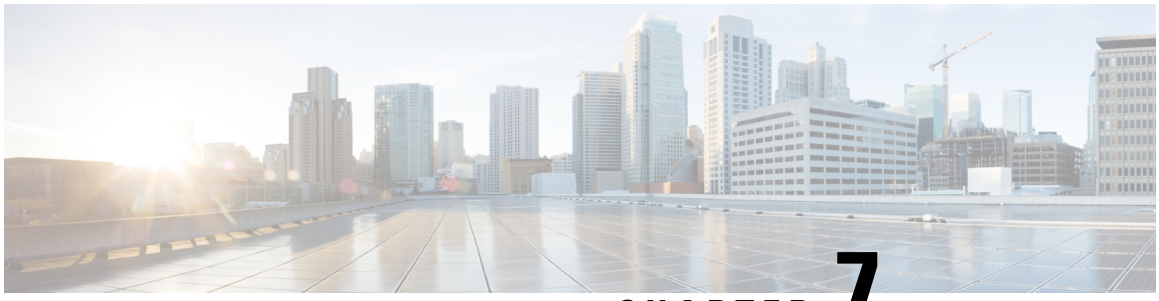
To get historical information about device software image changes, check the Network Audit.

Step 1 Choose Inventory > Device Management > Network Audit. To filter the results to show only image management operations, enter archive in the Audit Component field.



Step 2 Expand an event drawer to get details about a device change. For example, if you expand the drawer highlighted in the above figure, given in step 1, you can see that the device's running configuration file was successfully backed up to the archive at that time.

Archive configuration	**Success**
Fetch DATABASE configuration	Unsupported operation
Fetch VLAN configuration	Unsupported operation
Fetch running configuration	Success
Fetch startup configuration	Success
Syslog Message	<189>308716: *Jan 27 01:25:41.622: %SYS-5-CONFIG_I: Configured from console by vty0 (10.127.101.52)



CHAPTER 7

Manage Device Software Images

Set Up Software Image Management

Make Sure Devices Are Configured Correctly

can transfer files to and from devices only if the SNMP read-write community strings configured on your devices match the strings that were specified when the devices were added to .

Note To improve security, no longer uses some of the SSH CBC (Cipher Block Chaining) ciphers that older Cisco IOS-XE and IOS-XR versions use, as they have been deemed weak. For devices running Cisco IOS-XE, ensure that you upgrade to version 16.5.x or later. And for devices running Cisco IOS-XR, upgrade to version 6.1.2 or later. Otherwise, several Software Image Management operations will fail.

Verify the FTP/TFTP/SFTP/SCP Settings on the Server

If you will be using FTP, TFTP, SFTP, or SCP make sure that it is enabled and properly configured.

How to Control Images that are Saved to the Image Repository During Inventory Collection

Because collecting software images can slow the data collection process, by default, does not collect and store device software images in the image repository when it performs inventory collection. Users with Administration privileges can change that setting using the following procedure.

Step 1 Choose Administration > Settings > System Settings, then choose Inventory.

Step 2 To retrieve and store device images in the image repository when performs inventory collection, check the Collect images along with inventory collection check box.

Step 3 Click Save.

Software Image Management Processes and Supported Devices

The following table describes the different processes involved in managing software images and whether the processes are supported in the Unified Wireless LAN Controllers and devices.

Note Refer the Supported Device List for additional information on Platforms such as Protocols supported during Image Import, Image Distribution via Local File Server, Software Image Management Server and Support for TFTP FallBack, or ISSU and Activation without Distribution.

Table 14: Software Image Management Processes and Supported Devices

Software Image Management Processes	Description	Unified WLCs	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2
Image import from device	Ability to import software image from devices that are already managed by . The software image can then be distributed to other devices.	Not supported because the software image cannot be reassembled into a package.	Supported **Note** When the device is running in install mode, the running image will be "packages.conf". does not support importing of image in this format in the install mode.	Supported **Note** When the device is running in install mode, the running image will be "packages.conf". Prime Infrastructure does not support importing of image in this format in the install mode.
Image import from file	Ability to import software image from known location on a file server to . The software image can then be distributed to other devices.	Supported	Supported	Supported
Image import from URL	Ability to import software image from network accessible locations (URI/URL) to . The software image can then be distributed to other devices.	Supported	Supported	Supported
Import Image using Protocol	Ability to import software image from an FTP location to . The software image can then be distributed to other devices.	Supported	Supported	Supported
Image upgrade/distribution	Ability to upgrade software image on the managed devices from. This allows you to upgrade the software image for multiple devices based on demand or at a later point in time as scheduled. The feedback and status are displayed during the upgrade and devices can be restarted, if required. In large deployments, you can stagger reboots so that the service at a site is not completely down during the upgrade window.	Supported	Supported	Supported

Software Image Management Processes	Description	Unified WLCs	3850 Cisco IOS XE 3.2.2	5760 Cisco IOS XE 3.2.2
Image recommendation	Ability to recommend a compatible image for the devices that are managed from and downloaded from Cisco.com.	Not supported because the flash requirement is not available.	Supported	Supported
Image upgrade analysis	Ability to analyze the software images to determine the hardware upgrades required before you can perform the software upgrade.	Not supported because there is no minimum requirement for RAM or ROM. The newly upgraded image replaces the existing image after an upgrade.	Supported	Supported

Adjust Criteria for Cisco.com Image Recommendations

You can use Cisco.com to get information about recommended images based on criteria you provide. The following procedure shows how you can adjust those recommendations. The following table also lists the default settings.

Note To use these features, the device must support image recommendations.

Step 1 Choose Administration > Settings > System Settings, then choose .

Step 2 Adjust the recommendation settings as follows.

Setting	Description	Default
Recommend latest maintenance version of each major release	Only considers images if it is the latest maintenance version of each major release	Disabled
Recommend same image feature	Only considers images with same feature set as running device image	Disabled
Recommend versions higher than the current version	Only considers images that are higher than the running device image	Disabled
Include CCO for recommendation	Retrieves images from Cisco.com and the image repository	Enabled

Step 3 Click Save.

Adjust Image Transfer and Distribution Preferences

Use this procedure to specify the default protocols should use when transferring images from the software image management server to devices. You can also configure to perform, by default, a variety of tasks associated with image transfers and distributions—for example, whether to back up the current image before an upgrade, reboot the device after the upgrade, continue to the next device if a serial upgrade fails, and so forth. Users with Administration privileges can change that setting using the following procedure.

This procedure only sets the defaults. You can override these defaults when you perform the actual distribute operation.

Step 1 Choose Administration > Settings > System Settings, then choose Inventory.

Step 2 On the Basic tab, specify the tasks that should perform when distributing images:

Setting	Description	Default
Job Preferences		
Continue distribution on failure	If distributing images to multiple devices and distribution to a device fails, continues the distribution to other devices	Enabled
TFTP fallback	Inserts the TFTP fallback command into the running image so that it can be reloaded if image distribution fails	Disabled
Backup running image		Disabled
Insert boot command	Inserts the boot command into the running image, after image distribution	Disabled
Smart Flash Delete Before Distribution	Delete the unnecessary files from flash to free up the memory space before distribution	Disabled
Other Preferences		
Collect images along with inventory collection	Choose this option if you want the software image to be collected from the device and store in the image repository during inventory collection.	Disabled
Show latest images for the available major releases	Choose this option if you want to view the latest maintenance release.	Disabled
Show images with same feature support	Choose this option if you want to view the available images with the same features supported by the running image.	Disabled
Show available higher image versions	Choose this option if you want to view the available higher image versions for the running image.	Disabled
Remove the option to activate software during distribution jobs	Choose this option to remove the option to activate the software during distribution jobs.	Disabled

Setting	Description	Default
Copy operation to be initiated by the EPN Manager server	Choose this option if you want the copy operation to be initiated by the EPN Manager server.	Disabled

Step 3 Specify the default protocol should use when transferring images in the Image Transfer Protocol Order. Arrange the protocols in order of preference. If the first protocol listed fails, will use the next protocol in the list.

Note When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP for the image distribution, ensure that the device is managed in with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

Step 4 Click Save.

Add a Software Image Management Server to Manage Groups of Devices

To distribute images to a group of devices, add a software image management server and specify the protocol it should use for image distribution. You can add a maximum of three servers.

Step 1 Add the server.

a) Choose Administration > Servers > Software Image Management Servers.
b) Click the Add Row icon and enter the server name, IP address, and device group the server will support.
c) Click Save.

Step 2 Configure the server protocol settings.

a) Check the check box next to the server name, then click Manage Protocols.
b) Click the Add Row icon and enter the software image management protocol details (username, password, and so forth).
c) Click Save.

Change Cisco.com Credentials for Software Image Operations

When connects to Cisco.com to perform software image management operations (for example, to check image recommendations), it uses the credentials stored in the Account Settings page. You can change those settings using the following procedure.

Step 1 Choose Administration > Settings > System Settings, then choose General > Account Settings.

Step 2 Click the Cisco.com Credentials tab.

Step 3 Change the settings, then click Save.

Copy Software Images from Devices to the Image Repository (Create a Baseline)

Depending on your system settings, may copy device software images to the image repository during inventory collection (see How to Control Images that are Saved to the Image Repository During Inventory Collection, on page 86). If you need to perform this operation manually, use the following procedure, which imports software images directly from devices into the image repository.

Before you begin, ensure that images are physically present on the devices (rather than remotely loaded).

Note If you are importing many images, perform this operation at a time that is least likely to impact production.

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click the Add/Import icon.

Step 3 Click Submit.

How Do I Find Out Which Images Are Used by Network Devices?

To view a list of the images used by network devices, choose Reports > Reports Launch Pad > Device > Detailed Software.

To list the top ten images use by network devices (and how many devices are using those images), choose Inventory > Device Management > Software Images. Click Software Image Repository under Useful Links, then then click the Image Dashboard icon in the top-right corner of the page.

How Do I Know a Device Has the Latest Image?

If your device type supports image recommendations, you can use the following procedure to check if a device has the latest image from Cisco.com. Otherwise, use the Cisco.com product support pages to get this information.

Step 1 Choose Inventory > Device Management > Network Devices, then click the device name hyperlink to open the Device Details page.

Step 2 Click the Software Image tab and scroll down to the Recommended Images area. lists all of the images from Cisco.com that are recommended for the device.

How Do I Know Whether I have Permission to Download Software from Cisco.com

and it allows you to download the software images directly from Cisco.com. In order to download a EULA or K9 software image from Cisco.com, you must accept/renew the EULA agreement or K9 Agreement periodically.

does not display deferred software images. For detailed information, see Cisco Prime Infrastructure 3.2 Supported Devices list.

If you encounter any error message while importing software image from Cisco.com, see ASD Exceptions and Error Conditions, on page 103.

View the Images That Are Saved in the Image Repository

Use this procedure to list all of the software images saved in the image repository. The images are organized by image type and stored in the corresponding software image group folder.

Step 1 Choose Inventory > Device Management > Software Images. lists the images that are saved in the image repository within the Software Image Summary panel.

- Import new images into the image repository from network devices; file systems on client machines, IPv4 or IPv6 servers (URLs), FTP servers, and Cisco.com. See Add (Import) Software Images to the Repository, on page 94.
- Adjust the requirements that a device must meet in order to upgrade to this image. See Change the Device Requirements for Upgrading a Software Image, on page 97.
- Perform an upgrade analysis. See Verify That Devices Meet Image Requirements (Upgrade Analysis), on page 97.
- Copy new software images to devices. .
- Activate images, which makes a new image the device's running image. See Activate a New Software Image on Devices, on page 100.
- Commit Cisco IOS XR images, which persists the image across device reloads and creates a rollback point. See Commit Cisco IOS XR Images Across Device Reloads, on page 102.

Step 2 Go to Software Image repository and click a software image hyperlink to open the Image Information page that lists the file and image name, family, version, file size, and so forth.

From here you can:

- See which devices are using this image by checking the Device Details area at the bottom of the page.
- Adjust the requirements that a device must meet in order to upgrade to this image. (See Change the Device Requirements for Upgrading a Software Image, on page 97.)

Find Out Which Devices Are Using an Image

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 In the Software Image Summary panel, locate the image that you are interested in by expanding the image categories in the navigation area or entering partial text in one of the Quick Filter fields. For example, entering 3.1 in the Version field would list Versions 3.12.02S, 3.13.01S, and so forth.

View Recommended Images on Cisco.com

If your devices support Cisco.com image recommendations, you can use this procedure to check which images your devices should be using.

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click Software Image Repository under Useful Links.

Step 3 Choose one of the following image sources:

- Select Image from Local Repository to select an image stored locally. Then, under Local Repository:

Step 4 Select the image to distribute, then click Apply.

Step 5 Choose the image name in the Distribute Image Name field to change your selection and pick a new image, then click Save.

Download Images from Cisco.com

Depending on your device type, (see Adjust Criteria for Cisco.com Image Recommendations, on page 88).

will use the Cisco.com credentials that are set by the administrator. If default credentials are not set, you must enter valid credentials. (See Change Cisco.com Credentials for Software Image Operations, on page 90).

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click the Add/Import icon.

Step 3 In the Import Images dialog:

a) Click Cisco.com.

b) If the credentials are not auto-populated, enter a valid Cisco.com user name and password.

c) Click Login.

Step 4 Click Device Selection tab.

Step 5 You can click the Select devices by toggle button to choose devices from Group or Device option. You can select maximum 20 devices.

Step 6 If you choose Group option, select the Device groups and select the devices listed under Choose Devices pane. The selected devices are listed under the Selected Devices pane.

Step 7 Click Image Selection tab.

Step 8 Select images and click the Schedule tab.

Step 9 Click Submit.

Step 10 Verify that the images are listed on the Software Images page. (Click the Software Image Repository Link in the Useful Links section.)

Add (Import) Software Images to the Repository

displays the recommended latest software images for the device type you specify, and it allows you to download the software images directly from cisco.com. does not display deferred software images. For detailed information, see list.

Note In order to download a K9 software image from cisco.com, you must accept/renew the https://software.cisco.com/download/eula.html K9 agreement periodically.

The following topics explain the different ways you can add software images to the image repository. For an example of how to troubleshoot a failed import, see Manage Jobs Using the Jobs Dashboard, on page 19.

- Add a Software Image That Is Running on a Managed Device, on page 94
- Add a Software Image from an IPv4 or IPv6 Server (URL), on page 95
- Add a Software Image for an FTP Protocol Server (Protocol), on page 95
- Add a Software Image from a Client Machine File System, on page 96

Add a Software Image That Is Running on a Managed Device

This method retrieves a software image from a managed device and saves it in the image repository.

Note When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP for the image distribution, ensure that the device is managed in with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

Note that TFTP is supported only when copying images from the device to the server and not the other way around.

Limitations:

- For Cisco IOS-XR devices, direct import of images from the device is not supported by ; SMU and PIE imports are also not supported on these devices.

- For Cisco IOS-XE devices, if the device is loaded with the 'packages.conf' file, then images cannot be imported directly from that device.

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click the Add/Import icon.

Step 3 To view the status of the job, click the job link in the pop-up message or choose Administration > Job Dashboard.

Step 4 Verify that the image is listed on the Software Images page (Inventory > Device Management > Software Images).

Add a Software Image from an IPv4 or IPv6 Server (URL)

You can import software image from network-accessible IPv4 or IPv6 servers.

supports to import Non-Cisco standard image.

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click the Add/Import icon.

Step 3 In the Import Images dialog:

a) Click URL.

b) In the URL To Collect Image field, enter a URL in the following format (you can also use an HTTP URL where user credentials are not required):

http://username:password@server-ip/filename

c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.

d) Click Submit.

Step 4 To view the status of the job, click the job link in the pop-up message or choose Administration > Job Dashboard.

Step 5 Verify that the image is listed on the Software Images page (Inventory > Device Management > Software Images).

Add a Software Image for an FTP Protocol Server (Protocol)

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click the Add/Import icon.

Step 3 In the Import Images dialog:

a) Click Protocol.

b) Enter FTP in the Protocol field, then enter the FTP user name, password, server name or IP address, and file name. The following is a file name example:

/ftpfolder/asr901-universalk9-mz.154-3.S4.bin

c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.

d) Click Submit.

Step 4 To view the status of the job, click the job link in the pop-up message or choose Administration > Job Dashboard.

Step 5 Verify that the image is listed on the Software Images page (Inventory > Device Management > Software Images).

Add a Software Image from a Client Machine File System

Before you begin

When you import the software image file, the browser session is blocked temporarily. If the upload operation exceeds the idle timeout limit of the browser session, then you will be logged out of and the file import operation will be aborted. So it is recommended that you increase the idle timeout limit before you begin with this import operation. To increase the idle timeout, see Cisco Prime Infrastructure Administrator Guide.

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click the Add/Import icon.

Step 3 In the Import Images dialog:

a) Click File.

b) Click the Browse button and navigate to the software image file.

c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.

d) Click Submit.

Note You must use the URL or Protocol options to import files of larger size (say, greater than 200 MB), as importing through the File option is not recommended.

Step 4 To view the status of the job, click the job link in the pop-up message or choose Administration > Job Dashboard.

Step 5 Verify that the image is listed on the Software Images page (Inventory > Device Management > Software Images).

Import Software Images to the Virtual Image Repository

You can use the Virtual Image Repository (VIR) to automatically retrieve and store device images from specified URLs or files. You can schedule these downloads to occur regularly.

Currently, the VIR supports FTP or HTTP downloads only.

To import software images to the VIR:

Step 1 Choose Inventory > Device Management > Virtual Image Repository. The page lists the number of images currently retained in the repository.

Step 2 Click Import.

Step 3 Specify the Source from which to import the software image. You can specify one of the following sources:

- URL—Specify the FTP or HTTP URL from which to import the software image. You can use an HTTP URL where user credentials are not required.
- File—A local file on the client machine.

Step 4 Click Collection Options and then enter the required information.

Step 5 Click Schedule and specify the schedule on which to import image file. You can run the collection job immediately or schedule it to run at a later time. You can also schedule the job to recur automatically

Step 6 Click Submit.

Step 7 Choose Administration > Dashboards > Job Dashboard > User Jobs > Software Image Import to view the status about the image collection job. The Duration field is updated after the job completes.

Related Topics

Add (Import) Software Images to the Repository, on page 94
Distribute a New Software Image to Devices, on page 98

Change the Device Requirements for Upgrading a Software Image

Use this procedure to change the RAM, flash, and boot ROM requirements that a device must meet for a software image to be distributed to the device. These values are checked when you perform an upgrade analysis (see Verify That Devices Meet Image Requirements (Upgrade Analysis), on page 97).

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 In the Software Image Summary panel, locate and select the software image by clicking its associated hyperlink.

Step 3 Click the software image name hyperlink to open its image information.

Step 4 Adjust the device requirements:

- Minimum RAM (from 1 – 999999999999999)
- Minimum FLASH (from 1 – 999999999999999)
- Minimum Boot ROM Version

Step 5 Click Save.

Step 6 Click Restore Defaults, if you want to retain the previous requirements.

Verify That Devices Meet Image Requirements (Upgrade Analysis)

An upgrade analysis verifies that the device , the image is compatible with the device family, and the software version is compatible with the image version running on the device. After the analysis, displays a report that provides the results by device. The report data is gathered from:

- The software image repository, which contains information about minimum RAM, minimum Flash, and so on, in the image header.

- The inventory, which contains information about the active images on the device, as well as Flash memory, modules, and processor details.

Note Upgrade analysis is supported on all Cisco IOS-XR devices (such as Cisco NCS 1000, Cisco NCS 4000, Cisco NCS 5000, Cisco NCS 5500, and Cisco NCS 6000), except on Cisco ASR 9000 devices.

If you want to adjust the device requirements for an image, see Change the Device Requirements for Upgrading a Software Image, on page 97.

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click under Useful Links. (Do not select an image from the Software Images page.)

Distribute a New Software Image to Devices

You can distribute a software image to a device or set of similar devices in a single deployment. Prime Infrastructure verifies that the device and software image are compatible.

Based on a device's capabilities, Prime Infrastructure can use different transport protocols (SCP, TFTP, FTP, SFTP) to distribute images to devices. For better reliability and security, we recommend you to use secure protocols only (SFTP, SCP) for distributing software images. If you choose SCP protocol for the image distribution, ensure that the device is managed in Prime Infrastructure with full user privilege (Privileged EXEC mode), otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

We do not recommend using TFTP or FTP. If you choose TFTP protocol for the image distribution and if the device and the server are in different subnet, the image should be copied within the specified session time limit (one hour) which is maintained by the application otherwise the distribution will fail due to timeout error.

For Software Image Distribution to work efficiently, the device and server from which the distribution is performed must be in the same geographical location or site. If you want to distribute software images into different geographical location of Prime Infrastructure and device, create location group and map this location into Software Image Management server. This external server will transfer images from Prime Infrastructure to Software Image Management server and then start distributing to mapped device location. The Software Distribution job would return error if the distribution takes more time due to network slowness or low speed.

Note To ensure that there are no SNMP views blocking access to the CISCO-FLASH-MIB, remove the following command from the configuration for all routers and switches (if present) on which you want to download a software image:

```
snmp-server view ViewName ciscoFlashMIB excluded
```

Step 1 Choose Inventory > Device Management > Software Images

Step 2 Click Distribute in the Software Image Management Lifecyle widget.

Step 3 In the Image Selection window, choose the software images that you want to distribute.

Step 4 Click the Device Selection tab, to choose the devices that you want to distribute the image.

a) You can click the Select devices by toggle button to choose devices from Group or Device option.
b) If you choose Group option, select the Device group and select the devices listed under Choose Devices pane. The selected devices are listed under the Selected Devices pane.

By default, the devices for which the selected image is applicable are shown.

Step 5 Click the Image Details Verification tab and click the image row to do the following:

- Choose the image name in the Distribute Image Name field to change your selection and pick a new image, then click Save.
- Choose the value displayed in the Distribute Location field, select a new location in which to store the software image, then click Save.
- Choose the value displayed in the Software Image Management Server field, then click Save. You can choose either a Local file server or one of the servers created under Administration > Servers > Software Image Management Servers.

The Status and Status Message fields display the validity of the selections you made. For example, if the status is green, there is adequate space available to store the image on the specified location on the device.

Step 6 Click the Image Deployment tab and set the image deployment options as required:

- Backup Current Image—Before distributing new images, import the running images from the device to software images repository page.
- Insert boot command—To set the boot variable in the device boot path list.
- Activate—To enable the Activate option, you must check the Insert Boot Command check box.
  - Activate OFF—New image will be distributed and boot variable is set in device boot path list. Device will not be rebooted in this mode and will continue to run with the running image.
  - Activate Sequential—Once the image distribution is completed for all the selected devices, the devices will reboot sequentially.
  - Activate Parallel— Once the image distribution is completed for all the selected devices, the devices will reboot simultaneously.
- Smart Flash Delete Before Distribution—Clears the flash memory before image distribution if there is no sufficient space in the device.
- Continue on Failure—If the image distribution fails for one image, the next device in queue will be picked up for activation.
- TFTP Fallback—It prompts the device to reload the current running image from the TFTP server location during image distribution failure.

Step 7 Prime infrastructure allows you to use a maximum of one Local file server and three Software Image Management Servers for software image distribution. Each server can distribute the image to five devices at one instance. When the image distribution is completed for one device, the next subsequent device will be taken up for the image distribution.Click the Schedule Distribution tab and specify the schedule options, then click Submit.

The details about the image distribution job is displayed in the Software Image Management dashboard. You can also view the image distribution job details from Administration > Dashboards > Job Dashboard > User Jobs > Software Image Distribution. The Duration field is updated after the job completes.

Note Submit button will be enabled only after you select Now or Date for each Activation jobs

Activate a New Software Image on Devices

When a new image is activated on a device, it becomes the running image on the disk. Deactivated images are not removed when a new image is activated; you must manually delete the image from the device.

If you want to distribute and activate an image in the same job, see .

To activate an image without distributing a new image to a device — for example, when the device has the image you want to activate—use the following procedure. The activation uses the distribution operation but does not distribute a new image.

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click the Activate icon in the Software Image Management Lifecycle widget.

Step 3 In the Activation Source tab, choose Activate from Library or Activate from Completed Distribution Jobs.

Step 4 In the Activate Job Options window, choose the required settings and go to Step 10:

- Activate Options: Off, Sequential or Parallel
- Continue on failure: Continue the activation even if it fails on a device.
- Commit: Commit the image on the device post distribution.

Step 5 If you choose Activate from Library in the Activation Source tab, then click the Image Selection tab.

Step 6 In the Image Selection tab, choose the software images that you want to distribute.

Step 7 Click the Activate Job Options tab, and choose the required Activate Job options.

If you choose the ISSU option from the Activate drop-down list, the software image in the device will get upgraded without need for rebooting the device.

Step 8 Click Submit to activate the software image in the selected devices.

Deploy Software Images to Wireless/DC Devices

You can view the Device Upgrade Mode option only during image upgrade for Cisco 5760 Series Wireless Controller and Cisco Catalyst 3850 Ethernet Stackable Switch. The following table describes the possible device upgrade options and the corresponding image format for Cisco 5760 Series Wireless Controller and Cisco Catalyst 3850 Ethernet Stackable Switch.

Table 15: Upgrade/ Downgrade Mode Options

Device Upgrade Mode	Device Image Format Before Distribution	Device Image Format After Distribution
Change Install mode to Bundle mode	packages.conf	.bin
Change Install mode to Currently Existing mode	packages.conf	packages.conf
Change Bundle mode to Currently Existing mode	.bin	.bin
Change Bundle mode to Install mode	.bin	packages.conf

If the image distribution status is “Success”, you can check the new image version using any of the following options:

- ChooseInventory > Network Devices.
  - View the Software Version column in the Network Devices page.
  - Click the device name and click the Image tab.
- Use the show versioncommand in the device CLI.

Related Topics

Activate a New Software Image on Devices, on page 100

Supported Image Format for Stack Devices

Prime Infrastructure supports only .tar images for upgrade and downgrade for stacked devices. Stack device do not support.bin format. The list of supported stack devices are:

- Stack of CBS3100 switch modules
- Cisco Catalyst Switch Module 3110X for IBM Blade Center
- Cisco Catalyst Blade Switch 3120X for HP
- Cisco Catalyst Blade Switch 3130X for Dell M1000E
- Cisco Catalyst 2975 Switch
- Cisco 3750 Stackable Switches
- Cisco Catalyst 29xx Stack-able Ethernet Switch
- Cisco ME 3600X-24FS-M Switch
- Cisco ME 3600X-24TS-M Switch
- Cisco ME 3800X-24FS-M Switch Router

Note Cisco Catalyst 3650 and 3850 switches do not have.tar images on Cisco.com. For these switches, Prime Infrastructure supports .bin format.

Commit Cisco IOS XR Images Across Device Reloads

Note For Cisco IOS XR devices, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate.

When you commit a Cisco IOS XR package to a device, it persists the package configuration across device reloads. The commit operation also creates a rollback point on the device which can be used for roll back operations.

If you want to distribute, activate, and commit an image in the same job, use the procedure described in .

To commit an activated image, use the following procedure.

Note If you are only working on a single device, perform the commit operation from the Device Details page (click the Image tab, choose the image, and click Commit).

Step 1 Choose Inventory > Device Management > Software Images.

Step 2 Click the Commit icon in the Software Image Management Lifecycle widget.

Step 3 Select the devices with the image you want to commit and click Submit. (Images can only be committed if they have been activated.)

Step 4 Select the software image you want to activate, then click Submit.

Step 5 In the Schedule Distribution area, schedule the commit job to run immediately, at a later time, or on a regular basis.

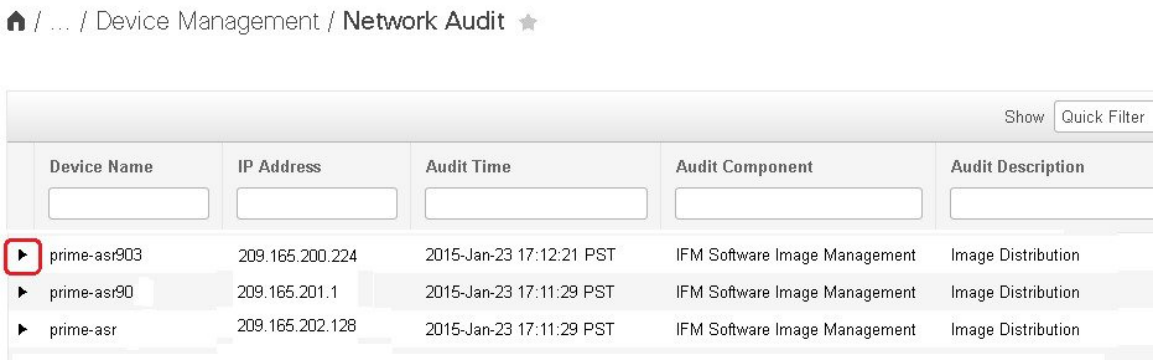
Step 6 Click Submit.

Step 7 Choose Administration > Job Dashboard to view details about the image activation job.

Check the Network Audit for Software Image Operations

To get historical information about device software image changes, check the Network Audit.

Step 1 Choose Inventory > Device Management > Network Audit. To filter the results to show only image management operations, enter software image in the Audit Component field.



Step 2 Expand an event drawer to get details about a device change. For example, if you expand the drawer highlighted in the above figure, you can see that the image listed in the job was successfully distributed to the device.

Device/Module ID	544544
Distribution Option : ActivatePatches	Yes
Distribution Option : BackUpCurrentImageFetch	No
Distribution Option : CfgXferProtocolOrder	TELNET, SSH
Distribution Option : Commit	No
Distribution Option : DeviceUpgradeMode	currentlyExists
Distribution Option : HaltUponError	No
Distribution Option : ISSUUpgrade	No
Distribution Option : ImgXferProtocolOrder	SCP,SFTP,FTP,TFTP
Distribution Option : InsertBootCommand	No
Distribution Option : JobDirectory	/opt/CSCOlumos/conf/ifm/swim/jobs
Distribution Option : RebootImmediately	No
Distribution Option : RebootMode	Sequential
Distribution Option : SCPDirectory	/localdisk/sftp
Distribution Option : SkipDistribution	No
Distribution Option : TftpDirectory	/localdisk/sftp
Distribution Option : TftpFallback	No
Distribution Option : UpgradeMode	Sequential
Distribution Option : UseSSH	Yes
Operation	Starting distribution of image to device
Running Image File Name	asr903rsp1-universalk9_npe.03.13.00.S.154-3.S-ext.bin
Running Image File Name	asr903rsp1-universalk9_npe.03.13.00.S.154-3.S-ext.bin

ASD Exceptions and Error Conditions

Cisco Prime Infrastructure uses the Cisco Automated Software Distribution (ASD) service to provide software information and download URLs to assist you in upgrading your device/application to the latest version.

The table describes the ASD exceptions and error conditions returned by ASD API in Prime Infrastructure while importing the software image from cisco.com.

Table 16: ASD Exceptions and Error Conditions

Error Code	Error Description
PID_INVALID	PID provided in the request is invalid. Please invoke the service with the valid PID.

Error Code	Error Description
IMG_NM_INVALID	Image_name provided is invalid. Please provide the valid image_name.
SWTID_INVALID	Software_type_id provided is invalid. Please provide a valid software_type_id.
INVALID_INPUT	Invalid input or No data found for the input provided.
INVALID_MTRANSID	Invalid metadata_trans_id.
INVALID_DWLDSID	Invalid download_session_id.
INVALID_DRETRYID	Invalid download_retry_id.
IMAGE_GUID_INVALID	The image_guid provided in the request is invalid. Please provide a valid image_guid.
PID_MISSING	PID is missing in the request. Please provide a valid PIDin the request.
CUR_REL_MISSING	Current_release is missing in the request. Please provide a valid current_release in the request.
OUT_REL_MISSING	Output_release is missing in the request. Please provide a valid output_release in the request.
IMG_NM_MISSING	Image_names is missing in the request. Please provide at least one valid image_names.
MISSING_DW_RETRY_ID	Download_retry_id is missing in the request. Please provide a valid download_retry_id in the request.
MTRANSID_MISSING	Metadata_trans_id is missing in the request. Please provide a valid metadata_trans_id in the request.
IMAGE_LIMIT_EXCEEDED	The number of image names entered in the request has exceeded the limit.
DRETRYID_EXPIRED	You were previously granted a download_retry_id that has expired
DWLDSID_EXPIRED	You were previously granted a download_session_id that has expired. \nPlease initiate the download service without the download_session_id.
MTRANSID_EXPIRED	Metadata_trans_id had been previously granted that has expired due to time limit on its validity. Please invoke the metadata service and initiate the download.
NO_DATA_FOUND	No Data Found.
IMAGE_GUID_MISSING	Image_guid is missing in the request. Please provide a valid image_guid in the request.
TIMEOUT	10000
CART_EMPTY	There are no items in the cart.
DWLD_WARN	You are receiving this warning message because our records indicates that you may not be authorized to download for the following product(s)

Error Code	Error Description
DWLD_WARN1	If you feel this message is in error, please: Email technical support <mailto:ent-dl@cisco.com> for 24x7 assistance. To expedite your request, please include the following information: User ID (Cisco.com ID used to download software) \Contact Name \Company Name \Contract Number \Product ID \Desired Software Release or File Name Please include the above message in your email. \Contact your Cisco representative, Partner or Reseller to ensure product(s) listed above are covered on a service contract that is associated to your Cisco.com profile. The Partner Locator link may assist in locating your nearest partner. You can add the service contracts for these products to your profile using the Cisco Profile Manager, or have your service administrator do this for you.
DWLD_WARN2	Please follow one of the options below to ensure that you are fully covered for service in the future and that your Cisco.com profile is accurate and up-to-date: Contact your Cisco representative, partner or reseller to ensure the products listed above are covered on a service contract that is associated with your Cisco.com profile. The Partner Locator link may assist in locating the nearest partner. You can add the service contracts for these products to your profile using the Cisco Profile Manager, or have your service access administrator do this for you. Your prompt attention to take action per this notice is appreciated in order to avoid unnecessary interruptions or delays in the process of downloading software.
K9_FORM_AR	K9 form have not been accepted or rejected to continue download.
EULA_FORM_AR	Eula form have not been accepted or rejected to continue download.
K9_FORM_ACC	K9 form have not been accepted to continue download.
EULA_FORM_ACC	EULA form have not been accepted to continue download.
K9_EULA_FORM_AR	Both Eula and k9 form have not been accepted or rejected to continue download.
SER_UNEXPECT_FAIL	Service has encountered an unexpected failure. Please contact the support with the data requested.

Upgrade Controller Software using Rolling AP Upgrade

You can upgrade APs and Controller software versions from Prime Infrastructure using Rolling AP Upgrade feature. You can add APs to an upgrade group and prevent all Access Points from rebooting simultanously. AP Upgrade groups will reboot sequentially in the order of your preference.

To enable Rolling AP Upgrade, follow the below procedure:

Before you begin

1. N+1 controller should be upgraded to new version.
2. Primary controller should be configured to boot from primary image.
3. Prime Infrastructure should be added as a trap receiver and AP register trap control should be enabled on both controllers.
4. N+1 controller should have the following configurations same as the primary controller:
   - WLANs

- AP Groups
- Mobility Groups
- RF Groups
- RF Profiles

Step 1 Click Configure and then click Network Devices under Network.

Step 2 Select the APs that you want to add to a group by clicking the corresponding checkboxes.

Step 3 Click Groups and Sites and then click Add to Group.

Step 4 Select the group that you want to add you APs to and then click Add.

The recommendation is to not have more than 10 groups per controller and 1000 APs per group. Now that you have added APs to a group, you need to intiailize the upgrade process.

Step 5 Click Configuration and then click Rolling AP Upgrade under Wireless Technologies.

Step 6 Select the Primary and the N+1 controllers.

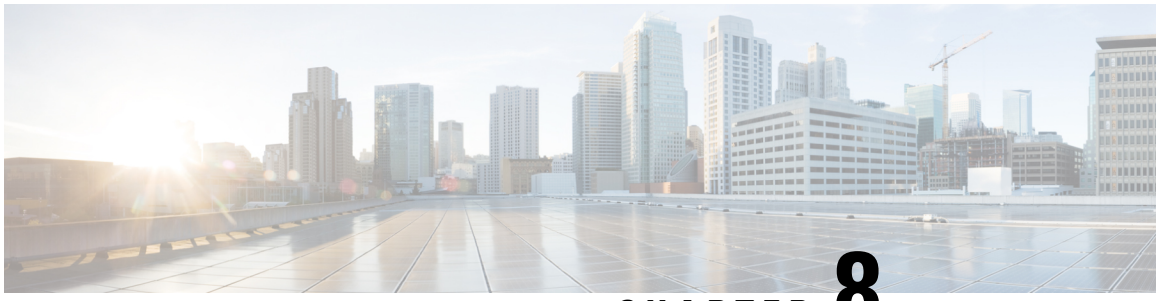
Note The controllers can either be standalone or redundancy paired controllers.

Step 7 If you want to move your APs back to the primary controller, check the corresponding checkbox. Otherwise, the APs, after reboot will get associated with the N+1 controller.

Step 8 To set the order in which the AP groups reboot, select an AP group and move it Up or Down the list.

Step 9 Select the transfer Protocol and enter the necessary details.

Step 10 To view the status of the job, click Administration and then click Job Dashboard under Dashboards.



CHAPTER 8

Perform Configuation Audits Using Compliance

This chapter contains the following topics:

How To Perform a Compliance Audit

The following table lists the basic steps for using the Compliance feature.

	Description	See:
1	Create a compliance policy that contains a name and other descriptive text.	Create a New Compliance Policy, on page 108
2	Add rules to the compliance policy. The rules specify what constitutes a violation.	Create Compliance Policy Rules, on page 109
3	Create a compliance profile (which you will use to run an audit on network devices) and: • Add a compliance policy to it. • Choose the policy rules you want to include in the audit. You can add multiple custom policies and/or predefined system policies to the same profile.	Create a Compliance Profile That Contains Policies and Rules, on page 112

4	Run a compliance audit by selecting a profile and scheduling an audit job.	Run a Compliance Audit, on page 113
5	View the results of the compliance audit and if necessary, fix the violations.	View the Results of a Compliance Audit, on page 114

Enable and Disable Compliance Auditing

The Compliance feature uses device configuration baselines and audit policies to find and correct any configuration deviations in network devices. It is disabled by default because some of the compliance reports can impact system performance. To enable the Compliance feature, use the following procedure.

Note To use the compliance feature, your system must meet the Professional sizing requirements, as specified in the .

Note In version 3.0, disabling compliance auditing disables the compliance from GUI and stops the compliance data collection in the background. User must restart the server and resync the devices for the compliance settings to be functional.

Step 1 Choose Administration > Settings > System Settings, then choose General > Server.

Step 2 Next to Compliance Services, click Enable, then click Save.

Step 3 Restart the application.

Step 4 Re-synchronize the device inventory: Choose Inventory> Network Devices, select all devices, then click Sync.

Note If compliance was enabled in before upgrading to version 3.0, after upgrade the compliance will be disabled in System Settings. User must enable it manually as per the steps mentioned in this section. In this scenario, restarting the server and resync of devices is not required.

Create a New Compliance Policy

You can create a new compliance policy starting with a blank policy template.

Step 1 Choose Configuration > Compliance > Policies.

Step 2 Click the Create Compliance Policy (+) icon in the Compliance Policies navigation area on the left.

Step 3 In the dialog box, enter a name and optional description, then click Create. The policy is added to the Compliance Policies navigation area on the left.

To duplicate the policy click the i icon and choose Duplicate Policy.

What to do next

Add rules to the compliance policy. See Create Compliance Policy Rules, on page 109.

Create Compliance Policy Rules

Compliance policy rules are platform-specific and define what is considered a device violation. A rule can also contain CLI commands that fix the violation. When you are designing the compliance audit job, you can select the rules you want to include in the audit (see Run a Compliance Audit, on page 113).

Step 1 Choose Configuration > Compliance > Policies, then select a policy from the navigation area on the left.

Step 2 From the work area pane, click New to add a new rule.

If a similar rule exists, you can copy the rule by clicking Duplicate, editing the rule, and saving it with a new name.

Step 3 Configure the new rule by entering your rule criteria.

Note supports all Java-based regular expressions. See http://www.rexegg.com/regex-quickstart.html.

a) Enter a title, description, and other information in the Rule Information text fields. This information is free text and does not impact any of the rule settings.
b) Specify the devices for this rule in the Platform Selection area.
c) (Optional) In the Rule Inputs area, click New and specify the input fields that should be displayed to a user when they run a policy that contains this rule. For example, you could prompt a user for an IP address.

Note If you choose the Accept Multiple Values check box, the audit will pass only if all the rule inputs match in the condition.

d) In the Conditions and Actions area, click New and specify the criteria that will be checked. This will determine the rule pass and fail conditions. For examples, see Examples—Rule Conditions and Actions, on page 110.

Step 4 Click Create. The rule is added to the compliance policy.

You can create as many rules as you want. Remember that when you want to run the audit job, you can pick the rules you want to validate.

Note It is recommended to use Java regex for testing the expressions while creating a new compliance policy rule and validating a rule or command using regular expressions, if any.

What to do next

Create a profile that contains the compliance policy and its rules, and then perform the audit using the profile. See Create a Compliance Profile That Contains Policies and Rules, on page 112.

Examples—Rule Conditions and Actions

Example: Block Options

This compliance policy checks if there are any rogue or unauthorized SNMP community strings are defined in the given blocks. If they are detected in the blocks, the policy raises a violation with the message “Detected unauthorized community string <1.1>” and removes all non-compliant SNMP strings from the blocks.

Tab	Tab Area	Field	Value
Rule Information		Rule Title	snmp-server community having non-standard entries
Platform Selection			Cisco IOS Devices, Cisco IOS-XE Devices
Condition 1			
Condition Details	Condition Scope Details	Condition Scope	Configuration
	Block Options	Block Start Expression (This field will be enabled only when Parse as Blocks checkbox is selected)	^snmp-server community .*
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community (.*)
Action Details	Select Match Action	Select Action	Continue
	Select Does Not Match Action	Select Action	Does Not Raise a Violation
Condition 2			

Condition Details	Condition Scope Details	Condition Scope	Previously Matched Blocks
	Block Options	Block Start Expression (This field will be enabled only when Parse as Blocks checkbox is selected)	^snmp-server community .*
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community ((public RO)|(private RW))
Action Details	Select Match Action	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a Violation
		Violation Message Type	User Defined Violation Message
		Violation Text	Detected unauthorized community string <1.1>.

Note In the above example, the matching criteria will be termed as 1.1, 1.2, and so on, for first condition. For the second condition, the matching criterial will be termed as 2.1, 2.2, and so on.

Example Conditions and Actions: Community Strings

This compliance policy checks if either snmp-server community public or snmp-server community private is configured on a device (which is undesirable). If it is, the policy raises a violation with the message "Community string xxxxx configured", where xxx is the first violation that was found.

Tab	Tab Area	Field	Value
Condition Details	Condition Scope Details	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community {public|private}
Action Details	Select Match Action	Select Action	Raise a violation
	Select Does Not Match Action	Select Action	Continue
		Violation Message Type	User Defined Violation Message
		Violation Text	Community string xxxxx configured.

Example Conditions and Actions: IOS Software Version

This compliance policy checks if Cisco IOS software version 15.0(2)SE7 is installed on a device. If it is not, the policy raises a violation with the message "Output of show version contains the string xxxxx," where xxxx is the Cisco IOS software version that does not match 15.0(2)SE7.

Tab	Tab Area	Field	Value
Condition Details	Condition Scope Details	Condition Scope	Device Command Outputs
		Show Commands	show version
	Condition Match Criteria	Operator	Contains the string
		Value	15.0(2)SE7
Action Details	Select Match Action	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a Violation
		Violation Message Type	User Defined Violation Message
		Violation Text	Output of show version contains the string xxxxx.

Example Conditions and Actions: NTP Server Redundancy

This compliance policy checks if the command ntp server appears at least twice on the device. If it does not, the policy raises a violation with the message "At least two NTP servers must be configured."

Tab	Tab Area	Field	Value
Condition Details	Condition Scope Details	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	(ntp server.*\n){2,}
Action Details	Select Match Action	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a violation
		Violation Message Type	User Defined Violation Message
		Violation Text	At least two NTP servers must be configured.

Create a Compliance Profile That Contains Policies and Rules

A compliance profile contains one or more compliance policies. When you add a compliance policy to a profile, all of the policy's rules are applied to the profile. You can customize the profile by selecting the policy

rules you want to include (and ignoring the others). If you group several policies in a profile, you can select and deselect the rules for each policy.

If you login as a Root, Admin or Super User, you will be able to do the following actions:.

- Create, edit or delete a profile.
- Select the rules that are created in the Policies page.

Note "Other" users need to enable the following task permissions to perform the relevant actions:

- Compliance Audit Profile Access to run the profile, refresh the profile and browse through the policies in the profile.
- Compliance Audit Profile Edit Access to create and edit a compliance audit profile.

The task permissions are located in the Administration > Users > Users, Roles & AAA > User Groups page.

If you do not select the Compliance Audit Profile Access task permission, you will not be able to view the Profile page, even if you have selected the Compliance Audit Profile Edit Access task permission.

Step 1 Choose Configuration > Compliance > Profiles.

Step 2 Click the Create Policy Profile (+) icon in the Compliance Profiles navigation area on the left. This opens the Add Compliance Policies dialog box.

Step 3 Select the policies you want to include in the profile. User defined policies will be available under the User Defined category.

a) In the Add Compliance Policies dialog box, choose the policies you want to add.
b) Click OK. The policies are added to the Compliance Policy Selector area.

Step 4 Select the rules you want to include in the policy.

a) Select a policy in the Compliance Policy Selector area. The policy's rules are displayed in the area on the right.
b) Select and deselect specific rules, then click Save.

Note The choices you make here only apply to the policy instance in this profile. Your choices do not modify the original version of the compliance policy.

What to do next

Schedule the compliance audit job as described in Run a Compliance Audit, on page 113.

Run a Compliance Audit

To run a compliance audit, select a profile, choose the devices you want to audit (using the policies and rules in the profile), and schedule the audit job.

Step 1 Choose Configuration > Compliance > Profiles.

Step 2 Select a profile in the Compliance Profiles navigation area on the left.

Step 3 Click the Run Compliance Audit icon in the Compliance Profiles navigation area.

Step 4 Expand the Devices and Configuration area, select the required devices and configuration files that you want to audit.

a) Select the devices (or device groups).

b) Specify which configuration file you want to audit.

- Use Latest Archived Configuration —Audit the latest backup file from the archive. If no backup file is available, does not audit the device.
- Use Current Device Configuration— Poll and audit the device's running configuration.

  When you select this option, first takes a backup of the configuration from device and then performs audit. This is useful when periodic or event triggered configuration backup is not enabled and also useful because archived configuration in is often out-of-sync with the device.

c) Click Next.

Step 5 Enter a value in the Configure Idle Time Limit (min) field. By default, the time limit is set to 5 minutes. Users can enter a number between 5 and 30 if they wish to change the time limit. The audit job will be aborted if it is idle for the configured time limit.

Step 6 Select Now to schedule the audit job immediately or select Date and enter a date and time to schedule it later.

Use the Recurrence option to repeat the audit job at regular intervals.

Step 7 Click Finish. An audit job is scheduled. A notification pop-up will appear once the audit job is scheduled. To view the status of the audit job, choose Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs.

Step 8 You will receive an email after the job completion. The email subject line contains, Hostname: Job type: Profile name: Job status for an audit job and Hostname: Job type: Job status for a fix job. The subject line also contains the subject specified by the user in the Mail Server Configuration screen or the Job Notification Mail screen, if any.

Step 9 You can view the following details in the email triggered for an audit job; Job Name, Job Type, Status, LastRunStatus, PI HostName, PI Host IP, Policy Profile Name, Total Device Count, Audited Device Count, Non-Audited Device Count, and links to verify the profile and job details.

Step 10 You can view the following details in the email triggered for a fix job; Job Name, Job Type, Status, LastRunStatus, PI HostName, PI host IP, and link to verify the job details.

Step 11 You will receive the job details in CSV format as an attachment. The CSV file is not secured with password.

What to do next

Check the audit results as described in View the Results of a Compliance Audit, on page 114.

View the Results of a Compliance Audit

Use this procedure to check an audit job results. The results will tell you which devices were audited, which devices were skipped, which devices had violations, and so forth. There might be several different compliance policies running on a single device.

After a job is created, you can set the following preferences for the job:

- Pause Series—Can be applied only on jobs that are scheduled in the future. You cannot suspend a job that is running.

- Resume Series—Can be applied only on jobs that have been suspended.
- Edit Schedule—Reschedule a job that has been scheduled for a different time.

Step 1 Choose Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs.

Step 2 Click the Audit Jobs tab, locate your job, and check the information in the Last Run column.

Last Run Result Value	Description
Failure	One or more devices audited have a violation in the policies specified in the profile.
Partial Success	The compliance job contains a mix of both audited and non-audited devices, and the compliance status of audited devices is successful.
Success	All devices audited conform to the policies specified in the profile.

For a compliance audit job, the number of violations supported is 20000 for Standard setup and 80000 for Pro and above setup of .

Step 3 If the audit check failed:

- To see which devices failed, hover over the "i" icon next to the Failure hyperlink to display a details popup.
- Launch a Device 360 view by selecting the job, clicking View Job Details, and clicking the "i" icon next to a device in the popup window.

Step 4 For the most detail, click the Failure hyperlink to open the Compliance Audit Violation Details window.

Note Use the Next and Previous buttons to traverse the Compliance Audit Violation Details window.

What to do next

To fix any of the violations, see .

Fix Compliance Violations on Devices

Prime Infrastructure allows you to fix any compliance violations that appear on devices.

Step 1 Choose Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs.

Step 2 Click Failure under the Last Run Result column for any job in which compliance violations were found. Prime Infrastructure displays the violation status of all policies that were run as part of the compliance audit.

Step 3 Choose a single or multiple Fixable violations in the Violation Details page and click Next.

If you choose all the fixable violations and if the number of fixable violations is more than 15000 then only the first 15000 rows will be selected.

Step 4 Click Save Startup Config and you can select the Copy Running Config to Startup option to copy the running configurationto the startup configuration.

Step 5 Click the expand arrow to view the devices for which the Enter Fix Input option is enabled.

Step 6 Choose the devices for which you want to apply a fix and click Enter Fix Input to enter the details.

Step 7 Click Next.

Step 8 Select the schedule for applying the configuration changes to the device, then click Schedule Fix Job.

Related Topics

Create a New Compliance Policy, on page 108
Create a Compliance Profile That Contains Policies and Rules, on page 112
View the Results of a Compliance Audit, on page 114
View Violation Summary Details, on page 116
View Violation Job Details, on page 116

View Violation Summary Details

You can run a report to display the violation summarized details for all the audit jobs that failed. To generate the report, follow these steps:

Step 1 Choose Configuration > Compliance > Violation Summary.

The report displays the summarized details of the job failure.

Step 2 You can download the reports in PDF and CSV formats.

You cannot export the following compliance reports if the server memory is less than the configured memory. Also, when one compliance export job is running, you cannot export another compliance report.

- Violation summary report
- PSIRT and EOX report (Device PSIRT, Device Hardware EOX, Device Software EOX, Field Notice)
- Compliance Jobs
  - Audit job failure > Violation details report
  - Audit job success report
  - Fix job success report
  - Fix job failure report

View Violation Job Details

The following table shows the details that can be viewed from the Violation Details page.

To View:	Do the following
The status of scheduled fixable violation jobs.	1. Go to the Violation Details page. 2. Click the Fixable column filter box and choose Running.

The details of Fixed violation jobs.	1. Go to the Violation Details page. 2. Click the Fixable column filter box and choose Fixed. 3. Click the Fixed link.
The details of Fix Failed violation jobs.	1. Go to the Violation Details page. 2. Click the Fixable column filter box and choose Fix Failed. 3. Click the Fix Failed link.

Import and Export Compliance Policies

Compliance policies are saved as XML files. You can export individual compliance policies and, if desired, import them into another server. Files can only be imported in XML format.

Step 1 Choose Configuration > Compliance > Policies.

Step 2 To export a compliance policy:

a) Mouse hover on "i" icon next to the policy in the Compliance Policies navigation area on the left.
b) In the popup window, click the Export Policy as XML hyperlink, and save the file.

Step 3 To import a compliance policy:

a) Click the Import Policies icon above the Compliance Policies navigation area on the left.
b) In the Import Policies dialog box, click Choose Policies.
c) Browse to the XML file and select it.
d) Click Import.

View the Contents of a Compliance Policy XML File

Compliance policies are saved as XML files. To view the contents of a policy's XML file:

Step 1 Choose Configuration > Compliance > Policies.

Step 2 Locate the policy in the Compliance Policies navigation area on the left, then hover your mouse over the "i" icon next to the policy.

Step 3 In the popup window, click the View Policy as XML hyperlink. displays the content in XML format.

View PSIRT and EOX Information

- View Device Security Vulnerabilities , on page 118
- View Device Hardware and Software End-of-Life Report , on page 118

• View Field Notices for Device , on page 119

Note The PSIRT and EOX page displays the PAS and RBML bundle generated dates. The PAS report holds the PSIRT and EoX records that are published on or before the bundle generated dates. It will not display the PSIRT records that are published post the bundle generation.

View Device Security Vulnerabilities

You can run a report to determine if any devices in your network have security vulnerabilities as defined by the Cisco Product Security Incident Response Team (PSIRT). The report includes Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX and Field Notice information. You can also view documentation about the specific vulnerabilities that describes the impact of a vulnerability and any potential steps needed to protect your environment.

Note PSIRT and EOX reports cannot be run for specific devices. When you schedule PSIRT and EOX jobs, the report is generated for all devices in Managed and Completed state (on the Inventory > Configuration > Network Devices page).

Before you begin

Sync the devices prior to scheduling the job. Choose Configuration > Network Devices, select the devices, then click Sync.

Step 1 Choose Reports > PSIRT and EoX.

Step 2 Schedule and run the job. The Schedule dialog box appears. You can set the Start Time and Recurrence options and then click the Submit button to schedule the job. Click the OK button, in the pop-up that appears, to delete the already scheduled job and create a new one.

A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX and Field Notice information is gathered and reported. Separate jobs on each of the tabs need not be created.

Step 3 Click View Job Details to view the current status of the PSIRT report.

Step 4 When the report is completed, click the Device PSIRT tab to view PSIRT information.

Step 5 In the PSIRT Title column, click the hyperlink to view the full description of a security vulnerability.

Step 6 (Optional) You can export the device PSIRT details in PDF and CSV format for each device and for all devices collectively.

View Device Hardware and Software End-of-Life Report

You can run a report to determine if any Cisco device hardware or software in your network have reached end of life (EOX). This can help you determine product upgrade and substitution options.

Step 1 Choose Reports > PSIRT and EOX.

Step 2 Click Schedule Job. The Schedule dialog box appears. You can set the Start Time and Recurrence options and then click the Submit button to Schedule the job. Click the OK button, in the pop-up that appears, to delete the already scheduled job and create a new one.

A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX and Field Notice information is gathered and reported. You do not create separate jobs on each of the tabs.

Step 3 After the job completes, click one of the following EOX tabs to view the report information specific to that tab:

- Device Hardware EOX
- Device Software EOX

Step 4 (Optional) You can export these device EOX details in PDF and CSV format for each device and for all devices collectively.

View Module Hardware End of Life Report

You can run a report to determine if any Cisco module hardware in your network have reach edits end of life (EOX).

Step 1 Choose Reports > PSIRT and EoX.

Step 2 Click Schedule Job. The Schedule dialog box appears. You can set the Start Time and Recurrence options and then click the Submit button to schedule the job. Click the OK button, in the pop-up that appears, to delete the already scheduled job and create a new one.

A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.

Step 3 Click the Module Hardware EOX tab to view module hardware information.

The Module PID column displays the PID data. It tends to be a single PID or group of PIDs. In the event of group of PIDs, the end of life details are displayed based on the PID that is mapped to a specific module hardware. Likewise, you cannot map PIDs with different end of life details. You must manually verify the report to map a PID with a specific EOL details. The Module PID column will not display any data if the hardware is not available in the container. The PAS details will not be displayed if the module chassis PID and the sub-modules PID are identical. The fixed modules do not have a PID. Thus, no EOL details will be displayed.

Step 4 (Optional) You can export the module hardware EOX details in PDF and CSV formats for each device and for all devices collectively.

View Field Notices for Device

You can run a report to determine if any Cisco devices that are managed and have completed a full inventory collection have any field notices. Field Notices are notifications that are published for significant issues, other than security vulnerability-related issues, that directly involve Cisco products and typically require an upgrade, workaround, or other customer action.

Step 1 Choose Reports > PSIRT and EOX.

Step 2 Click Schedule Job. The Schedule dialog box appears. You can set the Start Time and Recurrence options and then click the Submit button to schedule the job. Click the OK button, in the pop-up that appears, to delete the already scheduled job and create a new one.

A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX and Field Notice information is gathered and reported. You do not create separate jobs on each of the tabs.

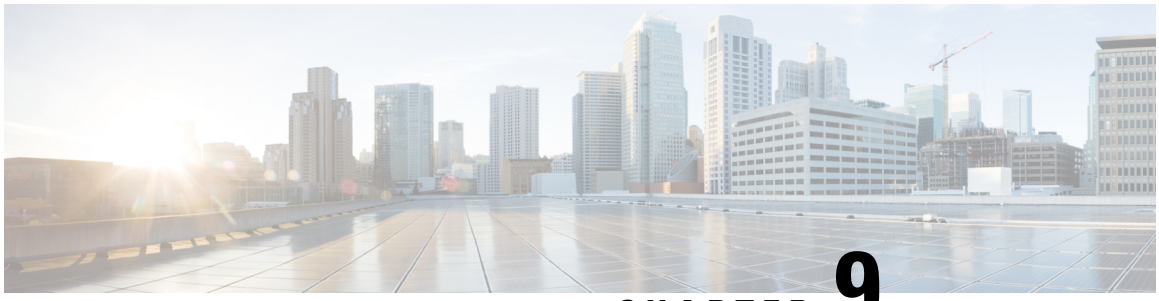
Step 3 Click the Field Notice tab to view field notice information.

Step 4 Click on the i icon in the Vulnerable column to open the Field Notice URL and Caveat Details dialog box. Click on the Field Notice URL to view more information on cisco.com.

Step 5 (Optional) You can export the device field notice details in PDF and CSV format for each device and for all devices collectively.

PART III

Visualize the Network



CHAPTER 9

Visualize the Network Topology

Network Topology Overview

The Network Topology window presents a graphical, topological map view of devices, the links between them, and the active alarms on elements in the map. In addition, the Network Topology window provides access to map element tools and functions, and allows you to drill-down to get detailed information about map elements.

The Network Topology window is accessed from the left sidebar (Maps > Topology > Network Topology). The content of the Network Topology window is determined by the device group you have selected. To select a device group, use the Device Groups panel on the left. From the Device Groups panel you can access the central device grouping functionality to create new groups, add devices to groups, and so on. See Create Groups of Devices for Easier Management and Configuration, on page 46 for more information.

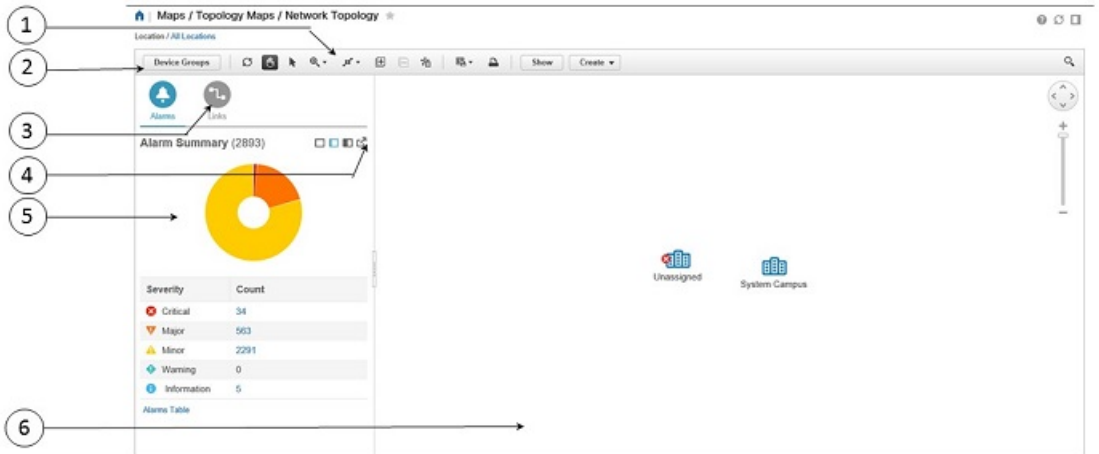
Each Network Topology map is divided into a left pane that contains alarm and link information, and a right pane that displays the map itself. When the left pane is expanded, additional columns might be added to the tables in the tabs.

- Alarm and Link Information (left pane)—Provides information relevant to the devices and topology shown in the map.
  - Alarm Summary—Shows all the current alarms for the selected group, categorized by alarm severity. In addition to a table showing the number of alarms for each alarm severity, the Alarm Summary tab provides a graphical pie chart view of the current alarms, which is color-coded based on alarm severity. This enables you to see, at a glance, the distribution of alarm severities and the number of alarms of each severity. In both the table and the pie chart you can drill down to see a table listing

the actual alarms of that severity. To see all the alarms for the selected device group, click the Alarms Table link at the bottom of the Alarm Summary tab.

- Links—Lists the links relevant to the selected device group and shows the highest severity alarm on the link. Selecting a link in the table, highlights the link in the topology map. Clicking the Links Table link at the bottom of the tab launches a separate window with a table of links.

- Topology map (right pane)—Displays the topology of the selected device group in graphical form. It displays the group's devices and sub-groups (if any) and the links between them (Physical, Ethernet, and technology-specific links). It also displays the active alarms on the devices or links so that you can easily identify problems in the network. You can drill down from the topology map to detailed information about a device or link in order to troubleshoot problems. The topology map can be customized, filtered, and manipulated to show exactly the information you need.



1	Topology toolbar	2	Device Groups pane
3	Links pane	4	Detach icon. Click the icon to open a detail window.
5	Alarm Summary pane. Click Alarms Table to display the alarm detail window.	6	Topology Map pane

Datacenter Topology

The data center topology keeps no link idle. The next-generation data center provides the ability to use all links in the LAN topology by taking advantage of technologies such as virtual PortChannels (vPCs). vPCs enable full, cross-sectional bandwidth utilization among LAN switches, as well as between servers and LAN switches.

A port channel bundles up to eight individual interfaces into a group to provide increased bandwidth and redundancy. Port channeling also load balances traffic across these physical interfaces. The port channel stays operational as long as at least one physical interface within the port channel is operational.

A virtual PortChannel (vPC) allows links that are physically connected to two different devices to appear as a single PortChannel to a third device. The third device can be any other networking device. A vPC allows

you to create redundancy by increasing bandwidth, enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

After you enable the vPC function, you create a peer keepalive link, which sends heartbeat messages between the two vPC peer devices.

Virtual Device Context (VDC) enables the virtualization of a single physical device in one or more logical devices. Each of the provisioned logical devices is configured and managed as if it were a separate physical device.

View Detailed Tables of Alarms and Links in a Network Topology Map

From the Network Topology window, you can access extended tables that list and provide more information about the alarms and links in the selected device group.

To open the extended details tables, click the Detach icon in the top right corner of the Alarm Summary (or click the hyperlink at the bottom of Alarm Summary or Links). The window that opens will contain an Alarms tab and a Links tab.

Be aware of the following when working with the extended tables:

- When the extended tables window is open, the left pane of the Network Topology window is disabled. When you close the extended tables window, the tabs in the left pane of the Network Topology window become fully functional again.
- There is synchronization between the extended tables and the information in the left pane in the Network Topology window. For example, if you select a link the extended links table, that link will also be selected in the left pane of the Network Topology window and the circuit/VC overlay will be shown in the topology map. Conversely, if you select a link in the left pane of the Network Topology window and then open the extended table, the same link will be selected in the extended table.
- Alarms in both the Network Topology window and in the extended tables are refreshed based on the user preference settings. See Set Up Your Alarm and Event Display Preferences, on page 267 and Customize the Alarm Summary, on page 268.
- Click the Export icon at the top right of the table to export the data from the table to a file (either PDF or CSV format). Export is available for alarms.

Filter Data in the Detailed Tables

You can also filter the data to find specific alarms or links using a quick filter or an advanced filter from the Show drop-down list. The quick filter narrows the content that is displayed in a column according to the text you enter above the column. The advanced filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. You can also create a user defined filter which, if saved, will be added to the Show drop-down menu.

To create and save a user defined filter:

Step 1 From the Show drop-down list above the extended tables of alarms and links, choose Advanced Filter.

Step 2 In the Advanced Filter data popup window, enter the advanced filter criteria, and then click Save As.

Step 3 In the Save Filter dialog box, enter a name for your filter and click Save.

To edit or remove a user defined filter, choose Manage User Defined Filters from the Show drop-down list.

Determine What is Displayed in the Topology Map

Choose Which Device Group(s) to Display in the Network Topology Map

The topology map enables you to visualize the topology of a device group or multiple device groups. The selected group(s) might cover a specific network segment, a customer network, or any other combination of network elements. Device grouping is hierarchical. There are two top-level parent groups containing multiple sub-groups - Location groups and User Defined groups. You can display multiple groups within the same top-level parent group. For example, you can display multiple Location groups but you cannot display one Location group and one User Defined group.

To determine which devices are displayed in the topology map,

After you have displayed the required group(s) in the topology map, you can access additional information about any device or link. See Get More Information About Devices

The topology map only displays devices for which the logged in user has access privileges, based on the virtual domains to which the user has been assigned.

Note If you encounter topology issues, such as topology components not rendering as expected or component data not being displaying on the map, we recommend that you clear your browser cache and try again.

To display network elements in the topology map:

Step 1 Choose Maps > Topology Maps > Network Topology.

Step 2 Customize the topology map as required by showing specific device/link types, adding manual links, and so on. See the following topics for more information:

- Change Which Link and Device Types are Shown in the Network Topology Map, on page 129
- Manually Add Links to the Topology Map, on page 128
- Change the Layout of a Network Topology Map, on page 131

View the Contents of a Sub-Group in the Topology Map

You can expand a sub-group to show its contents within the current context or you can drill down to see the contents of the sub-group independently of the current map context.

Note When expanding sub-groups, be aware that if a device belongs to more than one group, the device will appear in one of the expanded groups only. It will not appear in all of the groups to which it belongs. If your setup has devices that belong to multiple groups, rather view the groups individually in the topology map by selecting them in the Device Groups pane. This will ensure that you will always see all the devices that belong to a specific group.

To view the contents of a sub-group:

Step 1 Click on a sub-group in the topology map.

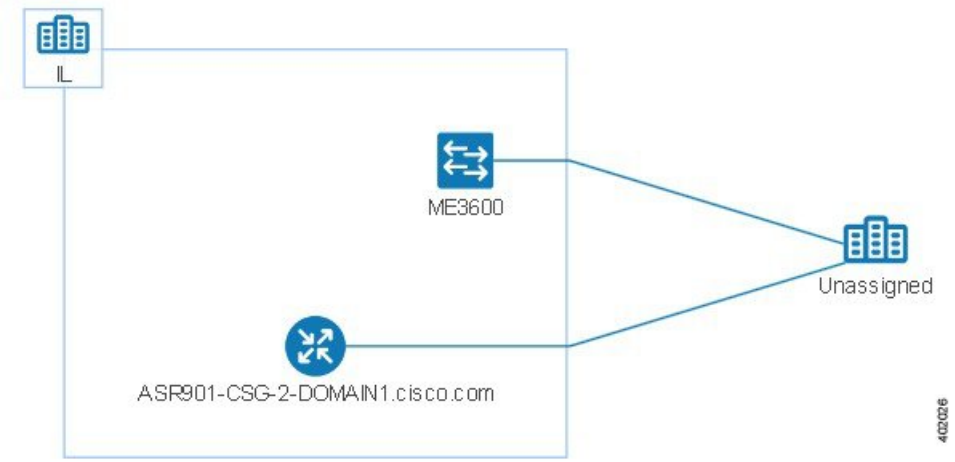
Step 2 In the displayed popup, click one of the following:

- Drill down group—Displays the sub-group on its own in the topology map, meaning that the currently displayed group is replaced with the selected sub-group. Note that the sub-group name is selected in the Device Groups pane.

  Note You can double-click on the sub-group to quickly drill down into the group.

- Expand group—Adds the contents of the sub-group to the current topology map display.

In the figure below, the IL group is expanded.



Manually Add Devices and Networks to the Topology Map

You can display devices and networks that are not managed by the system on the topology map and on the geo map by adding them manually.

Step 1 In the topology toolbar, choose Create > Create Unmanaged Device or Create > Create Unmanaged Network.

Step 2 Click on the map to add the device/network to the map.

Step 3 Click on the newly-added device/network in the map. From the displayed panel, you can add the device/network to a group, rename the device/network, or delete the device/network.

After you have added a device or network to the topology map, it will also be available in the geo map. The unmanaged device will appear in the list of unmapped devices and you can set its location.

Manually Add Links to the Topology Map

If you know that two devices are connected but cannot discover the link and show it on the map, you can add the link manually. After you add this link, it will be shown by default whenever the relevant group is shown on the map.

Following are the most common scenarios in which manual links could be used:

- From the optical/DWDM controller of a trunk port on a Cisco NCS device running IOS-XR (NCS 4000, 9000, 5000, 1000) to an add/drop port pair in NCS 2000 devices.
- From the optical/DWDM controller of a client port on a Cisco NCS device running IOS-XR (NCS 4000, 9000, 5000, 1000) to NCS 2000 transponder client ports (representing connections for 10GE/100GE ports).
- From 10GE/100GE controllers of ports on a Cisco NCS device running IOS-XR (NCS 4000, 9000, 5000,1000) to NCS 2000 transponder client ports (representing connections for 10GE/100GE ports).
- Between two trunk ports on Cisco NCS 2000 series devices with 400-G-XP linecards. This link must be created as a managed OTU link.
- From a Cisco NCS 2000 series device with 400-G-XP linecard and a Cisco NCS 4000 series device with 4H-OPW-QC2 linecards. This link must be created as a managed OTU link.

Manual links can be :

- Unmanaged links: For visualization purposes only. If you know that two devices are connected but you do not need full management of the link between them, you can add an unmanaged manual link to the map. The link will appear as a grey dashed line.

To manually add a link between two devices:

Step 1 Click and hold down the mouse on the first device in the topology map and drag it to the second device.

Step 2 In the Interface Details dialog, select the source interface on the first device and the target interface on the second device from the drop-down lists of available interfaces, and click OK.

The link between the two selected devices will be displayed on the map.

Change Which Link and Device Types are Shown in the Network Topology Map

You can choose to display only certain types of links or devices in the network topology map. Click the Show button and select Links or Device Families to see a full list of link and device types and select the ones you want to display.

Step 1 In the left sidebar, choose Maps > Topology Maps > Network Topology.

Step 2 Click Show in the topology toolbar and choose Links or Device Families.

Step 3 In the Links dialog:

- Select the types of links you want displayed in the topology map, for example, physical layer links, Ethernet layer links, and so on. The Links dialog only shows link types that exist in your network. If a link type exists in your network but not in the selected device group, it will be disabled.
- If you want to differentiate aggregated links from single links, select the Display Aggregated Links as check box.
- Click OK. The topology map will reflect your selections. Only the link types you selected will be displayed.

Step 4 In the Devices dialog:

- Select the device types you want displayed in the topology map, for example, routers, switches and hubs, optical networking, and so on. The Devices dialog only shows device types that exist in your network. If a device type exists in your network but not in the selected device group, it will be disabled.
- Click OK. The topology map will reflect your selections. Only the device types you selected will be displayed.

Note If you have selected to display optical networks on the map, by default you will see the devices that serve as optical line amplifiers (if any). Deselect the Display Optical Line Amplifier check box under Device Functions if you do not want these optical line amplifier devices to be displayed on the map. The Display Optical Line Amplifier check box under Device Functions only appears if there are optical devices in setup which support Line Amplifier functionality.

Show/Hide Alarms and Labels in the Topology Map

You can choose to hide the device name labels and you can hide alarms altogether or you can display alarms of specific severities only.

Step 1 In the left sidebar, choose Maps > Topology Maps > Network Topology.

Step 2 Click the Show button in the topology toolbar.

Step 3 Select the items you want displayed in the topology map:

- Labels—Labels associated with devices, such as device names.
- Faults—Deselect the check box to hide fault information altogether. Select the check box to show all alarms or use the slider to show only faults of a certain severity or higher.

Step 4 Close the Show dialog. Your selections are applied to the topology map.

Isolate Specific Sections of a Large Topology Map

In cases where a topology map is displaying thousands of devices, you might want to focus on specific devices or sets of devices. The Overview pane shows you the entire topology map in miniature and lets you select the area you want to display in the large topology map. It also provides an at-a-glance view of the alarm status of the elements in the topology map.

Step 1 Click the Overview icon in the topology toolbar. The Overview pane appears in the at the bottom right of the topology map and displays the following:

- Dot—indicates any network element. The color of the dot indicates the severity of alarms associated with the network element.
- Line—indicates a link. The color of the line indicates the severity of the associated alarm.
- Blue rectangle—indicates the selection area. The area within the rectangle is displayed in the map pane. Handles on the corners enable you to resize the selection area.
- Pan mode cursor—cursor displayed within the selection area. Use this cursor to move the selection area, and thereby view different elements in the map pane.
- Zoom mode cursor—displayed outside the selection area. Use this cursor to define a new selection area or to zoom in on an existing selection area.

Step 2 Draw a rectangle by dragging the mouse over the area you want to see in the topology map.

Step 3 Click the ‘x’ in the upper right corner to close the Overview pane.

Get More Information About Devices

From the topology map, you can drill down to get more information about a device.

Step 1 Click on the required device in the topology map. A popup appears showing basic device information and alarm information for the device.

Step 2 Click View 360 to access the Device 360 view for detailed information about the device.

Get More Information About Links

The representation of links in the topology map provides some information about the link:

- A solid line represents any type of discovered link between two elements in the topology map.
- A dotted line represents an unmanaged link that has been manually drawn in the topology map.
- A dot-dash line represents an aggregated link (if Aggregated Links is selected in the Show popup).

- An alarm severity badge indicates the highest severity alarm currently affecting the link.

From the topology map, you can drill down to get more information about a link by clicking on the required link in the topology map.

- For simple links, the displayed popup shows the link type and the A-side and Z-side of the link.
- For aggregated links, the displayed popup shows a table listing all the underlying links.

View Fault Information for Devices and Links

If a device or link has an alarm associated with it, an alarm badge is displayed on the device icon or on the link in the topology map. The color of the alarm badge corresponds with the alarm severity—minor (yellow), major (orange), or critical (red)—and matches the alarms displayed in the Alarm Browser.

For groups, the alarm badge represents the most severe alarm that is currently active for any of the group members.

Link-related alarms, such as Link Down, generate an alarm badge on the relevant link in the topology map. After the link up alarm is received, the link alarms and corresponding badges are cleared.

See Alarm Severity Icons, on page 269 for more information.

Change the Layout of a Network Topology Map

You can specify how the devices and other network elements (such as labels, nodes, and the connections between them) are arranged in the topology map:

- Symmetrical (default)—Maintains the symmetry that is inherent in the topology. This ensures that adjacent nodes are closer to each other and prevents node overlapping.
- Circular—Arranges the network elements in a circular style highlighting the clusters inherent in the network topology.
- Hierarchical—Ensures that the dependencies on the relationships and flows between elements are maintained.
- Incremental—Maintains the relative positions of specific elements while adjusting the positions of newly added elements. Use this layout to re-render nodes/links and to clean up overlaps.

Save the Layout of a Network Topology Map for Future Web GUI Sessions

retains your layout changes and your selections for the current browser session only. Therefore, after you have changed the topology map layout to suit your needs, it is highly recommended that you save the layout so that you do not have to manually rearrange the topology map each time.

Note The layout is saved for the selected device group only.

Choose Layout > Save Manual Layout from the Topology toolbar. You can reload the layout at any time by choosing Layout > Load Manual Layout.

If you want to return to the default system layout after you have saved your manual layout, you must delete the manual layout. Choose Layout > Delete Manual Layout.

Show Clock Synchronization Networks on a Network Topology Map

If Synchronous Ethernet (Sync-E) or Precision Time Protocol (PTP) clock synchronization is configured on the devices in your network, you can visualize the clock synchronization network on the topology map.

- The Sync-E overlay shows the topology and hierarchy of the sync-E network, including the primary clock and the primary and secondary clock inputs for each device. This allows the clock signal to be traced from any Sync-E enabled device to the primary clock or from the primary clock to a Sync-E enabled device.
- The PTP overlay shows the clock synchronization tree topology, the PTP hierarchy, and the clock role of each device in the tree - primary, boundary, subordinate, or transparent.

Step 1 In the left sidebar, choose Maps > Topology Maps > Network Topology.

Step 2 Click on the Device Groups button, select the required device group(s), and click Load.

Step 3 Click Show in the topology toolbar and choose Technology. Click the question mark icon for a description of what will be displayed on the map for each technology.

Step 4 Select the required technology and click OK.

The clock synchronization network is shown as an overlay over the existing network in the map. The legend at the bottom right explains the notations used in the map for the selected technology.

Note If you select a different device group, the technology overlay will be removed.

Save the Topology Map as an Image File

You can save the entire topology map or selected objects from the topology map as an image file. This will enable you to store copies of the topology map in a specific state which you can use as a point of reference in the future when multiple changes are made to the topology.

To save the topology map as an image file:

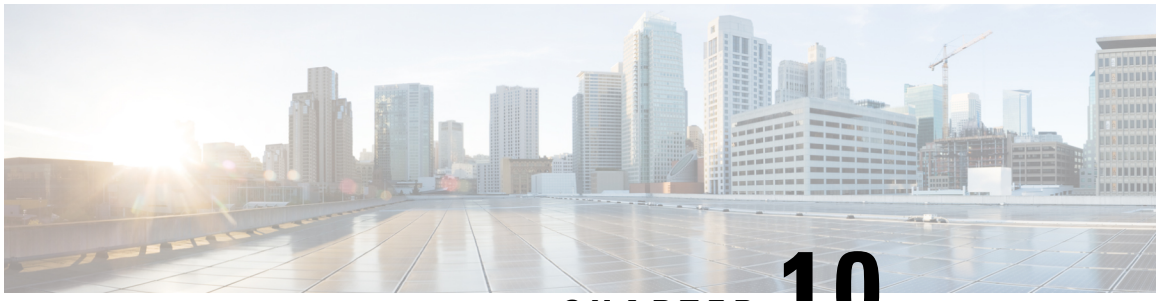
Step 1 Choose Maps > Topology Maps > Network Topology.

Step 2 Click on the Device Groups button, select the required device group(s), and click Load.

Step 3 Make content and layout changes to the topology map as required.

Step 4 Click the Save Image icon in the topology toolbar.

Step 5 From the Save Image drop down list, select the file type of the image being saved.
The image is saved in your local Temp folder.



CHAPTER 10

Use Wireless Site Maps

This chapter contains the following topics:

Introduction to Next Generation Wireless Site Maps

Cisco Prime Infrastructure introduces Next Generation wireless site maps from Release 3.2. The Next Generation site maps are enhanced with a new user interface which offers larger and more detailed maps.

To access the Next Generation wireless site maps, choose Maps > Wireless Maps > Site Maps (New).

The Domain Sidebar menu lists the campuses, buildings, outdoor areas, and floors in a tree view. When you click a campus, building, outdoor area, or floor in the tree view, the corresponding map along with different panels appear in the right pane.

Related Topics

Work with Site Maps, on page 137

Configuring Map Properties, on page 157

Configure Outdoor Areas, on page 143
Configure Buildings, on page 144
Configure Floor Areas, on page 149
Edit Floor Elements, on page 157
Use Monitoring Tools, on page 169
Using Planning Mode, on page 176
Data Filtering, on page 189

How Wireless Site Maps Are Organized

The wireless site maps have a predetermined hierarchy:

- Campuses are the highest level in the map hierarchy. Campus represents a single business location or site. Campuses consist of at least one building, with one or more floor areas, and many outside areas.
- Buildings represent single structures within a campus, serving to organization-related floor-area maps. You can add as many buildings you want to a single campus map. A building can have one or more floors and outside areas associated with it. You can add buildings only to a campus map.
- Floor areas are within the building which comprises of cubicles, walled offices, wiring closets, and so on. You can add floor areas only to building maps. You can add up to 100-floors to each building map that you create.
- Basement levels are similar to floor areas, except they are numbered in reverse order from floor areas. You can add basements to building maps only. You can add up to 100 basement levels to each building map you create, in addition to the 100 floor areas.
- Outside areas are the exterior locations. Although they are typically associated with buildings, outside areas must be added directly to campus maps, at the same level as buildings. You can add as many outside areas to a campus map as you want.

Cisco Prime Infrastructure comes with two default campus maps:

- System Campus—This is the default campus map. If you create a new building, floor, basement, or outside area, but do not create as part of your campus map, these subordinate maps are automatically created as children of the System Campus map.
- Unassigned—This is the default map for all network endpoints and hosts that you have not assigned to any other map (including the System Campus).

Guidelines for Preparing Image Files for Use Within Wireless Site Maps

- Use any graphics application that saves to the raster image file formats such as: PNG, JPEG, or GIF.
- For floor and outdoor area maps, Cisco Prime Infrastructure allows bitmap images such as PNG, JPEG, GIF, and CAD vector formats (DXF and DWG).
- Ensure that the dimension of the image is larger than the combined dimension of all buildings and outside areas that you plan to add to the campus map.
- Maximum dimensions supported for images used in wireless floor plan maps are:
  - PNG images - 20,000 pixels by 15,000 pixels.

- JPG images - 20,000 pixels by 20,000 pixels.

- Gather the horizontal and vertical dimensions of the site in feet or meters before importing. This helps you to specify these dimensions during import.
- If you are entering campus, building, floor, or outside area dimension in meters, change the default map measurement units to meters.
- Once you have created the maps, you can assign network elements to them. You can manually do this by selecting individual devices and assigning them to campuses, buildings, floors, and outside areas as needed. For wireless access points and access controllers, you can add them to your maps automatically by using your organization's access points or wireless access controllers naming hierarchy.

Troubleshoot Problems with CAD Image File Imports in Wireless Site Maps

Cisco Prime Infrastructure uses a native image conversion library to convert CAD and MET vector files into raster format. Select one of the following supported target raster formats during the CAD or MET file import: PNG, JPEG or (JPG), and GIF.

If Cisco Prime Infrastructure cannot load the native image conversion library, it displays an error message saying "Unable to convert the autocad file". If you receive this error message, make sure that all the required dependencies are met for the native library using the Linux `ldd` command. The following four DLLs must be present under `/webnms/rfdlls` install directory in Cisco Prime Infrastructure: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problem persists, install all the required libraries and then restart Cisco Prime Infrastructure server.

Floor and outside area map images imported from CAD files are enhanced for zooming and panning. Without zoom, the image clarity is close to that of the original CAD file. But an imported CAD file can appear blurred during zoom. If you are having a problem with blurred floor map images, make sure that all relevant parts of the image are clearly visible in the original CAD file. Then import the CAD file again, and choose PNG or GIF as the target conversion file format, instead of JPEG or JPG.

Large floor map images can take time to import. While the conversion is in progress, not all the image is visible on the map. If you have a high-resolution image (an image with a resolution of 180 megapixels and a file size of 60 MB), it may take two minutes or more for the imported image to appear on the map.

Work with Site Maps

Note All special characters except '&<>"/ are allowed while creating sitemaps and group from Release 3.1 onwards.

Choose Maps > Wireless Maps > Site Maps (New) to access this page.

Click the Site Hierarchy icon in the upper left corner of the Site Maps page to view or hide the Domain Navigator menu. The Domain Navigator menu lists all the campuses, buildings, floors, and outdoor areas in a tree hierarchy.

You can search the tree hierarchy to quickly find a campus, building, outdoor area, or floor. To search the tree hierarchy, enter the site name in the Search text box within the Domain Navigator menu. The tree hierarchy is filtered based on the parameter entered. Click the search result to view the corresponding map along with service domain panels which contain various site elements in the right pane. For example, if you select a

campus in the Domain Navigator menu, the right pane displays corresponding campus map along with various service domain panels. These service domain panels show the count of buildings, outdoor areas, floors, APs, clients, and critical radio for a particular camps.

Note

- The search result in the Domain Navigator menu does not show the hierarchy to which building a particular floor belongs to. Click the floor icon to view more details in the right pane.
- If background images are absent, Site Maps show buildings stacked on top of each other over Atlantic Ocean, as their geo coordinates are (0,0) by default.
- There is a temporary discrepancy between the data which is displayed on the floor directly and the data displayed on the service domain panels.

You can perform these operations on the Site Maps page:

- Add Sites, on page 138
- Remove a Site, on page 139
- Update a Site, on page 139
- Import Maps Archive
- Export Maps Archive, on page 140
- Import Bulk APs in CSV Format, on page 140
- Export Bulk APs in CSV Format, on page 141

Add Sites

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 In the Domain Navigator, navigate to the site map. The available site panels are displayed in the right pane.

Step 3 Click Add Site in the upper right corner of the Sites page. The New Site window appears. All the mandatory fields are displayed with a yellow background.

Step 4 Enter a name for the site in the Site Name text box. The site name can contain up to 32 characters.

Step 5 Enter the email address in the Contact text box. The contact details can contain up to 32 characters.

Step 6 Select the parent location group from the Parent Location Group drop-down list.

Step 7 Upload a site map by clicking the Click to select a file or drag it here. Browse to the site image file or drag and drop the image file to the Click to select a file or drag it here area.

Step 8 Enter civic location details in the Civic Location text box. The Longitude and Latitude text boxes are automatically updated when you enter valid civic location details.

Step 9 Enter the actual dimension of the site in the Width and Length text boxes.

Step 10 Click Save to save the details.

Remove a Site

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 In the Domain Navigator, navigate to the site map. The available site panels are displayed in the right pane.

Step 3 In the site panel on the right pane, click Delete.

Step 4 Confirm the deletion by clicking Remove.

Update a Site

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 From the Domain Navigator, navigate to the site map. The available site panels are displayed in the right pane.

Step 3 In the site panel, click Edit.

Step 4 In the Edit window, you can update the site attributes including the image file.

Step 5 Click Save.

Import Maps Archive

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 In the Domain Navigator, navigate to the site map. The available site panels are displayed in the right pane.

Step 3 From the Import drop-down list, choose Map Archive.

Step 4 The Import Map Archive wizard opens.

- On the Choose Format page, you can choose either of the following map format types:
  - XML Format
  - 3rd Party XML / Zip

Step 5 On the Select File page, click Click to select file or drag it here to browse to map location to import or you can drag and drop the map file into the Click to select file or drag it here area. You can import either the zip or tar format files. You can download a sample template to understand the format by clicking the Sample template can be downloaded here link.

Step 6 Select Verify. A message saying “Uploading file to server. Please wait for validation results” appears. Once the validation is complete, the result appears which contains information about map path, message, status, and overwrite information. You can overwrite or ignore.

Step 7 Click Process. The map import process starts.

The Summary table shows the Map Path, Message, and Status information. A green dot in the Status column represents a successful import to the database. A red dot represents that there was an error while importing the map.

From the Show drop-down list, choose All or Quick Filter to search using the Map Path and Message.

Step 8 After the import process is successful, click Done.
The imported maps appear in the Domain Navigator left sidebar menu on the Site Maps page.

Export Maps Archive

Before you begin

If you have manually updated the DB, there can be a DB discrepancy.

Before you export the maps, ensure that the edit operation works fine for the site, building, and floors in the source location. If the Edit building operation fails, you must adjust your position and save it in the source location.

To avoid missing the maps (site, building, floors) during the import maps operation, ensure that you follow the above check in the source location where you have exported the maps. When you import maps, the map data (position, coordinates, latitude, longitude) are validated before creation.

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 From the Export drop-down list, choose Map Archive.

Step 3 The Export Map Archive wizard opens.

Step 4 On the Select Sites page, configure the following. You must either select map information or calibration information to be included in the maps archive.

- Map Information—Turn the On/Off toggles to include map information in the archive.
- Calibration Information—To export calibration information, turn the On/Off toggles. You can either select the Calibration Information for selected maps or All Calibration Information radio button. If you select Calibration Information for selected maps, then the calibration information for the selected site maps is exported. If you select All Calibration Information, then the calibration information for the selected map along with additional calibration information that is available in the system is also exported.
- In the Sites left sidebar menu, check one or more check boxes of the site, campus, building floor, or outdoor area that you want to export. Check the Select All check box to export all the maps.

Step 5 Select the Generate Map Archive. A message saying "Exporting data is in progress" is displayed.
A tar file is created and is saved onto your local machine.

Step 6 Click Done.

Import Bulk APs in CSV Format

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 From the Import drop-down list which is located in the upper right corner of the page, choose Bulk AP in CSV.

Step 3 The Import Bulk AP wizard opens.

Step 4 On the Upload CSV tab, click Choose File and browse to the location of the CSV file that you want to import. You can download a sample template by clicking the Sample template can be downloaded here link.

Step 5 Click theSummary tab to view if the CSV import was successful or not. The Summary table contains Map Path, Message, and Status information.

Step 6 Click Done.

Export Bulk APs in CSV Format

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 From the Export drop-down list located in the upper right corner of the page, choose Bulk AP.

The Export Bulk AP wizard opens.

Step 3 The Select APs page lists all the available APs.

- You can use the Search Panel to search the access point that you want to export. You can search using the AP name, MAC address (Ethernet and Radio), or IP address, and click Search.
- You can select APs that are available in a particular outdoor area, site, campus, or floor. To do that:
  - Click the Select Site text box and check the check box of the corresponding outdoor area, site maps, campus, or floor.
  - Click OK. The selected site details appear in the Select Site field.
  - Click Search. The APs that are available in the selected sites are displayed.
  - Select the Include Unassigned check box to include APs that are not assigned to any floors.

Step 4 From the Show drop-down list, choose All or Quick Filter to search access points by the AP Name, MAC Address, Model, Controller, Status, or Floor.

Step 5 Check one or more AP Name check boxes and select Assign Floor to assign the selected APs to a floor.

Step 6 Click Assign To Floor, select the floor to which you want to assign the AP in the Sites window, and click OK.

Step 7 Click Generate CSV.

The CSV file is exported.

Step 8 Click Done.

Import Access Points for GeoMap

Step 1 Click Maps > Wireless Maps > Site Maps.

Step 2 Click Import > APs for GeoMap.

Step 3 Click or drag the file you'd like to Import (you can download a sample CSV file) and click Summary.

Step 4 Click Done.

Export Access Points for GeoMaps

Step 1 Click Maps > Wireless Maps > Site Maps.

Step 2 Click Export > APs for GeoMap.

Step 3 Select the APs whose Geo location you want to export in the Select APs tab.

APs associated to the controllers managed in Prime Infrastructure are listed here. You can also use the Search Panel to search for an AP by AP Name, Mac Address, or IP.

Step 4 Click Edit APs and edit the Longitude and Latitude values of the selected APs.

Step 5 Click Generate CSV to generate a CSV file.

Edit Map Properties

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 Click the User Preferences icon in the top right corner of the Sites page to edit the following map properties:

- Units of Measure—From the Units of Measure drop-down list, choose Feet or Meters to set the dimension measurement for maps.
- Wall Usage Calibration—From the Wall Usage Calibration drop-down list, choose Auto, Use Walls, or Do Not Use Walls. Wall usage calibration helps Cisco Prime infrastructure to take drawn walls into consideration while calculating heatmaps.
- Floor Start Index—From the Floor Start Index drop-down list, choose the floor level which is either 0 or 1.
- Refresh Map from Network—Select the Enable radio button for Cisco Prime Infrastructure to update maps by polling Cisco WLAN Solution every time an operator requests for a map update. Select the Disable radio button for Cisco Prime Infrastructure to update maps from its stored database.
- Advanced Debug Mode—Select the Enable radio button to allow Location Appliance and Cisco Prime Infrastructure to use the location accuracy testpoint feature.
- Use Dynamic Heatmaps—Select the Enable radio button to use the dynamic heatmaps. When the dynamic heatmaps are enabled, Cisco Prime Infrastructure recomputes the heatmaps to represent changed RSSI values.
- Minimum Number of APs for Dynamic Heatmaps—In the text box, enter the minimum number of APs that you want to use for dynamic heatmaps calculation. The minimum number of APs required is 3, and the maximum number of APs required is 10.
- Recomputation Frequency (hours)—In the text box, enter the heatmap recomputation frequency. The default frequency is 6 hours. The minimum frequency is 1 hour, and the maximum frequency is 24 hours.

Step 3 Click Save.

Configure Outdoor Areas

You can add outdoor areas to a campus map in Cisco Prime Infrastructure database regardless of whether you have added outdoor area maps to the database or not. You can define the dimensions of the area and add it to the database. The map can be of any size because Cisco Prime Infrastructure automatically resizes the map to fit the workspace.

Related Topics

- Add an Outdoor Area, on page 143
- Remove an Outdoor Area, on page 144
- Edit Outdoor Areas, on page 143

Add an Outdoor Area

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 Click Add Outdoor in the upper right corner of the campus page to which you want to add the outdoor area map. The New Outdoor Area window is displayed. All the mandatory fields are displayed with a yellow background.

- Outdoor Area Name—Enter the outdoor area name. The outdoor area name can contain up to 32 characters.
- Contact—Enter an email ID or a contact name. The contact details can contain up to 32 characters.
- Height (Feet)—Enter the outdoor area's height in feet. You can change this later in the User Settings.
- Type (RF Model)—From the drop-down list, choose Cubes And Walled Offices, Drywall Office Only, or Outdoor Open Space (default).
- Image File Name—Click Choose File and browse to the image and upload the file. You can import only PNG, GIF, or JPEG image formats.
- Civic Location—Enter the outdoor area's location details.
- Longitude and Latitude—Enter the outdoor area's North-West corner coordinate values.
- Dimensions (Feet)—Enter the actual outdoor area's dimension. You can later change the dimensions in the User Settings.

Edit Outdoor Areas

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 From the Domain Navigator, navigate to the campus site map. The available outdoor area panels are displayed in the right pane.

Step 3 Hover your mouse cursor to the outdoor area panel that you want to edit, and click the Edit icon.

Step 4 In the Edit Outdoor Area window, modify the outdoor area attributes including the image.

Step 5 Click Save.

Remove an Outdoor Area

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator, navigate to the campus site map. The available outdoor area panels are displayed in the right pane.

Step 3 Hover your mouse cursor to the outdoor area panel that you want to delete, and click the Delete icon.

Step 4 Click Remove to confirm the deletion.

Configure Buildings

You can add buildings only to a campus map. If you do not add them to a campus map you created, Cisco Prime Infrastructure adds them to the default System Campus map automatically.

Related Topics

- Add a Building, on page 144
- Edit a Building, on page 145
- Remove a Building, on page 145

Add a Building

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 Click Add Building in the upper right corner of the campus page to which you want to add this building. The New Building window appears. All the mandatory fields are displayed with a yellow background.

- Building Name—Enter a name for the building. The name must be unique among the other building names you plan to add to the same campus map. The building name can contain up to 32 characters.
- Contact—Enter an email ID or a contact name. The contact details can contain up to 32 characters.
- Num.Floors—Enter the number of floors in the building including the ground floor.
- Num. Basements—Enter the number of basements in the building.
- Civic Location—Enter the location information of the building.
- Longitude and Latitude—Enter the building's North-West corner coordinates.
- Dimensions (Feet)—Enter the building's actual dimension. You can change the dimension later in the User Settings.

To position a building, you can drag and drop a building on the floor and then position the building.

Edit a Building

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 From the Domain Navigator, navigate to the campus site map. The available building panels are displayed in the right pane.

Step 3 Hover your mouse cursor to the building panel that you want to edit, and click the Edit icon.

Step 4 In the Edit Building window, edit the building attributes.

Step 5 Click Save.

Remove a Building

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 From the Domain Navigator, navigate to the building map. The available building panels are displayed in the right pane.

Step 3 Hover your mouse cursor to the building that you want to delete, and click the Delete icon.

Step 4 Confirm Remove to confirm the deletion.

Note Deleting a building also deletes all its container maps. The APs from the deleted maps are moved to an Unassigned state.

Monitor Floor Areas

The floor view navigation pane provides access to multiple map functions like:

- Search on map—Use the Search feature to find specific floor elements like APs, clients, rogue APs, and so on. The elements that match the search criteria are displayed on the floor map along with a table in the right pane. When you hover your mouse over the table, it points to the search element on the floor map with a connecting line.
- Zoom in and out—The zooming levels depend upon the resolution of an image. A high-resolution image may provide more zoom levels. Each zoom level is made of a different style map shown at different scales, each one showing more or less detail. Some maps will be of the same style but at a smaller or larger scale.
  - Zoom In—You need to zoom in to see a map with more details. You can do this by using the zoom bar on the left side of the map. Click the Zoom In (+) icon at the top left side of the map. To center and zoom in on a location, double click the location. If you are zooming in using the keyboard, click the + sign. If you are using a mouse, use the mouse scroll wheel to zoom in.
  - Zoom Out—To see a map with less details you need to zoom out. To do this, click the Zoom Out (-) icon at the top left side of the map. If you are zooming out using the keyboard, click the - sign. If you are using a mouse, use the mouse scroll wheel to zoom out.

- Get Help—Click the Get Help (i) sign on the left side of the map to view the next generation map icons. Below table lists the Next Generation Map icons.

Table 17: Next Generation Map Icons

Icon	Description
Icons	
	802.11 Tags
	Rogue AP
	Adhoc Rogue
	Rogue Client
	Interferers
	Wips Attacks
	GPS Markers
	Choke Points
	WiFi TDOA Receivers
	Services
AP Status	
	Unknown

Icon	Description
	Critical
	Major
	Minor
	Warning
	Information
	Ok
Radio Status	
	Not Associated
	Unreachable
	Admin Disable
	Down
	Minor Fault

Icon	Description
	Ok
Clients (by RSSI/SNR)	
	Not available
	Excellent
	Good
	Fair
	Poor
A P Mode	
A	Autonomous
L	Local
M	Monitor
F	FlexConnect
R	Rogue Detector
S	Sniffer
B	Bridge
C	SE-Connect
Se	Sensor
Radio Band/Mode	
a	802.11 a/n/ac (5GHZ)
b	802.11 b/g/n (2.5GHZ)
n	802.11 a/b/g/n (2.4GHZ)
m	XOR (Monitor Mode)

Related Topics

- FlexConnect Groups and CCKM

Configure Floor Areas

You can add floor and basement areas to any building you have added to the campus map. Follow these guidelines while adding a floor:

- You can only add floor and basement areas to building maps.
- You can only add floor and basement areas up to the number of floors and basements you specified while adding a building to the campus map. If you enter these incorrectly, you must first edit the building map and then upload the floor map.

Related Topics

- FlexConnect Groups and CCKM
- FlexConnect Groups and Local Authentication

Add Floor Areas to Building

Step 1 Choose Maps > Wireless Maps > Site Maps (New) to navigate to this page.

Step 2 In the Domain Navigator left menu, navigate to the building to which you are adding the floor map.

Step 3 Click Add Floor in the upper right corner of the building page.

The New Floor window appears. All the mandatory fields are displayed with a yellow background.

- Floor Name—Enter a floor name. The floor name supports up to 32 characters.
- Contact—Enter the contact name or the email ID. The contact details can contain 32 characters.
- Floor Number—From the drop-down list, choose the floor number.
- Floor Height—Enter the floor-to-floor height in feet.
- Type (RF Model)—The RF model for the floor or basement. The model selected is used to calculate wireless signal strength, heat maps, and other wireless-related features for the floor or basement area.
- Image File Name—Click Choose File and select the floor map to upload. The floor map size is automatically calculated and displayed. Cisco Prime Infrastructure allows bitmap images such as PNG, JPEG, GIF, and CAD vector formats (DXF and DWG).

  Note You can filter layers of CAD images by navigating to the floor map and then clicking Tools > Show/Hide CAD Layers

- Civic Location—Enter the location information of the floor. The longitude, latitude, and the location information are updated as per the valid civic location entered.
- Longitude and Latitude—Enter the north-west corner coordinates.
- Dimensions (Feet)—Enter the actual size in width and height. You can change the size later in the User Settings.

- Position (Feet)—Enter the horizontal and vertical position. The horizontal position is the distance from the top left corner of the floor area to the left edge of the campus map. The vertical position is the distance from the top left corner of the floor area to the top edge of the campus map. You can enter these dimensions in feet or meters. If you modify this, then the longitude, latitude, and location icon on the map is updated.

Step 4 Click Save.

Configure Display Setting for Various Floor Elements

Click the Display Settings icon located at the upper right corner of the floor to configure various floor elements. The floor map along with these panels appear in the right pane: Access Point, Mesh, 802.11 Tags, Overlay Objects, Clients, Rogue AP, Adhoc Rogue, Rogue Client, Interferers, wIPS Attacks, MSE/CMX Settings, and Map Properties.

You can modify the appearance of the floor map by selecting or unselecting various parameters. For example, if you want to view only the access point information on the floor map, check the Access Point check box. You can expand each panel to configure various settings available for each floor element.

Related Topics

- Configuring Display Settings for Access Points, on page 150
- Configuring Display Settings for Mesh Access Points, on page 152
- Configuring Display Settings for 802.11 Tags, on page 154
- Configuring Display Settings for Overlay Objects, on page 154
- Configuring Display Settings for Clients, on page 155
- Configuring Display Settings for Rogue Access Points, on page 155
- Configuring Display Settings for Adhoc Rogues, on page 155
- Configuring Display Settings for Rogue Clients, on page 156
- Configuring Display Settings for Interferers, on page 156
- Configuring Display Settings for wIPS Attacks, on page 156
- Configuring Display Settings for MSE/CMX Site Maps Integration, on page 156

Configuring Display Settings for Access Points

Check the Access Points check box to view all APs on the map. Expand the Access Points panel to configure these settings:

- Display Label—From the drop-down list, choose a text label you want to view on the floor map for access point. The available display labels are:
  - Name—Displays the AP name.
  - AP MAC Address—Displays the AP MAC address.
  - Controller IP—Displays the IP address of Cisco WLC to which the AP is connected.
  - Radio MAC Channel—Displays the radio MAC address.

- Channel—Displays the Cisco Radio channel number or Unavailable (if the access point is not connected).
- TX Power—Displays the current Cisco Radio transmit power level (with 1 being high) or Unavailable (if the access point is not connected). If you change the radio band, the information on the map changes accordingly.

  The power levels differ depending on the type of access point. The 1000 series access points accept a value between 1 and 5, the 1230 access points accept a value between 1 and 7, and the 1240 and 1100 series access points accept a value between 1 and 8.
- Tx Power (dBm)—Displays the radio frequency (RF) power in decibels (dBm) for all radios in the AP.

Note Power level displays 0 (zero) if the radio is in scanning mode or is unavailable.

- Channel and Tx Power—Displays both the channel and transmit power level (or Unavailable if the access point is not connected).
- Coverage Holes—Displays a percentage of clients whose signal has become weaker until the client lost its connection, Unavailable for unconnected access points, or MonitorOnly for access points in monitor-only mode.
- MAC Addresses—Displays the MAC address of the access point, whether or not the access point is associated to a controller.
- Names—Displays the access point name. This is the default value.
- Controller IP—Displays the IP address of the controller to which the access point is associated or Not Associated for disassociated access points.
- Utilization—Displays the percentage of bandwidth used by the associated client devices (including receiving, transmitting, and channel utilization). Displays Unavailable for disassociated access points and MonitorOnly for access points in monitor-only mode.
- Profiles—Displays the load, noise, interference, and coverage components of the corresponding operator-defined thresholds. Displays Okay for thresholds not exceeded, Issue for exceeded thresholds, or Unavailable for unconnected access points.

  se the Profile Type drop-down list to choose Load, Noise, Interference, or Coverage.
- CleanAir Status—Displays the CleanAir status of the access point and whether or not CleanAir is enabled on the access point.
- Average Air Quality—Displays the average air quality on this access point. The details include the band and the average air quality.
- Minimum Air Quality—Displays the minimum air quality on this access point. The details include the band and the minimum air quality.
- Average and Minimum Air Quality—Displays the average and minimum air quality on this access point. The details include the band, average air quality, and minimum air quality.

- Associated Clients—Displays the number of associated clients, Unavailable for unconnected access points or Monitor Only for access points in monitor-only mode.
- Dual-Band Radios—Identifies and labels the XOR dual band radios on the Cisco Aironet 2800 and 3800 Series Access Points.
- Bridge Group Names
- Antenna Angle—Displays Azimuth angle and elevation for all radio antennas.

- Air Quality—You can either select Average AQ or Minimum AQ. You can set the access point heatmap type to view those details for the air quality selected on the map.
- Heatmap Opacity (%)—Drag the slider between 0 to 100 to set the heatmap opacity.
- RSSI Cut off (dBm)—Drag the slider to set the RSSI cutoff level. The RSSI cutoff ranges from -60 dBm to -90 dBM.
- Map Opacity (%)—Drag the slider to set the map opacity.
- Show Mobility Express— Toggle to view APs managed by a Mobility Express AP.

The AP details are reflected on the map immediately. Hover your mouse cursor over the AP icon on the map to view AP details and RX neighbor information.

Related Topics

- Quick View of APs, on page 160

Configuring Display Settings for Mesh Access Points

Note Mesh option is available only if you have any Mesh AP available on the floor.

Select the Mesh check box to view all Mesh APs on the map. Expand the Mesh panel to configure these settings:

- Link Label—From the Link Label drop-down list, choose a label for the mesh link:
  - None
  - Link SNR
  - Packet Error Rate
- Link Color—From the Link Color drop-down list, choose a color for the mesh link:
  - Link SNR
  - Packet Error Rate

The Link label and color settings are reflected on the map immediately. You can display both SNR and Packet Error Rate values simultaneously.

Table 18: Link Colors: SNR and PER

Color	Link Signal/Noise Ratio (SNR)	Packet Error Rate (PER)
Green	Represents an SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower
Amber	Represents a SNR between 20 and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
Red	Represents a SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)

Table 19: Link Colors: SNR and PER

Color	Link Signal/Noise Ratio (SNR)	Packet Error Rate (PER)
Green	Represents an SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower
Amber	Represents a SNR between 20 and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
Red	Represents a SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)

Table 20: Link Colors: SNR and PER

Color	Link Signal/Noise Ratio (SNR)	Packet Error Rate (PER)
Green	Represents an SNR above 25 dB (high value)	Represents a PER of one percent (1%) or lower
Amber	Represents a SNR between 20 and 25 dB (acceptable value)	Represents a PER that is less than ten percent (10%) and greater than one percent (1%)
Red	Represents a SNR below 20 dB (low value)	Represents a PER that is greater than ten percent (10%)

To modify the mesh access points display based on the number of hops between them and their parents, do the following:

- In the Mesh Parent-Child hierarchical View, choose the appropriate options from the Quick Selections drop-down list. A description of the options is provided in this table:

Table 21: Quick Selection Options

Field	Description
Select only Root APs	Choose this setting if you want the map view to display root access points only.
Select up to 1st hops	Choose this setting if you want the map view to display 1st hops only.
Select up to 2nd hops	Choose this setting if you want the map view to display 2nd hops only.
Select up to 3rd hops	Choose this setting if you want the map view to display 3rd hops only.

Field	Description
Select up to 4th hops	Choose this setting if you want the map view to display 4th hops only.
Select All	Select this setting if you want the map view to display all access points.

- Click Update Map View to refresh the screen and display the map view with the selected options.

Note Map view information is retrieved from the Prime Infrastructure database and is updated every 15 minutes.

Note You can also select or unselect the check boxes of access points in the mesh hierarchical view to modify which mesh access points are displayed. For a child access point to be visible, the parent access point to root access point must be selected.

Configuring Display Settings for 802.11 Tags

Select the 802.11 Tags check box to view tag location status on the map. Expand the 802.11 Tags panel to configure these settings:

- Show All Tags—Turn the On/Off toggles for tags to appear on the map.
- Display Label—Choose the tag identifier that you want to display on the map.
  - None
  - MAC Address
  - Asset Name
  - Asset Group
  - Asset Category

Configuring Display Settings for Overlay Objects

Expand the Overlay Objects panel to configure these settings. You can turn the On/Off toggles for the overlay objects to appear on the map.

- Coverage Areas
- Location Regions
- Obstacles
- Rails
- Markers

- GPS Markers
- ChokePoints
- WiFi TDOA Receivers
- Services

Configuring Display Settings for Clients

Expand the Clients panel to configure these settings.

- Show Client Clusters—Turn theOn/Off toggles to view wireless client cluster on the floor map.
- Color Code by—You can view clients by their RSSI or SNR information by setting the color code: RSSI or SNR.
- Display Label—From the drop-down list, choose the client identifier to display on the map:
  - None
  - User Name
  - IP Address
  - MAC Address
  - Asset Name
  - Asset Group
  - Asset Category

Note Autonomous AP client tracking is not supported through Cisco MSE.

Configuring Display Settings for Rogue Access Points

Expand the Rogue AP panel to configure these settings:

- Show Rogue APs Cluster—Turn the On/Off toggles to view all rogue APs in the cluster on the floor map.
- Show Rogue AP Zone of Impact—Turn the On/Off toggles to display the zone of impact for rogues APs. The rogue impact zone is determined by the transmission power of the Rogue AP and the number of clients associated with the rogue AP. The opacity of the circle on the map denotes the severity. A solid red circle represents a very strong impacted zone.

Configuring Display Settings for Adhoc Rogues

Expand the Adhoc Rogue panel to configure these settings:

- Show Adhoc Rogues Cluster—Turn the On/Off toggles to view adhoc rogue APs in the cluster.

- Show Rogue AP Zone of Impact—Turn the On/Off toggles to display the zone of impact for adhoc rogues APs.

Configuring Display Settings for Rogue Clients

Check theRogue Client check box to view all the rogue clients on the map. Expand the Rogue Client panel to configure these settings:

- Show Rogue Clients Cluster—Turn the On/Off toggles to view rogue clients in the cluster.

Quick View of Rogue Clients on the Map

Hover your mouse cursor over the Rogue Clients icon on the floor map to view the MAC address of the rogue client. You can click the Rogue Clients icon to view rogue clients details in the right pane:

- Detected By
- State
- Assoc. Rogue AP
- Detecting APs
- First Seen
- Last Seen
- Last Located
- Last Reported

Configuring Display Settings for Interferers

Check theInterferers check box to view all interferers on the map. Expand the Interferes panel to configure these settings:

- Show Zone of Impact—Displays the approximate interference impact area. The opacity of the circle denotes its severity. A solid red circle represents a very strong interferer that likely disrupts Wi-Fi communications, a light pink circle represents a weak interferer.

Configuring Display Settings for wIPS Attacks

Expand the wIPS Attacks panel to configure:

- Show wIPS Attack Cluster—Turn the On/Off toggles to view all wIPS attacks on the map.

Configuring Display Settings for MSE/CMX Site Maps Integration

Expand the MSE/CMX Settings panel to integrate site maps with Cisco Mobility Services Engine (MSE) or Cisco Connected Mobile Experiences (CMX).

- From the Show Data drop-down list, choose to view mobility services engine data from a range including the past two minutes up to the past 24 hours. This option only appears if a mobility services engine is present in Cisco Prime Infrastructure.
- To integrate maps with Cisco MSE, select the MSE radio button, and click Change MSE Assignment.

Note Autonomous AP client tracking is not supported through Cisco MSE.

1. In the Assigned MSEs table, select the mobility services engine to which the maps have to be synchronized.
2. Click Synchronize to complete the synchronization process.
3. Click Cancel to discard the changes to mobility services engine assignment.

- To integrate maps with Cisco CMX, select the CMX radio button, and click Change CMX Assignment.

Note If you delete AP from the Next Generation map floor, you must export the CMX floor map again to get the latest update from CMX. Otherwise, CMX assumes that it is using the same floor plan and AP positions and sends data which results in an inconsistency between floor clients count and other mobility entities.

1. In the Assigned CMXs table, select the CMX to which the maps have to be synchronized.
2. Click Synchronize to synchronize maps data to Cisco CMX.
3. Click Cancel to discard the changes to mobility services engine assignment.

Note When a Controller is removed from inventory, you need to manually re-sync the corresponding site maps in MSE or CMX again.

Configuring Map Properties

Expand the Map Properties panel to configure:

- Auto Refresh—Provides an interval drop-down list to set how often to refresh map data from the database. From the Auto Refresh drop-down list, set the time intervals: None, 1 min, 2 mins, 5 mins, and 15 mins.

Edit Floor Elements

Using the Edit option available on the floor area, you can add, position, define, draw, and enhance various floor elements. Click Edit at the upper right corner of any floor area to:

- Add, position, and delete these floor elements:
  - Access Points
  - ChokePoints
  - WiFi TDOA Receivers
- Add, edit, and delete these overlays:
  - Coverage Areas
  - Obstacles
  - Location Regions
  - Rails
  - Markers
  - GPS Markers

Related Topics

- Add, Position, and Delete APs, on page 158
- Add, Position, and Delete Choke Points, on page 161
- Add, Position, and Delete WiFi TDOA Receivers, on page 162
- Add Coverage Area, on page 163
- Create Obstacles, on page 164
- Location Region Creation, on page 165
- Rail Creation, on page 167
- Place GPS Markers, on page 168

Add, Position, and Delete APs

Cisco Prime Infrastructure computes Heat maps for the entire map which shows the relative intensity of the RF signals on the coverage area map. This display is only an approximation of the actual RF signal intensity because it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects of RF signals bouncing off obstructions.

Antenna gain settings have no effect on heatmaps and location calculations. Antenna gain is implicitly associated to the antenna name. Because of this, the following apply:

- If an antenna is used and marked as “Other” in Prime Infrastructure, it is ignored for all heatmap and location calculations.
- If an antenna is used and marked as a Cisco antenna in Prime Infrastructure, that antenna gain setting (internal value on Prime Infrastructure) is used no matter what gain is set on the controller.

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Floor Elements panel, next to Access Points, click Add.
All the access points that are not assigned to any floors appear in the list.

- In the Add APs page, select check box(es) of the access points that you want to add to the floor area, and click Add Selected.
- To add all access points, click Select All, and click Add Selected.
- To directly assign access points to the floor area, click +.
- You can search for access points using the search option available. Use the Quick Filter and search using the AP name, MAC address, Model, or Controller. The search is case-insensitive. The search result appears in the table. Click + icon to add to the floor area.

Step 5 Close the Add APs window after assigning access points to the floor area.

Step 6 Each access point that you added to the floor map appears on the right side of the map. You need to position them correctly.

Step 7 In the Floor Elements pane, next to Access Points, click Position to place them correctly on the map.

- Click and drag each access point to the appropriate location or update the x and y coordinates and AP Height in the Selected AP Details page. When you drag an access point on the map, its horizontal (x) and vertical (y) position appears in the text box. When selected, the access point details are displayed n the right pane. The Selected AP Details page shows the following:
  - Position by 3 points—You can draw three points on the floor map and position AP using the points created. To do this:
    - Click Position by 3 points.
    - To define the points, click anywhere on the floor map to start drawing the first point. Click again to finish drawing a point. A pop-up appears to set the distance to first point. Enter the distance in meters and click Set Distance.
    - Define the second and third points in the similar way and click Save.
  - Position by 2 Walls—You can define two walls on the floor map and position AP between the defined walls. This helps you know the position of AP between two walls. This helps you to understand the AP position between the walls.
    - Click Position by 2 walls.
    - To define the first wall, click anywhere on the floor map to start drawing the line. Click again to finish drawing a line. A pop-up appears to set the distance to first wall. Enter the distance in meters and click Set Distance.
    - Define the second wall in the similar way and click Save.

      The AP is placed automatically as per the defined distance between the walls.
  - AP NameShows—Shows the AP Name.
  - AP Model—Indicates the model type of the selected access point.
  - MAC Address—Displays the MAC address.
  - x—Enter the horizontal span of the map in feet.
  - y—Enter the vertical span of the map in feet.

- AP Height—Enter the height of the access point.
- Protocol—Protocol for this access point: 802.11a/n/ac, 802.11b/g/n (for Hyper Location APs), or 802.11a/b/g/n.
- Antenna—Antenna type for this access point.
- Antenna Image—Shows the AP image.
- Antenna Orientation—Depending on the antenna type, enter the Azimuth and Elevation orientations in degrees.

Note
- For APs with internal antennas, the Azimuth and Elevation values for all radios are locked together; i.e. if you change the settings for one radio, the orientation parameters get copied to other radios as well.
- Azimuth option does not appear for Omnidirectional antennas because their pattern is nondirectional in azimuth.

Note Changing the AP Azimuth, Elevation, and Power level values impact the heat map and coverage values.

Step 8 When you have completed placing and adjusting each access point, click Save.

Clicking Save causes the antenna gain on the access point to correspond to the selected antenna. This might cause the radio to reset.

Heatmap is generated based on the new position of the AP.

Step 9 In the Floor Elements panel, next to Access Points, click Delete.
The Delete APs page appears which lists all the assigned and places access points.

- Select check box(es) of the access points that you want to delete, and click Delete Selected.
- To delete all access points, click Select All, and click Delete Selected.
- To directly delete an access points from the floor, click the Delete icon.
- Use Quick Filter and search using the AP name, MAC address, Model, or Controller. The search is case-insensitive. The search result appears in the table. Click the Delete icon to delete from the floor area.

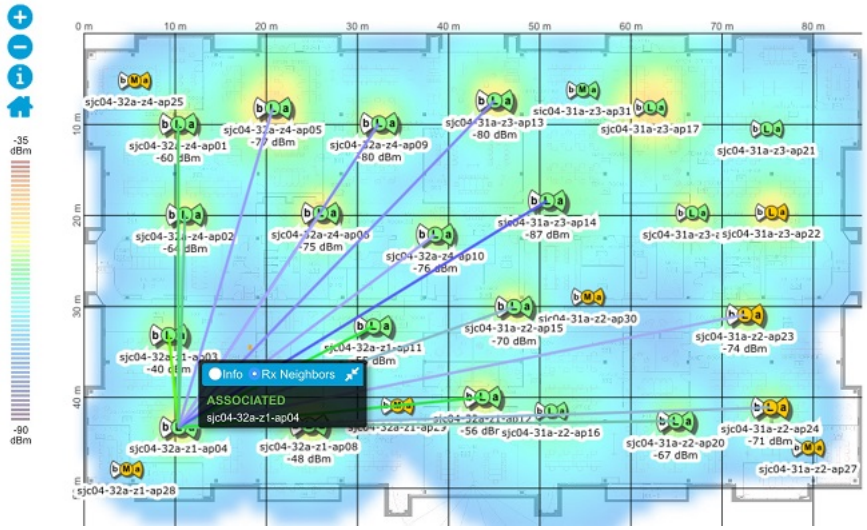
Quick View of APs

Hover your mouse cursor over the AP icon on the floor map to view AP details and Rx Neighbor information.

- Select Info to view the following AP details :
  - Associated—Indicates whether the AP is associated or not.
  - Name—Displays the AP Name.
  - MAC Address—Displays the AP MAC address.
  - Model—Displays the AP Model number.
  - Op./Admin/Mode—Displays the operational status and the AP mode.

- Type—Displays the radio type.
- Channel—Displays the channel number of the access point.
- Antenna—Displays the antenna name.
- Azimuth—Displays the direction of the antenna.

- Select the Rx Neighbors radio button to view the immediate Rx neighbors for the selected AP on the map with a connecting line. It also shows whether the AP is associated or not along with the AP name.



Add, Position, and Delete Choke Points

Choke points are installed and configured as recommended by the Choke point vendor. After the choke point installation is complete and operational, the chokepoint can be entered into the location database and plotted on an Prime Infrastructure map.

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Floor Elements panel, next to Choke Points, click Add.
The Add Choke Points page lists all recently added chokepoints that are in the database but are not yet mapped.

- Select check box(es) of the choke point that you want to add to place on the floor map and click Add Selected.
- To add all choke points, click Select All, and click Add Selected.
- You can search for choke points using the search option available. Use Quick Filter and search using the name, MAC address, or IP address. The search is case-insensitive. The search result appears in the table. Select the chokepoint check box and click Add Selected.

Step 5 Close the Add Choke points window after assigning access points to the floor area.

Step 6 The choke points that you added to the floor map appears on the right side of the map. You are now ready to position them on the map.

Step 7 In the Floor Elements pane, next to Choke Points, click Position to place them correctly on the map.

- Left-click the chokepoint icon and drag it to the proper location on the map.
- The MAC address, name, and coverage range of the chokepoint appear in the dialog box when you click the chokepoint icon for placement.
- Click Save. You are returned to the floor map and the added chokepoint appears on the map.

Note The newly created chokepoint icon might or might not appear on the map depending on the display settings for that floor. If the choke point does not appear on the map, ensure that the Choke Points toggle is set to On in the Display Settings > Overlay Objects.

Note The rings around the chokepoint icon indicate the coverage area. When a CCX tag and its asset passes within the coverage area, location details are broadcast, and the tag is automatically mapped on the chokepoint coverage circle. When the tag moves out of the chokepoint range, its location is calculated as before and is no longer mapped on the chokepoint rings.

Note The MAC address, name, entry/exit chokepoint, static IP address, and range of the chokepoint appear when you hover your mouse cursor over its map icon.

Note Do not click Save Settings unless you want to save this display criteria for all maps.

You must synchronize the network design to the mobility services engine or location server to push chokepoint information.

Step 8 In the Floor Elements panel, next to choke Points, click Delete.
The Delete choke points page appears which lists all the assigned and places choke points.

- Select check box(es) of the choke points that you want to delete, and click Delete Selected.
- To delete all choke points, click Select All, and click Delete Selected.
- To directly delete a choke point from the floor, click the Delete icon.
- Use Quick Filter and search using the Name, MAC address, or IP address. The search is case-insensitive. The search result appears in the table. Click the Delete icon to delete from the floor area.

Step 9 Click (i) sign to launch the AP 360° view.

Add, Position, and Delete WiFi TDOA Receivers

The Wi-Fi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset. TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Floor Elements panel, next to Wifi TDOA Receivers, click Add.
The Add Wifi TDOA Receivers page lists all recently added Wi-Fi TDOA receivers that are in the database but are not yet mapped.

- Select check box(es) of the Wifi TDOA receivers that you want to add to place on the floor map and click Add Selected.
- To add all Wifi TDOA Receivers points, click Select All, and click Add Selected.
- You can search for a Wifi TDOA receiver using the search option available. Use the Quick Filter and search using the Name, MAC address, or IP Address. The search is case-insensitive. The search result appears in the table. Select the Wifi TDOA receiver check box and click Add Selected.

Step 5 A map appears with a green WiFi TDOA receiver icon located in the top left-hand corner. You are now ready to position the Wi-Fi TDOA receiver on the map.

Step 6 Each access point that you added to the floor map appears on the right side of the map. You need to position them correctly.

Step 7 In the Floor Elements pane, next to Wifi TDOA Receivers, click Position to place them correctly on the map.

- Left-click the Wifi TDOA receiver icon and drag it to the proper location on the map.
- The MAC address and name of the Wi-Fi TDOA receiver appear in the left pane when you click the WiFi TDOA receiver icon for placement.
- Click Save when the icon is placed correctly on the map. The MAC address of the Wi-Fi TDOA receiver appears when you hover your mouse cursor over its map icon.

If the Wifi TDOA receivers does not appear on the map, ensure that the Wifi TDOA Receivers toggle is set to On in the Display Settings > Overlay Objects.

Step 8 In the Floor Elements panel, next to Wifi TDOA Receivers, click Delete.
The Delete Wifi TDOA Receivers page appears which lists all the assigned and placed Wifi TDOA Receivers.

- Select check box(es) of the Wifi TDOA Receivers that you want to delete, and click Delete Selected.
- Use the Quick Filter and search using the Name, MAC address, or IP Address. The search is case-insensitive. The search result appears in the table. Click the Delete icon to delete the choke point from the floor area.

Add Coverage Area

Any floor area or outside area defined as part of a building map is by default considered a wireless coverage area.

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a coverage area or a polygon-shaped area.

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Overlays panel, next to Coverage Areas, click Add.
A pop-up appears.

Step 5 To draw a coverage area, from the Type drop-down list, choose Coverage Area.

- Enter the name of the area you are defining, and click Ok.
- Move the drawing tool to the area you want to outline.
  - Click the left mouse button to begin and end drawing a line.
  - When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.

    The outlined area must be a closed object to appear highlighted on the map.
- Click Save to save the newly drawn area.

Step 6 To draw a polygon-shaped area, from the Type drop-down list, choose Perimeter.

- Enter the name of the area you are defining, and click Ok.
- Move the drawing tool to the area you want to outline.
  - Click the left mouse button to begin and end drawing a line.
  - When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.

Step 7 To edit a coverage area, in the Overlays panel, next to Coverage Areas, click Edit.

- The available coverage areas are highlighted on the map.
- Make the changes and click Save after the changes.

Step 8 To delete a coverage area, in the Overlays panel, next to Coverage Areas, click Delete.

- The available coverage areas are highlighted on the map.
- Hover your mouse cursor on the coverage area and click delete.
- Click Save after the deletion.

Create Obstacles

You to create obstacles so that they can be taken into consideration while computing RF prediction heatmaps for access points.

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Overlays panel, next to Obstacles, click Add.

Step 5 In the Obstacle Creation window, select an Obstacle Type from the Obstacle Type drop-down list. The type of obstacles you can create are: Thick Wall, Light Wall, Heavy Door, Light Door, Cubicle, and Glass.

Step 6 Click Add Obstacle.

Step 7 Move the drawing tool to the area where you want to create an obstacle.

- Click the left mouse button to begin and end drawing a line.

- When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.
- Click Done.
- The outlined area must be a closed object to appear highlighted on the map.
- Click Save to save the obstacle.

Step 8 To edit an obstacle, In the Overlays panel, next to Obstacles, click Edit.

- All the available obstacles are highlighted on the map.
- Click Save after the changes.

Step 9 To delete an obstacle, In the Overlays panel, next to Obstacles, click Delete.

- All the available obstacles are highlighted on the map.
- Hover your mouse cursor on the obstacle and click to delete.
- Click Save after the deletion.

Place Markers

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Overlays panel, next to Markers, click Add.

Step 5 Enter the name for the markers, and then click Add Marker. A drawing icon appears.

Step 6 Click the drawing icon and place the marker on the map.

Step 7 Click Save.

Step 8 To resynchronize Prime Infrastructure and mobility services engine, choose Services > Synchronize Services.

Step 9 In the Overlays panel, next to Markers, click Edit.

- The available markers are highlighted on the map.
- Make changes, and click Save.

Step 10 In the Overlays panel, next to Markers, click Delete.

- All the available markers are highlighted on the map.
- Hover your mouse cursor on the marker you want to delete, and click to delete.

Step 11 Click Save after the deletion.

Location Region Creation

You can create inclusion and exclusion area to further refine location calculations on a floor. You can define the areas that are included (inclusion areas) in the calculations and those areas that are not included (exclusion

areas). For example, you might want to exclude areas such as an atrium or stairwell within a building but include a work area (such as cubicles, labs, or manufacturing floors).

Define Inclusion Region on a Floor

Area within a floor or outside area map where wireless coverage data, such as signal strength, will be either mapped (included) or ignored (excluded).

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Overlays panel, next to Location Regions, click Add.

Step 5 In the Location Region Creation window, select Inclusion Type drop-down list.

Step 6 Click Location Region. A drawing icon appears to outline the inclusion area.

Step 7 To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

Step 8 Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.

Step 9 Repeat Step 8 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.

Step 10 Choose Save to save the inclusion region.

Step 11 Select the Location Regions check box if it is not already selected. If you want it to apply to all floor maps, click Save settings. Close the Layers configuration page.

Step 12 To resynchronize Prime Infrastructure and MSE databases, choose Services > Mobility Services > Synchronize Services.

Note If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 13 In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize. You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Note Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Define Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Overlays panel, next to Location Regions, click Add.

Step 5 In the Location Region Creation window, select Exclusion Type drop-down list

Step 6 Click Location Region. A drawing icon appears to outline the exclusion area.

Step 7 To begin defining exclusion area, move the drawing icon to a starting point on the map and click once.

Step 8 Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.

Step 9 Repeat Step 8 until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.

Step 10 To define additional exclusion regions, repeat Step 5 to Step 9.

Step 11 When all exclusion areas are defined, choose Save to save the exclusion region.

Step 12 Select the Location Regions check box if it is not already selected, click Save settings, and close the Layers configuration page when complete.

Step 13 To resynchronize Prime Infrastructure and location databases, choose Services > Synchronize Services.

Step 14 In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize. You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Edit Location Regions

In the Overlays panel, next to Location Regions, click Edit.

- The available location regions are highlighted on the map.
- Make changes, and click Save.

Delete Location Regions

In the Overlays panel, next to Location Regions, click Delete.

- The available location regions are highlighted on the map.
- Hover your mouse cursor on the location region you want to delete, and click to delete.
- Click Save.

Rail Creation

You can define a rail line on a floor that represents a conveyor belt. Additionally, you can define an area around the rail area known as the snap-width to further assist location calculations. This represents the area in which you expect clients to appear. Any client located within the snap-width area is plotted on the rail line (majority) or just outside of the snap-width area (minority).

The snap-width area is defined in feet or meters (user-defined) and represents the distance that is monitored on either side (east and west or north and south) of the rail.

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Overlays panel, next to Location Regions, click Add.

Step 5 Enter a snap-width (feet or meters) for the rail and then click Add Rail. A drawing icon appears.

Step 6 Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 7 Click the drawing icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 8 Click Save.

Step 9 To resynchronize Prime Infrastructure and mobility services engine, choose Services > Synchronize Services.

Step 10 In the Synchronize page, choose Network Designs from the Synchronize drop-down list and then click Synchronize.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Step 11 In the Overlays panel, next to Rails, click Edit.

- The available rails are highlighted on the map.
- Make changes, and click Save.

Step 12 In the Overlays panel, next to Rails, click Delete.

- All the available rail lines are highlighted on the map.
- Hover your mouse cursor on the rail line you want to delete, and click to delete.

Step 13 Click Save after the deletion.

Place GPS Markers

Before you begin

The X, Y coordinates for each GPS marker are linear measures (feet or meter) of the position relative to the North West (upper left) corner of the floor. These X, Y coordinates have corresponding latitude and longitude values. For each GPS marker, there must be no discrepancies in its latitude and longitude. A warning message appears if the latitude and longitude values do not match the co-ordinate (X,Y) distances.

When there are several GPS markers on the floor (three or more), for all of them the X, Y, latitude, longitude must agree with each other, and with the latitude and longitude of the floor.

If the floor is positioned at 0,0 co-ordinates inside the building, the latitude and longitude of the floor are the same as that of the building. Here, the NW corner of the floor coincides with the NW corner of the building.

Ensure that the latitude/longitude and horizontal/vertical regions are accurate before adding the GPS markers

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Edit at the upper right corner of the page.

Step 4 In the Overlays panel, next to GPS Markers, click Add.

Step 5 Enter the name for the GPS markers.

Step 6 Enter the value for Latitude and Longitude. GPS Markers identify the campus, building, or floor by longitude and latitude.

Step 7 Click Add GPS Marker.

Step 8 Click the drawing icon and place the GPS marker on the map.

Step 9 Click Save.

Step 10 In the Overlays panel, next to GPS Markers, click Edit.

- The available markers are highlighted on the map.
- Make changes, and click Save.

Step 11 In the Overlays panel, next to GPS Markers, click Delete.

- All the available GPS markers are highlighted on the map.
- Hover your mouse cursor on the GPS marker you want to delete, and click to delete.

Step 12 Click Save after the deletion.

Use Floor Tools

Use Monitoring Tools

Track Client Movement Using Client Playback

You can track the movement of a client on a floor using the Client Playback feature in Cisco Prime Infrastructure. Note that this feature is only available for clients detected by CMX.

To see a client's movement in a floor, follow the below procedure:

Step 1 Click Maps > Wireless Maps > Site Maps.

Step 2 Select Campus > Building > Floor.

Step 3 Add the APs that have the associated or probing clients.

Step 4 Click Services > Mobility Services > Connected Mobile Experiences.

Step 5 Export the maps and import them to CMX.

Step 6 Navigate to the desired sitemap and synchronize the floor with CMX.

Step 7 Click the desired client on the floor.

Step 8 Click Data > Client > Playback.
The map will display client's movement over a period of time.

Inspect Location Readiness

You can configure Prime Infrastructure to verify the ability of the existing access point deployment to estimate the true location of a client, rogue client, rogue access point, or tag within 10 meters at least 90% of the time. The location readiness calculation is based on the number and placement of access points.

You can also check the location quality and the ability of a given location to meet the location specification (10 m, 90%) based on data points gathered during a physical inspection and calibration.

The Inspect Location Readiness feature is a distance-based predictive tool that can point out problem areas with access point placement.

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Tools at the upper right corner of the page, and click Inspect Location Readiness.

The deprecated Site Maps page opens. A color-coded map appears showing those areas that meet (indicated by Yes) and do not meet (indicated by No) the ten meter, 90% location specification.

Note If RSSI is not displayed, you can enable AP Heatmaps by selecting the AP Heatmaps check box on the left sidebar menu.

Note If clients, tags, and access points are not displayed, verify that their respective check boxes are selected on the left sidebar menu. Licenses for both clients and tags must also be purchased for each to be tracked.

Inspect Voice Readiness

The voice readiness tool allows you to check the RF coverage to determine if it is sufficient for your voice needs. This tool verifies RSSI levels after access points have been installed.

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Tools at the upper right corner of the page, and click Inspect Voice Readiness.

The deprecated Site Maps page opens.

Step 4 Choose the applicable Band, AP Transmit Power, and Client parameters from the drop-down lists.

Note By default, the region map displays the b/g/n band for Cisco Phone-based RSSI threshold. The new settings cannot be saved.

Step 5 Depending on the selected client, the following RSSI values might not be editable:

- Cisco Phone—RSSI values are not editable.
- Custom—RSSI values are editable with the following ranges:
  - Low threshold between -95dBm to -45dBm
  - High threshold between -90dBm to -40dBm

Step 6 The following color schemes indicate whether or not the area is voice ready:

- Green—Yes
- Yellow—Marginal
- Red—No

The accuracy of the Green/Yellow/Red regions depends on the RF environment and whether or not the floor is calibrated. If the floor is calibrated, the accuracy of the regions is enhanced.

RF Calibration Methods

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Tools at the upper right corner of the page, and click Inspect Voice Readiness.

The deprecated Site Maps page opens. On the RF Calibration Models page, you can:

- Apply calibration models to maps
- View calibration model properties
- Edit calibration model details

Adjust RF Calibration Models Used in Wireless Maps

Prime Infrastructure provides multiple RF models to characterize the attenuation characteristics of the floor areas in the wireless site maps you create. These calibration models are used as RF overlays with measured RF signal characteristics that can be applied to different floor areas. If none of these is precise enough for your needs, you can create one or more custom calibration models that better represent the attenuation characteristics of your actual floor areas and then apply them to your maps of these floor areas. This enables your team to:

- Lay out one or more floors in a real-world building.
- Use the RF calibration tool to measure the RF attenuation characteristics of the actual floor.
- Save the RF characteristics of that floor as a new calibration model.
- Apply that calibration model to all the other floors with the same physical layout.

You can collect data for a calibration using one of two methods:

- Point mode data collection—Calibration points are selected and their coverage area is calculated one location at a time.
- Linear mode data collection—A series of linear paths are selected and then calculated as you traverse the path. This approach is generally faster than point mode. You can also employ point mode data collection to augment data collection for locations missed by the linear paths.

Calibration models can only be applied to clients, rogue clients, and rogue access points. Calibration for tags is done using the Aeroscout System Manager (for more information on this product and how to use it, send an email inquiry to cisco-rtls@cisco.com).

Use a laptop or other wireless device to open a browser to a Prime Infrastructure server and perform the calibration process.

To expedite the calibration process for both spectrums, Cisco recommends using a client device that supports both 802.11a/n and 802.11b/g/n radios.

For more information on the calibration process, see the following related topics.

- View the List of Current RF Calibration Models
- Accessing Current Calibration Models
- Apply Wireless Calibration Models to Wireless Site Maps
- View RF Calibration Model Properties
- Create New RF Calibration Models
- Calibrate, Compute and Apply New RF Calibration Models
- Compute Collected "Live" Data Points for New RF Calibration Models
- Apply Fully Calibrated New RF Calibration Models to Floor Areas in Wireless Site Maps
- Delete RF Calibration Models

Create New RF Calibration Models

To create a new calibration model, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Choose Select a command > RF Calibration Models > Go.

Step 3 Choose Select a command > Create New Model > Go.

Step 4 Enter a name for the new RF calibration model, then click OK.

The new model appears in the list along with the other RF calibration models, with a status of "Not Yet Calibrated". To calibrate the model, see the related topic "Calibrate, Compute and Apply New RF Calibration Models"

Calibrate, Compute and Apply New RF Calibration Models

To fully apply a newly created RF calibration model, you must:

1. Collect “live” calibration data.
2. Compute that data so that the model can use it.
3. Apply the model to the floors you want.

To complete this process with a new RF calibration model that you have just created and named (but whose status is "Not Calibrated"), follow the steps below. Before you begin, you will need to have your data collection

device enabled, along with a connection to the Prime Infrastructure server. If you are not using the Cisco Centralized architecture, you will also need to know the data collection device's MAC address.

Step 1 Choose Maps > Site Maps.

Step 2 Choose Select a command > RF Calibration Models > Go.

Step 3 Click the model name to open the Calibration Model > Model Name page.

Step 4 Choose Select a command > Add Data Points > Go.

Step 5 Enter the MAC address of the device being used to perform the calibration. Manually-entered MAC addresses must be delimited with colons (such as FF:FF:FF:FF:FF:FF).

If this process is being performed from a mobile device connected to Prime Infrastructure through the Cisco Centralized architecture, the MAC address text box is automatically populated with the device address.

Step 6 Choose the appropriate campus and building, and then the floor area, basement level, or outdoor area where you want to perform the calibration. Then click Next.

Step 7 When the chosen floor area map and access point (AP) locations appear, a grid of plus marks (+) indicates the locations where data collection must be performed.

Using these locations as guidelines, you can perform either a point or linear collection of data. You can do this via appropriate placement of either the Calibration Point pop-up (point) or the Start and Finish pop-ups (linear) that appear on the map when the respective options are displayed.

Step 8 To perform a point collection of data for the calibration, do the following:

a) Choose Collection Method > Point and select the Show Data Points check box (if not already selected). A Calibration Point pop-up appears on the map.

b) Position the tip of the Calibration Point pop-up at one of the data points on the map (+), and click Go. A dialog box appears showing the progress of the data collection.

Rotate the calibrating client laptop during data collection so that the client is heard evenly by all APs in the vicinity.

c) When the data collection is complete for a selected data point and the coverage area is plotted on the map, move the Calibration Point pop-up to another data point, and click Go.

The coverage area plotted on the map is color-coded and corresponds with the specific wireless LAN standard used to collect the data. Information on color-coding is provided in legend on the left side of the page. Additionally, the progress of the calibration process is indicated by two status bars above the legend, one for 802.11a/n and one for 802.11b/g/n.

To delete data points for locations selected in error, click Delete and move the black square that appears over the appropriate data points. Resize the square as needed by pressing **Ctrl** and then moving the mouse.

d) Repeat point collection Steps A through C until the calibration status bar of the relevant spectrums (802.11a/n, 802.11b/g/n) display as "Done".

The calibration status bar indicates data collection for the calibration as done after roughly 50 distinct locations and 150 measurements have been gathered. For every location point saved in the calibration process, more than one data point is gathered. The progress of the calibration process is indicated by two status bars above the legend, one for 802.11b/g/n and one for 802.11a/n.

Step 9 To perform a linear collection of data for the calibration, do the following:

a) Choose Collection Method > Linear and select the Show Data Points check box (if not already selected). A line appears on the map with both Start and Finish pop-ups.

b) Position the tip of the Start pop-up at the starting data point.
c) Position the Finish pop-up at the ending data point.
d) Position yourself with your laptop at the starting data point, and click Go. Walk slowly and steadily toward the end point along the defined path. A dialog box appears to show that data collection is in process.

   Do not stop data collection until you reach the end point, even if the data collection bar indicates completion.

   Only Intel and Cisco adapters have been tested with this method. Make sure that both Enable Cisco-compatible Extensions and Enable Radio Management Support are enabled in the Cisco-compatible Extension Options.

e) Press the space bar (or Done on the data collection panel) when you reach the end point. The collection pane displays the number of samples taken before it closes to reveal the map. The map displays all the coverage areas where data was collected.

   To delete data points for locations selected in error, click Delete and move the black square that appears over the appropriate data points. Resize the square as needed by pressing **`Ctrl`** and then moving the mouse.

   The coverage area is color-coded and corresponds with the specific wireless LAN standard used to collect that data. Information on color-coding is provided in legend on the left-hand side of the page.

f) Repeat linear collection Steps B through E until the status bar for the respective spectrum is filled in (done).

   You can augment linear collection with point mode data collection to address missed coverage areas.

Step 10 When you are finished collecting data points, click the name of the calibration model at the top of the page to display the model again.

If needed, you can now stop and complete the computation and application of the stored data points at a later time. If you decide to do this, continue by following the instructions in the related topics "Compute Collected "Live" Data Points for New RF Calibration Models" and then "Apply Fully Calibrated New RF Calibration Models to Floor Areas in Wireless Site Maps".

Step 11 To calibrate the model against the collected data points: Choose Select a command > Calibrate > Go.

Step 12 When calibration processing completes, click the Inspect Location Quality link. A map displays showing RSSI readings.

Step 13 To apply the newly calibrated model to the wireless site map floor area on which it was created (and to any other floor areas with similar attenuation characteristics): Choose Maps > Site Maps. On the Maps page, choose the link that corresponds to the floor area where you want to apply the new RF calibration model.

Step 14 With the floor area map displayed, choose Select a command > Edit Floor Area > Go.

Step 15 From the Floor Type (RF Model) drop-down list, choose the newly created calibration model. Click OK to apply the model to the floor.

This process can be repeated for as many models and floors as needed. After an RF calibration model is applied to a floor, all location determination performed on that floor is done using the RF attenuation data in the calibration model.

Compute Collected "Live" Data Points for New RF Calibration Models

To compute previously collected calibration data so that it can be used with an RF calibration model,, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 From the Select a command drop-down list, choose RF Calibration Models, then click Go.

Step 3 Click the name of the model for which "live" data points were previously collected. The Calibration Model > Model Name page displays the RF calibration model you selected.

Step 4 From the Select a command drop-down list, choose Calibrate and click Go.

Step 5 When calibration processing completes, click the Inspect Location Quality link. A map displays showing RSSI readings.

Apply Fully Calibrated RF Calibration Models to Floors in Wireless Site Maps

To use a new RF calibration model, you must apply the model to the floor on which it was created (along with other floors with similar attenuation characteristics).

To apply the model to the floor, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Locate the specific floor to which the model is applied.

Step 3 From the Select a command drop-down list, choose Edit Floor Area, then click Go.

Step 4 From the Floor Type (RF Model) drop-down list, choose the newly-created RFcalibration model.

Step 5 Click OK to apply the model to the floor.

This process can be repeated for as many models and floors as needed. After a model is applied to a floor, all location determination performed on that floor is done using the specific collected attenuation data from the calibration model.

Delete RF Calibration Models

To delete a calibration model, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Choose Select a command > RF Calibration Models > Go. The list of current RF calibration models displays.

Step 3 Click the name of the model you want to delete. The Calibration Model > Model Name page displays.

Step 4 Choose Select a command > Delete Model > Go. Prime Infrastructure deletes the calibration model.

View RF Calibration Model Properties

To view or edit current calibration models, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Choose Select a command > RF Calibration Models > Go.

Step 3 Click the model name to access the RF calibration model whose properties you want to view or change.

Step 4 To view or edit the selected model's properties:

a) Choose Select a command > Properties > Go.

You can view or edit the following properties:

- Sweep Client Power for Location—Click to enable. You might want to enable this if a high density of access points (APs) exists and transmit power is reduced or unknown. Using the sweep range may improve location data accuracy, but scalability will be affected negatively.
- HeatMap Binsize—Choose 4, 8, 16, or 32 from the drop-down list.
- HeatMap Cutoff—Determine the heatmap cutoff. Cisco recommends a low heatmap cutoff especially if the AP density is high and RF propagation conditions are favorable. A higher cutoff value increases scalability but might cause difficulty when locating clients.

Step 5 When you are finished, click OK.

Apply RF Calibration Models to Wireless Site Maps

To apply a current calibration model to a map, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Choose Select a command > RF Calibration Models > Go. The Model Name and Status for each calibration model are listed.

Step 3 Click the model name to access the RF calibration model you want.

Step 4 Choose Select a command > Apply to Maps > Go.

Using Planning Mode

You can calculate the recommended number and location of access points based on whether data and/or voice traffic and/or location are active.

Based on the throughput specified for each protocol (802.11a or 802.11 b/g), planning mode calculates the total number of access points required that would provide optimum coverage in your network.

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Tools at the upper right corner of the page, and click Planning Mode.

Planning mode does not use AP type or Antenna pattern information for calculating the number of access points required. The calculation is based on the access point coverage area or the number of users per access point.

Planning Mode options are:

- Add APs—Enables you to add access points on a map. See the Using Planning Mode to Calculate Access Point Requirements for details.
- Delete APs—Deletes the selected access points.
- Map Editor—Opens the Map Editor window. See the Using the Map Editor for more details.

- Synchronize with Deployment—Synchronizes your planning mode access points with the current deployment scenario.
- Generate Proposal—View a planning summary of the current access points deployment.
- Planned AP Association Tool—Allows you to perform add, delete or import an AP Association from an excel or CSV file. Once an access point is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered they get pushed into a standby bucket and get associated when discovered.

Note AP association is subjected to a limitation that AP should not belong to any floor or outdoor area. If the AP is already assigned to a floor or outdoor area, then the standby bucket holds the AP and when removed from the floor or outdoor, get positioned to the given floor. One Mac address cannot be put into bucket for multiple floor or outdoor areas.

Step 4 The map synchronization works only if the AP is associated to a base radio MAC address and not to its Ethernet MAC address.

What Does the Wireless Site Map Editor Do?

You use the map editor to define, draw, and enhance floor plan information. The map editor allows you to create obstacles so that they can be taken into consideration while computing RF prediction heatmaps for access points. You can also add coverage areas for location appliances that locate clients and tags in that particular area.

The planning mode opens the map editor in the browser window from which the planning tool is launched. If the original browser window has navigated away from the floor page, you need to navigate back to the floor page to launch the map editor.

- Guidelines for Using the Map Editor
- Guidelines for Placing Access Points
- Guidelines for Inclusion and Exclusion Areas on a Floor
- Opening the Map Editor
- Map Editor Icons
- Using the Map Editor to Draw Coverage Areas
- Using the Map Editor to Draw Obstacles
- Defining an Inclusion Region on a Floor
- Defining an Exclusion Region on a Floor
- Defining a Rail Line on a Floor

Guidelines for Using the Wireless Site Map Editor

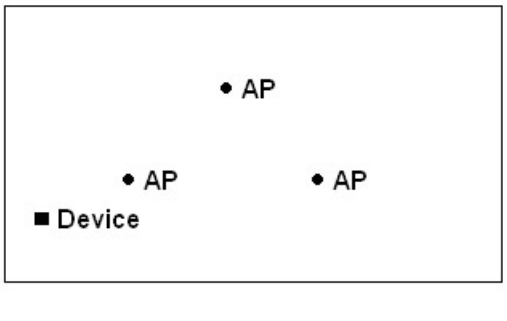
Consider the following when modifying a building or floor map using the map editor:

- We recommend that you use the map editor to draw walls and other obstacles rather than importing an FPE file from the legacy floor plan editor.
- If necessary, you can still import FPE files. To do so:
  1. Navigate to the desired floor area.
  2. Choose Select a command > Edit Floor Area > Go.
  3. Select the FPE File check box.
  4. Browse to the FPE file and click OK.
- You can add any number of walls to a floor plan with the map editor. However, the processing power and memory of a client workstation may limit the refresh and rendering aspects of Prime Infrastructure.
- We recommend a practical limit of 400 walls per floor for machines with 1 GB RAM or less.
- All walls are used by Prime Infrastructure when generating RF coverage heatmaps.

Guidelines for Placing Access Points

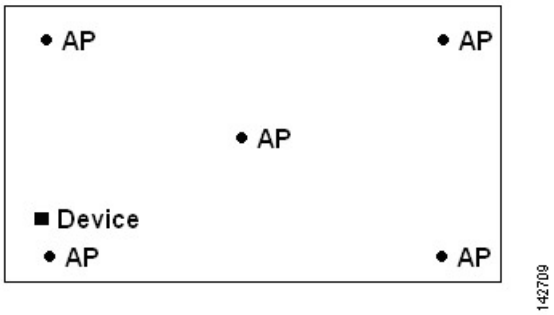
Place access points (APs) along the periphery of coverage areas to keep devices close to the exterior of rooms and buildings. Access points placed in the center of these coverage areas provide good data on devices that would otherwise appear equidistant from all other APs.

Figure 2: Access Points Clustered Together



By increasing overall AP density and moving APs towards the perimeter of the coverage area, location accuracy is greatly improved.

Figure 3: Improved Location Accuracy by Increasing Density



In long and narrow coverage areas, avoid placing APs in a straight line. Stagger them so that each AP is more likely to provide a unique snapshot of a device location.

Figure 4: Refrain From Straight Line Placement

Although the design in might provide enough AP density for high bandwidth applications, location suffers because each AP view of a single device is not varied enough; therefore, location is difficult to determine.

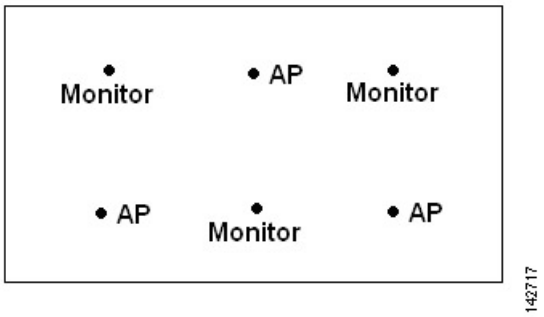
Move the APs to the perimeter of the coverage area and stagger them. Each has a greater likelihood of offering a distinctly different view of the device, resulting in higher location accuracy.

Figure 5: Improved Location Accuracy by Staggering Around Perimeter

Most current wireless handsets support only 802.11b/n, which offers only three non-overlapping channels. Therefore, wireless LANs designed for telephony tend to be less dense than those planned to carry data. Also, when traffic is queued in the Platinum QoS bucket (typically reserved for voice and other latency-sensitive traffic), lightweight APs postpone their scanning functions that allow them to peak at other channels and collect, among other things, device location information. The user has the option to supplement the wireless LAN deployment with APs set to monitor-only mode. Access points that perform only monitoring functions do not provide service to clients and do not create any interference. They simply scan the airwaves for device information.

Less dense wireless LAN installations, such as voice networks, find their location accuracy greatly increased by the addition and proper placement of monitor APs.

Figure 6: Less Dense Wireless LAN Installations



Verify coverage using a wireless laptop, handheld, or phone to ensure that no fewer than three APs are detected by the device. To verify client and asset tag location, ensure that the Prime Infrastructure reports client devices and tags within the specified accuracy range (10 m, 90%).

If you have a ceiling-mounted AP with an integrated omni-directional antenna, the antenna orientation does not really need to be set in Prime Infrastructure. However, if you mount that same AP on the wall, you must set the antenna orientation to 90 degrees.

Guidelines for Placing Inclusion and Exclusion Areas on a Floor Map

Inclusion and exclusion areas can be any polygon shape and must have at least three points.

You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor area when it is created. The inclusion region is indicated by a solid aqua line, and generally outlines the entire floor area.

You can define multiple exclusion regions on a floor area.

Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Launch and Use the Wireless Site Map Editor

Follow these steps to use the map editor:

Step 1 Choose Maps > Site Maps.

Step 2 Select the desired campus and building.

Step 3 Click the desired floor area. The Site Maps > Campus Name > Building Name > Floor Area Name page appears.

Step 4 Choose Select a command > Map Editor > Go. The Map Editor page appears.

Make sure that the floor plan images are properly scaled so that all white space outside of the external walls is removed. To make sure that floor dimensions are accurate, click the compass tool.

Step 5 Position the reference length. The Scale Floor menu appears with the line length supplied. Enter the dimensions (width and height) of the reference length, then click OK.

Step 6 Determine the propagation pattern from the Antenna Mode drop-down list.

Step 7 Make antenna adjustments by sliding the antenna orientation bar to the desired degree of direction.

Step 8 Choose the desired access point.

Step 9 Click Save.

Wireless Site Map Editor Icons

Table 22: Wireless Site Map Editor Icons

Icon	Description
	Scale Floor—Click anywhere on the map to start drawing a line. Double click to finish the line and enter the new line length in the popup shown. This will modify the floor dimensions to the new dimensions.
	Measure Distance—Click anywhere on the map to start drawing a line. Double click to finish the line. The line length in feet/meters is shown at the top.
	Copy/Move Obstacles—Select obstacles either by drawing a box on the map or by clicking the obstacles. To copy obstacles, click Copy. This will create new obstacles just above the selected obstacles. To move the obstacles, drag the selected obstacles to a new position. Clicking anywhere on the map will unselect all the elements.
	Delete Mode—Select the elements to be deleted either by drawing a box on the map or clicking each element. Use the **Shift** key to select multiple elements. Use the **Ctrl** key to toggle selection of elements, one at a time. Clicking anywhere on the map will unselect all the elements. Click Delete to delete the selected elements
	Modify Mode—Click an element and click the vertices to reshape or drag the element to a new position. Clicking anywhere on the map will unselect the selected element.
	Draw Coverage Area
	Draw Location Region
	Draw Rail
	Draw Obstacle—Click anywhere on the map to start drawing. Double click to finish drawing. Use Ctrl-z to undo, Ctrl-y to redo and 'Esc' key to cancel the current drawing.
	Place Marker
	Navigation—Remove any selected modes such as drawing or editing and switches to navigation mode where you can view the map and perform zooming or panning.

Define Coverage Areas in Wireless Site Maps

If you have a building that is non-rectangular or you want to mark a non-rectangular area within a floor, you can use the map editor to draw a coverage area.

Step 1 Add the floor plan if it is not already represented in Prime Infrastructure.

Step 2 Choose Maps > Site Maps.

Step 3 Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.

Step 4 Choose Select a command > Map Editor > Go. The Map Editor page appears.

Step 5 Click the Draw Coverage Area icon on the toolbar.

A pop-up appears.

Step 6 Enter the name of the area that you are defining, then click OK.

A drawing tool appears.

Step 7 Move the drawing tool to the area you want to outline.

- Click the left mouse button to begin and end drawing a line.
- When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.

The outlined area must be a closed object to appear highlighted on the map.

Step 8 Click the disk icon on the toolbar to save the newly drawn area.

Obstacle Color Coding in Wireless Site Maps

The following table describes the color coding applied to obstacles on wireless site maps, as well as the estimated signal loss used to calculate RF signal strength in the vicinity of these obstacles.

Table 23: Obstacle Color Coding

Type of obstacle	Color coding	Signal Loss (in dB)
Thick wall		13
Light wall		2
Heavy door		15
Light door		4
Cubicle		1
Glass		1.5

Define Inclusion Regions in Wireless Site Maps

To help refine device location information displayed on a floor area in a wireless site map, you can define the regions that you want included (inclusion regions) in location data and regions that you do not want included (exclusion regions). For example, you might want to exclude common areas (such as an atrium or stairwells within a building), but include work areas (such as cubicles, labs, or manufacturing floors).

By default, Prime Infrastructure defines an inclusion region for each newly added floor. When you define a new inclusion region, any previously defined inclusion region is automatically removed. An inclusion region is indicated by a solid aqua line outlining the region.

Step 1 Choose Maps > Site Maps.

Step 2 Click the name of the appropriate floor area.

Step 3 Choose Select a command > Map Editor > Go.

Step 4 On the map, click the aqua box on the toolbar.

A message box appears reminding you that only one inclusion area can be defined at a time.

Step 5 Click OK in the message box. A drawing icon appears to help you outline the inclusion area.

Step 6 To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

Step 7 Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.

Step 8 Repeat Step 7 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion region.

Step 9 Choose Save from the Command menu or click the disk icon on the toolbar to save the inclusion region.

If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 10 To return to the floor map to enable inclusion regions on heatmaps, choose Exit from the Command menu.

Step 11 Select the Location Regions check box if it is not already selected. To apply the changes to all floor maps, click Save settings.

Step 12 To resynchronize Prime Infrastructure and MSE databases, choose Services > Synchronize Services. If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change and there is no need for an explicit resynch.

Step 13 In the Synchronize page, choose Synchronize > Network Designs, then click OK. You can confirm that the synchronization is successful by viewing two green arrows in the Sync Status column.

Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Define Exclusion Regions in Wireless Site Maps

To refine location calculations on a floor, you can define regions that are excluded (exclusion regions) from the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion regions are generally defined within the borders of an inclusion region.

Step 1 Choose Maps > Site Maps.

Step 2 Click the name of the appropriate floor area.

Step 3 Choose Select a command > Map Editor > Go. The Map Editor page appears.

Step 4 At the map, click the purple box on the toolbar.

Step 5 Click OK in the message box that appears. A drawing icon appears to help you outline the exclusion region.

Step 6 To begin defining the exclusion region, move the drawing icon to the starting point on the map, and click once.

Step 7 Move the drawing icon along the boundary of the region you want to exclude. Click once to start a boundary line, and click again to end the boundary line.

Step 8 Repeat Step 7 until the region is outlined and then double-click the drawing icon. The defined exclusion region is shaded in purple when the region is completely defined.

Step 9 To define additional exclusion regions, repeat Step 5 to Step 8.

Step 10 When all exclusion regions are defined, choose Save from the Command menu or click the disk icon on the toolbar to save the exclusion region.

To delete an exclusion region, click the region to be deleted. The selected region is outlined by a dashed purple line. Next, click the X icon on the toolbar. The region is removed from the floor map.

Step 11 To return to the floor map to enable exclusion regions on heatmaps, choose Exit from the Command menu.

Step 12 Select the Location Regions check box if it is not already selected, click Save settings, and close the Layers configuration page when complete.

Step 13 To resynchronize Prime Infrastructure and location databases, choose Services > Synchronize Services.

Step 14 In the Synchronize page, choose Synchronize > Network Designs and then click Synchronize. You can confirm that the synchronization is successful by viewing the green arrows in the Sync. Status column.

Define Rail Lines in Wireless Site Maps

You can define rail lines on any floor area. Rail lines help you streamline location calculations and summarize the display of location data on wireless clients who are constantly on the move and for whom you do not require precise location data (such as for handheld wireless devices on a busy manufacturing floor area or outside construction site).

You can also define an area around the rail line known as the snap width. The snap width represents the area in which you expect roaming clients to appear. The snap-width represents the distance that is monitored on either side (either east/west or north/south) of the rail. Any client located within the snap-width area is either plotted directly on the rail line (the majority of roaming clients) or just outside of the snap-width area (minority).

Rail lines do not apply to tags. You can choose to define the snap-width area in either feet or meters.

Step 1 Choose Maps > Site Maps.

Step 2 Click the name of the appropriate floor area.

Step 3 Choose Select a command > Map Editor > Go. The Map Editor page appears.

Step 4 In the map, click the rail icon (to the right of the purple exclusion-area icon) on the toolbar.

Step 5 In the message dialog box that appears, enter a snap-width (feet or meters) for the rail and then click OK. A drawing icon appears.

Step 6 Click the drawing icon at the starting point of the rail line. Click again when you want to stop drawing the line or change the direction of the line.

Step 7 Click the drawing icon twice when the rail line is completely drawn on the floor map. The rail line appears on the map and is bordered on either side by the defined snap-width region.

To delete a rail line, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the X icon on the toolbar. The area is removed from the floor map.

Step 8 To return to the floor map to enable rails on heatmaps, choose Exit from the Command menu.

Step 9 With the floor map displayed, choose the Layers drop-down list.

Step 10 Select the Rails check box if it is not already selected, then click Save settings, and close the Layers configuration pane when complete.

Step 11 To resynchronize Prime Infrastructure and mobility services engine, choose Services > Synchronize Services.

Step 12 In the Synchronize page, choose Synchronize > Network Designs and then click Synchronize.

You can confirm that the synchronization is successful by viewing the green arrows in the Sync. Status column.

Search Wireless Site Maps

You can use the following parameters in the Search Maps page:

- Search for
- Map Name
- Search in
- Save Search
- Items per page

After you click Go, the map search results page appears, with the options shown in the following table.

Table 24: Wireless Site Map Search Results

Field	Options
Name	Clicking an item in the Name column provides a map of an existing building with individual floor area maps for each floor.
Type	Campus, building, or floor area.
Total APs	Displays the total number of Cisco Radios detected.
a/n Radios	Displays the number of 802.11a/n Cisco Radios.
b/g/n Radios	Displays the number of 802.11b/g/n Cisco Radios.

Adjust RF Antennas Using the Wireless Site Map Editor

Follow these steps to use the wireless site map editor to adjust RF antennas:

Step 1 Choose Maps > Site Maps.

Step 2 Click the campus containing the building and floor area you want. The Site Maps > Campus Name page appears.

Step 3 Click the building you want. The Site Maps > Campus Name>Building Name page appears.

Step 4 Click the floor area, basement level, or outside area you want. The Site Maps > Campus Name > Building Name > Floor Area Name page appears.

Step 5 Choose Select a command > Map Editor > Go. The Map Editor page appears.

Before proceeding, ensure that the floor area images are properly scaled, so that all white space outside of the external walls is removed. To ensure that floor dimensions are accurate, click the compass tool on the toolbar and then adjust as needed.

Step 6 Position the reference length. When you do, the Scale menu appears with the line length supplied. Enter the dimensions (width and height) of the reference length, then click OK.

Step 7 Determine the propagation pattern from the Antenna Mode drop-down list.

Step 8 Make antenna adjustments by sliding the antenna orientation bar to the desired degree of direction.

Step 9 Choose the desired access point.

Step 10 Click Save.

Locate Low-Coverage Areas Using AP Location Readiness

You can configure Prime Infrastructure to verify the ability of the existing access point (AP) deployment to estimate the true location of a client, rogue client, rogue AP, or tag within 10 meters at least 90 percent of the time. The location readiness calculation is based on the number and placement of APs. The Inspect Location Readiness feature is a distance-based predictive tool that can point out problem areas with AP placement.

To access the Inspect Location Readiness tool, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Click the applicable floor area name to view the map.

If RSSI is not displayed, you can enable AP Heatmaps by selecting the AP Heatmaps check box on the left sidebar menu.

If clients, tags, and APs are not displayed, verify that their respective check boxes are selected on the left sidebar menu. Licenses for both clients and tags must also be purchased for each to be tracked.

Step 3 Choose Select a command > Inspect Location Readiness > Go.

A color-coded map appears, showing those areas that meet (indicated by "Yes") or do not meet ("No") the 10-meter, 90-percent location specification.

Assess the Quality of AP Coverage Using RF Calibration Data

After completing a RF calibration model based on data points generated during a physical tour of the area (see the related topic, "Calibrate, Compute and Apply New RF Calibration Models"), you can inspect the location quality of the access points (APs). The assessment of a given location’s ability to meet the location

accuracy specification (that is: within 10 meters, 90 percent of the time) will be based on data points gathered during physical inspection and calibration.

To inspect location quality based on calibration, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Choose Select a command > RF Calibration Model > Go. A list of RF calibration models appears.

Step 3 Click the appropriate RF calibration model.

Details on the RF calibration model are displayed. These include: the date of last calibration, number of data points by signal type (802.11a, 802.11 b/g) used in the calibration, location, and coverage.

Step 4 Under the Calibration Floors heading, click the Inspect Location Quality link. Prime Infrastructure displays a color-coded map giving the percentage of location errors. You can modify the distance selected to see the effect on the location errors.

Determine If RF Coverage is Sufficient for Voice Readiness

The VoWLAN Readiness (voice readiness) tool allows you to check the RF coverage to determine if it is sufficient for your voice needs. This tool verifies RSSI levels after access points (APs) have been installed.

To access the VoWLAN Readiness Tool (VRT), follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Click the name of the floor area, outside area, or basement level you want to inspect for voice readiness.

Step 3 From the Select a command > Inspect VoWLAN Readiness > Go.

Step 4 Choose the applicable Band, AP Transmit Power, and Client parameters from the drop-down lists.

By default, the region map displays the b/g/n band for Cisco Phone-based RSSI thresholds. Any new settings cannot be saved. Depending on the selected client, the following RSSI values may not be editable:

- Cisco Phone—RSSI values are not editable.
- Custom—RSSI values are editable within the following ranges:
  - Low threshold between -95dBm to -45dBm
  - High threshold between -90dBm to -40dBm

Step 5 Examine the map for problem areas. The map is color-coded as follows:

- Green—Voice ready
- Yellow—Marginal
- Red—Not Voice ready

The accuracy of the Green/Yellow/Red region color-coding depends on the RF environment and whether or not the floor area map has been calibrated (for details on this, see the related topic "Calibrate, Compute and Apply New RF Calibration Models"). If the floor area map is calibrated, the accuracy of the region coding will be enhanced.

Step 6 You can troubleshoot areas with poor or no coverage by adjusting the AP Transmit Power setting, as follows:

- Set the AP Transmit Power field to "Max" (the maximum downlink power settings). If the map still shows some yellow or red regions, more APs are probably required to provide full VoWLAN coverage.
- Set the AP Transmit Power field to "Current". If the calibrated model shows red or yellow regions where voice will be deployed, increasing the power level of the APs may help.

Show Wired Device Info

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Tools at the upper right corner of the page, and click Show Wired Device Info.

A pop-up page appears which contains the following information:

- Summary and details about wired switches
- Summary and details about wired clients

Step 4 Click Ok to return to close the window.

Configure Interferer Notification

Step 1 Choose Maps > Site Maps (New).

Step 2 From the Domain Navigator left sidebar menu, select the applicable floor to open the floor view page.

Step 3 Click Tools at the upper right corner of the page, and click Configure Interferer Notification.

Step 4 In the Interferer CAS Notification Configuration window, check the check box(es) of the device for which you want a notification to be generated:

- Bluetooth Link
- Microwave Oven
- 802.11FH
- Bluetooth Discovery
- TDD Transmitter
- Jammer
- Continuous Transmitter
- DECT Like Phone
- Video Camera
- 802.15.4
- WiFi Inverted
- WiFi Invalid Channel
- SuperAG
- Radar

- Canopy
- Xbox
- WiMAX Mobile
- WiMAX Fixed

Step 5 Click Save.

Show/Hide

Click Tools at the upper right corner of the page, and click Show/Hide to show or hide the grid that displays distance in feet on the map.

Export to PDF

Click Tools at the upper right corner of the page, and click Export to PDF to export floor plan as a PDF.

Measure Distances

Step 1 Click Tools at the upper right corner of the page, and click Measure Distance.

Step 2 Click anywhere on the map to start drawing line. Measured line length in feet is shown in the tool tip.

Data Filtering

Filtering Access Points Data

The access point filtering options include the following:

- Choose the radio type: 2.4 GHz or 5 GHz.
- Click Add Rule to add a query:
  - Choose the access point identifier you want to view on the map: Name, MAC Address, Tx Power, Channel, Avg Air Quality, Min. Air Quality, Controller IP, Coverage Holes, Tx Utilization, Rx Utilization, Profiles, CleanAir Status, Associated Clients, Dual-Band Radios, Radio, or Bridge Group Name.
  - Choose the parameter by which you want to filter the access point.
  - Type the specific filter criteria in the text box for the applicable parameters, and click Go. The access point search results appear.
  - Click Apply Filter to view the filter results on map.

When you hover your mouse cursor over the search result in the table, the location of the AP gets pointed with a line on the map.

Filtering Clients Data

The Clients filter option appears if an MSE is added in to Cisco Prime Infrastructure. The Clients filtering options include the following:

- Click Add Rule to add a query:
  - Choose the client identifier you want to view on the map: IP Address, User Name, MAC Address, Asset Name, Asset Group, Asset Category, Controller, SSID, Protocol, or State.
  - Type the specific filter criteria in the text box for the applicable parameters, and click Go. The clients search results appear in the table.
  - Click Apply Filter to view the filter results on map.

If there are multiple IPv6 addresses for a client, then you can specify any one IP address to uniquely identify the client.

When you hover your mouse cursor over the search result in the table, the location of the client gets pointed with a line on the map.

Filtering Tags Data

The tag filtering options include the following:

- Choose a tag identifier you want to view on the map: MAC Address, Asset Name, Asset Group, Asset Category, or Controller.
- Choose the parameter by which you want to filter the tag. Once selected, type the specific device in the text box. Click Go. The search results appear in the table.
- Click Apply Filter to view the filter results on maps.

Filtering Rogue AP Data

Click Apply Filter to view the filter results on maps.

- Choose the Rogue AP identifier you want to view on the map: MAC Address, Classification Type, or State.
- Choose the State—Use the drop-down list to choose from Alert, Authenticated, Associated, Idle, Pending, or Probing.
  - Classification Type—Enter the classification type in the text box.
  - Click Go. The search results appear in the table.
- Click Apply Filter to view the filter results on maps.

Filtering Adhoc Rogues Data

The Rogue Adhoc filter dialog appears that contains these parameters:

- MAC Address—If you want to view a particular MAC address, enter it in the MAC Address text box.
- State—Use the drop-down list to select from Alert, Known, Acknowledged, Contained, Threat, or Unknown contained states.
- On Network—Use the drop-down list to specify whether or not you want to display rogue adhocs on the network.
- Click Go. The search results appear in the table.
- Click Apply Filter to view the filter results on maps.

Filtering Interferer Data

If you enable Interferer floor setting and then click the blue arrow to the right, the Interferers filter dialog box appears. Interferer filtering options include the following:

- Interferer Status
- Interferer Type
- Click OK when all applicable filtering criteria are selected.

Filtering Access Points Heatmap Data

An RF heatmap is a graphical representation of RF wireless data where the values taken by variables are represented in maps as colors. The current heatmap is computed based on the RSSI prediction model, Antenna Orientation, and AP transmit power.

f you enable the Access Point Heatmap floor setting and click the blue arrow to the right of the Floor Settings, the Contributing APs dialog appears with heatmap filtering options.

Prime Infrastructure introduces dynamic heatmaps. When dynamic heatmaps are enabled, the Prime Infrastructure recomputes the heatmaps to represent changed RSSI values.

Access point heatmap filtering options include the following:

- Heatmap Type
  - Coverage—If you have monitor mode access points on the floor plan, you have a choice between IDS or coverage heatmap types. A coverage heatmap excludes monitor mode access points.

Note The coverage overage area heatmap shows the span of the signal (in terms of area) and intensity of the signal. The RSSI cutoff is the lowest value of RSSI in dBM which is considered a usable signal and it is shown in dark blue color. RSSI cutoff value in rendering heat map, identifies the span over which the signal is higher than the specified RSSI cutoff value.

- Air Quality—Not applicable for XOR Monitor mode radios. If you choose Air Quality, you can further filter the heat map type for access points with average air quality or minimum air quality. Select the appropriate radio button. It displays heatmaps for radios operating in client serving mode. Cisco Aironet 2800 and 3800 Series APs operate with Fixed-A band and XOR 2.4 GHz or XOR 5.4 GHz mode radios.
- IDS—Available only for radios operating in monitor mode. IDS heatmap option is displayed only if there is at least one AP in the floor in the monitor mode or at least one XOR radio in the monitor mode.

Note Only APs in Local, FlexConnect, or Bridge mode can contribute to the Coverage and Air Quality Heatmap.

- Show only XOR—Displays heatmaps only for the XOR radios. With this you can differentiate between the heatmaps for fixed and dual band radios.
- Total APs—Displays the number of access points positioned on the map.
- Select the access point check box(es) to determine which heatmaps are displayed on the image map.

Click OK when all applicable filtering criteria are selected.

Use Planning Mode to Help Place APs in Wireless Site Maps

You can calculate the recommended number and location of access points (APs) based on any combination of data traffic, voice traffic, and location.

Based on the throughput specified for each protocol (802.11a or 802.11 b/g), planning mode calculates the total number of APs required to provide optimum wireless coverage in your network.

Planning Mode options include:

- Add APs—Enables you to add APs to a map. See the related topic "Use Planning Mode to Calculate Access Point Coverage Requirements" for details.
- Delete APs—Deletes the selected APs.
- Map Editor—Opens the Map Editor window.
- Synchronize with Deployment—Synchronizes your planning mode APs with the current deployment scenario.
- Generate Proposal—View a planning summary of the current APs deployment.
- Planned AP Association Tool—Allows you to perform add, delete or import an AP Association from an excel or CSV file. Once an AP is defined, it can be associated to a base radio MAC address using the Planned AP Association Tool. If the AP is not discovered they get pushed into a standby bucket and get associated when discovered.

  AP association works only if AP does not belong to any floor or outdoor area. If the AP is already assigned to a floor or outdoor area, then the standby bucket holds the AP; when the AP is removed from the floor

or outdoor area, it will be positioned to the given floor. One Mac address cannot be put into bucket for multiple floor or outdoor areas.

Map synchronizations work only if the AP is associated to a base radio MAC address and not to its Ethernet MAC address.

Planning mode does not use AP type or Antenna pattern information for calculating the number of APs required. The calculation is based on the AP coverage area or the number of users per AP.

Step 1 Choose Maps > Site Maps.

Step 2 Choose the desired campus, building, and floor area.

Step 3 Choose Select a command > Planning Mode > Go.

Use Planning Mode to Calculate Access Point Coverage Requirements

Prime Infrastructure planning mode lets you calculate the number of access points (APs) required to cover an area by placing fictitious APs on a map and viewing the coverage area. Based on the throughput specified for each protocol (802.11a/n or 802.11b/g/n), planning mode calculates the total number of APs required to provide optimum coverage in your network. You can calculate the recommended number and location of APs based on the following criteria:

- Traffic type active on the network: data or voice traffic or both
- Location accuracy requirements
- Number of active users
- Number of users per square foot

Step 1 Choose Maps > Site Maps.

Step 2 Choose the desired campus, building, and floor area. A color-coded map appears showing all elements (APs, clients, tags) and their relative signal strength.

Step 3 Choose Select a command > Planning Mode > Go. A blank floor area map appears.

Step 4 Click Add APs.

In the page that appears, drag the dashed-line rectangle around the area of the map for which you want to calculate the total number of recommended APs.

Adjust the size or placement of the rectangle by selecting the edge of the rectangle and holding down the **Ctrl** key. The rectangle is resizable by dragging on the handles on its edges and corners.

Step 5 From the Add APs drop-down list, choose Automatic.

Step 6 Choose the AP Type and the appropriate antenna and protocol for the selected AP.

Step 7 Choose the target throughput for the AP.

Step 8 Select the check box(es) next to the service(s) used on the floor. You must select at least one service.

Step 9 Select the Advanced Options check box to select the following AP planning options:

- Demand and Override Coverage per AP

- Safety Margin (for the Data/Coverage and Voice safety margin options)

Step 10 Click Calculate.

The recommended number of APs for the selected parameters appears. Recommended calculations assume the need for consistently strong signals unless adjusted downward by the safety margin advanced option. In some cases, the recommended number of APs will be higher than the amount actually required.

Walls are not used or accounted for in planning mode calculations.

Step 11 Click Apply to generate a map showing the proposed deployment of the recommended APs in the selected area.

Step 12 Choose Generate Proposal to display a textual and graphical report of the recommended AP number and deployment based on the given inputs.

Configure Refresh Settings for Wireless Site Maps

Prime Infrastructure provides various refresh options for wireless site maps:

- Load—Refreshes map data from the Prime Infrastructure database on demand.
- Auto Refresh—Provides an interval drop-down list to set how often to refresh the map data from the database.
- Refresh from network—Refreshes the map status and statistics directly from the controller through an SNMP fetch rather than polled data from the Prime Infrastructure database.
- Refresh browser—Refreshes the complete page, or refreshes the map and its status and statistics if you are on a map page.

If you have monitor mode access points on the floor plan, you have a choice between IDS or coverage heatmap types. A coverage heatmap excludes monitor mode access points, and an IDS heatmap includes them.

How RF Heatmaps are Calculated

A radio frequency heat map is a graphical representation of the strength of the RF signals generated by Wi-Fi access points covering a floor area, basement level. Because WLANs are very dynamic and nondeterministic in nature, administrators can never be certain of the coverage at any one spot at a particular moment. To help combat this challenge, Prime Infrastructure provides a map of your floor plan along with visual cues as to the Wi-Fi coverage on the floor. These maps are called heatmaps because they are similar to the colored maps used to show varying levels of heat in oceanography or geographical sciences. Color is used to show the various levels of signal strength. The different shades in the heatmap reflect differing RF signal strengths.

This color visualization provides a quick view of the current state of coverage (without having to walk around measuring it), the signal strength, and any gaps or “holes” in the WLAN. This enhances the speed and ease with which you support your organization and troubleshoot specific problems.

The RF heatmap calculation is based on an internal grid. Depending on the exact positioning of an obstacle in that grid, the RF heatmap, within a few feet or meters of the obstacle, might or might not account for the obstacle attenuation. The RF prediction heatmaps for access points approximates the actual RF signal intensity. It takes into account the attenuation of obstacles drawn using the Map Editor but it does not take into account the attenuation of various building materials, such as drywall or metal objects, nor does it display the effects

of RF signals bouncing off obstructions. The thick wall (color-coded orange) with a loss of 13 dB might not be enough to contain the RF signal beyond the walls of the heatmap.

In detail, grid squares partially affected by an obstacle crossing the grid square might or might not incorporate the obstacle attenuation according to the geometry of the access point, obstacle, and grid.

For example, consider a wall crossing one grid square. The midpoint of the grid square is behind the wall from the AP, so the whole grid square is colored with attenuation, including (unfortunately) the top left corner that is actually in front of the wall.

The midpoint of the grid square is on the same side of the wall as the AP, so the whole grid square is not colored with attenuation, including (unfortunately) the bottom right corner that is actually behind the wall from the AP.

The RF heatmap calculation can be static or dynamic. By default, it is dynamic. The main purpose of the dynamic heatmap feature is to recompute the RF heatmaps due to obstacles. The Prime Infrastructure server maintains a current list of all APs' RSSI strengths. Prime Infrastructure uses neighboring APs' RSSI strength to modify the RF heatmaps for all APs.

To configure static heatmap calculation, you must disable the dynamic heatmap option in the map properties page.

Floor View Navigation Pane Tools

The main Floor View navigation pane provides access to multiple map functions and includes the following functionality:

- Zoom In/Zoom Out—Click the magnifying glass icon with the plus sign (+) to enlarge the map view. Click the magnifying glass icon with the minus sign (-) to decrease the size of the map view.
- Map Size—See the related topic "Pan and Zoom with Next Generation Maps".
- Show Grid—Click to show or hide the grid that displays distance in feet on the map.
- RSSI Legend—Hover your mouse cursor over the RSSI Legend icon to display the RSSI color scheme (ranging from red/-35 dBm to dark blue/-90 dBm).
- Add Access Points—Click to open the Add Access Points page. For more information, see the related topic "Add Access Points to a Floor Area".
- Remove Access Points—Click to open the Remove Access Points page. Select the access points that you want to remove and click OK.
- Position Access Points—Click to open the Position Access Points page.
- Add Chokepoints—Click to open the Add Chokepoints page. For more information, see the Cisco Context-Aware Services Configuration Guide.
- Add WiFi TDOA Receivers—Click to open the Add Wi-Fi TDOA Receivers page. For more information, see the Cisco Context-Aware Services Configuration Guide.
- Auto Refresh—From the drop-down list, choose the length of time between each system refresh.
- Refresh from Network—Click to initiate an immediate refresh of the current data.
- Planning Mode—Click to open the Planning Mode window.
- Map Editor—Click to open the Map Editor.

- Full Screen—Click to increase the size of the map to full screen. Once there, click Exit Full Screen to return to the normal view.

Create Wireless Site Maps Using Automatic Hierarchy Creation

Before you begin

Automatic Hierarchy Creation uses regular expressions to help you create wireless site maps and assign access points (APs) to them quickly and easily. To use this feature, you must first:

- Create a naming pattern for your wireless APs. This AP naming pattern must include the names of the campuses and buildings, and the names of the floor areas, basements, and outdoor areas, that you have either created or plan to create for your wireless site maps. If you have already created these wireless site maps, the names you use in your wireless AP naming pattern must match those used for your wireless site maps (including spelling and capitalization). You will also want to select a delimiter character to separate the parts of the AP naming pattern. For example: If you have a campus named "San Jose", a building named "01", a floor area named "GroundFloor", and an AP on that floor named "AP3500il", you might creating naming pattern for APs like this: "San Jose-01-GroundFloor-AP3500i1".
- You have already used Prime Infrastructure to discover your APs and wireless LAN controllers, and have renamed the APs using your naming pattern.

Warning It is recommended that you take a maps backup before proceeding, as you cannot revert changes made in the maps location info.

Step 1 Choose Maps > Automatic Hierarchy Creation to display the Automatic Hierarchy Creation page.

Step 2 Enter the name of an AP on your network in the text box, or choose one from the list.

This name is used to create a regular expression to create your maps.

To update a previously created regular expression, click Load and Continue next to the expression and update the expression accordingly. To delete a regular expression, click Delete next to the expression.

Step 3 Click Next.

Step 4 If your AP‘s name has a delimiter, enter it in the text box and click Generate basic regex based on delimiter. The system generates a regular expression that matches your AP’s name based on the delimiter.

For example, using the dash (-) delimiter in the AP name San Jose-01-GroundFloor-AP3500i1, produces the regular expression /(.*)-(.*)-(.*)-(.*)/. If you have a more complicated AP name, you can manually enter the regular expression.

You are not required to enter the leading and trailing slashes.

As a convention, Prime Infrastructure displays regular expressions in slashes.

Step 5 Click Test. The system displays the maps that will be created for the AP name and the regular expression entered.

Step 6 Using the Group fields, assign matching groups to hierarchy types.

For example, if your AP is named: SJC14-4-AP-BREAK-ROOM

In this example, the campus name is SJC, the building name is 14, the floor name is 4, and the AP name is AP-BREAK-ROOM.

Use the regular expression: /([A-Z]+)(\d+)-(\d+)-(.*)/

From the AP name, the following groups are extracted:

a. SJC

b. 14

c. 4

d. AP-BREAK-ROOM

The matching groups are assigned from left to right, starting at 1.

To make the matching groups match the hierarchy elements, use the drop-down list for each group number to select the appropriate hierarchy element.

This enables you to have almost any ordering of locations in your AP names.

For example, if your AP is named: EastLab-Atrium2-3-SanFrancisco

If you use the regular expression: /(.*)-(.*)-(.*)-(.*)/

with the following group mapping:

a. Building

b. Device Name

c. Floor

d. Campus

Automatic Hierarchy Creation produces a campus named SanFrancisco, a building under that campus named EastLab, and a floor in EastLab named 3.

The two hierarchy types, Not in device name and Device have no effect, but enable you to skip groups in case you need to use a matching group for some other purpose.

Automatic Hierarchy Creation requires the following groups to be mapped in order to compute a map on which to place the AP:

Campus group present in match?	Building group present in match?	Floor group present in match?	Resulting location
Yes	Yes	Yes	Campus > Building > Floor
Yes	Yes	No	Failed match
Yes	No	Yes	Campus > Floor (where Floor is an outdoor area)
Yes	No	No	Failed match
No	Yes	Yes	System Campus > Building > Floor
No	Yes	No	Failed match

Campus group present in match?	Building group present in match?	Floor group present in match?	Resulting location
No	No	Yes	Failed match
No	No	No	Failed match

Automatic Hierarchy Creation attempts to guess the floor index from the floor name. If the floor name is a number, AHC will assign the floor a positive floor index. If the floor name is a negative number or starts with the letter B (for example, b1, -4, or B2), AHC assigns the floor a negative floor index. This indicates that the floor is a basement.

When searching for an existing map on which to place the AP, AHC considers floors in the AP's building with the same floor index as the AP's name.

For example, if the map SF > MarketStreet > Sublevel1 exists and has a floor index of -1, then the AP SF-MarketStreet-b1-MON1 will be assigned to that floor.

Step 7 Click Next. You can test against more APs. You may test your regular expression and matching group mapping against more APs by entering the AP names in the Add more device names to test against field, and clicking Add.

You then click Test to test each of the APs names in the table. The result of each test is displayed in the table.

If required, return to the previous step to edit the regular expression or group mapping for the current regular expression.

Step 8 Click Next, then click Save and Apply. This applies the regular expression to the system. The system processes all the APs that are not assigned to a map.

You can edit the maps to include floor images, correct dimensions, and so on. When Automatic Hierarchy Creation creates a map, it uses the default dimensions of 20 feet by 20 feet. You will need to edit the created maps to specify the correct dimensions and other attributes.

Maps created using Automatic Hierarchy Creation appear in the maps list with an incomplete icon. Once you have edited a map, the incomplete icon disappears. You may hide the column for incomplete maps by clicking the Edit View link.

View Google Earth Maps in Wireless Site Maps

You must have Google Earth installed on your computer and configured to auto-launch when data is sent from the server.

Google Earth uses SSL 3.0 for communication. But in Cisco Prime Infrastructure 3.2 Release by default it supports only TLSv1.2. You must perform these steps if you want Google Earth support:

- Do ssh login to Cisco Prime Infrastructure server with admin privileges.
- Use the ncs run set-tls-versions <tls-versions> command to enable the required TLS version. For example, to enable TLSv1.2, TLSv1.1 and TLSv1.0, issue the following command: prime-server/admin# ncs run tls-server-versions TLSv1.2 TLSv1.1 TLSv1
- Restart the application

To view Google Earth Maps in Wirelss Site Maps:

Step 1 Choose Maps > Google Earth. The Google Earth Maps page displays all folders and the number of access points included within each folder.

Step 2 Click Launch for the map you want to view. Google Earth opens in a separate page and displays the location and its access points.

View Google Earth Map Details in Wireless Site Maps

To view details for a Google Earth Map folder, follow these steps:

Step 1 Choose Maps > Google Earth.

Step 2 Click the folder name to open the details page for this folder. The Google Earth Details provide the access point names and MAC or IP addresses.

Step 3 To delete an access point, select the applicable check box and click Delete.

Step 4 To delete a folder, select the check box next to the folder name, then click Delete. Deleting a folder also deletes all subfolders and access points inside the folder.

Step 5 Click Cancel to close the details page.

Use Geographical Coordinates to Group APs into Outdoor Locations on Wireless Site Maps

To group access points together into outdoor locations, use the Latitude/Longitude geographical coordinates for each access point. You first need to create the required access point geographical coordinates, which you can then import into Prime Infrastructure. You can create either of the following file types to provide the coordinates:

- A KML (Google Keyhole Markup Language) File
- A CSV File (Spreadsheet format with comma-separated values)

Prerequisites for Creating Outdoor Locations Using Geographical Coordinates

You must provide the following geographical information for each access point. You can create the geographical coordinates in Google Earth and then import them into Prime Infrastructure. If you add an AP to a Google Earth map without having the AP associated on a standard map, you will not see a heatmap when you view the AP in Google Earth.

- Longitude (East or West)—Angular distance in degrees relative to Prime Meridian. Values west of Meridian range from –180 to 0 degrees. Values east of Meridian range from 0 to 180 degrees. The default is 0.

  Coordinates in degrees, minutes, seconds, direction:

  - Degrees (–180 to 180)

- Minutes (0 to 59)
- Seconds (00.00 to 59.99)
- Direction—East or West (E, W)

Decimal format (converted from degrees, minutes, and seconds).

- Longitude can range from –179.59.59.99 W to 179.59.59.99 E.

- Latitude (North or South)—Angular distance in degrees relative to the Equator. Values south of the Equator range from –90 to 0 degrees. Values north of the Equator range from 0 to 90 degrees. The default is 0.

  Coordinates in degrees, minutes, seconds, direction:

  - Degrees (–90 to 90)
  - Minutes (0 to 59)
  - Seconds (00.00 to 59.99)
  - Direction—North or South (N, S)

  Decimal format (converted from degrees, minutes, and seconds):

  - Latitude can range from –89.59.59.99 S to 89.59.59.99 N

- Altitude—Height or distance of the access point from the surface of the earth in meters. If not provided, value defaults to 0. Values range from 0 to 99999.
- Tilt—Values range from 0 to 90 degrees (cannot be negative). A tilt value of 0 degrees indicates viewing from directly above the access point. A tilt value of 90 degrees indicates viewing along the horizon. Values range from 0 to 90. The default azimuth angle is 0.
- Range—Distance in meters from the point specified by longitude and latitude to the point where the access point is being viewed (the Look At position) (camera range above sea level). Values range from 0 to 999999.
- Heading—Compass direction in degrees. The default is 0 (North). Values range from 0 to ±180 degrees.
- Altitude Mode—Indicates how the <altitude> specified for the Look At point is interpreted.
  - Clamped to ground—Ignores the <altitude> specification and places the Look At position on the ground. This is the default.
  - Relative to ground—Interprets the <altitude> as a value in meters above the ground.
  - Absolute—Interprets the <altitude> as a value in meters above sea level.
- Extend to ground—Indicates whether or not the access point is attached to a mast.

Use Google Earth to Import Geographical Coordinates Into Outdoor Locations On Wireless Site Maps

You can create the geographical coordinates in Google Earth and then import them into Prime Infrastructure. You can create either a folder or individual placemarks. Creating a folder helps group all the Placemarks into a single folder and allows you to save the folder as a single KML (a.k.a. XML) file. KML is a file format used to display geographic data in Google Earth. If you create individual Placemarks, you must save each Placemark individually.

Using a KML file, folders can be created hierarchically to any depth. For example, you can create folders and placemarks organized by country, city, state, zip. In CSV files, there is one level of hierarchy only.

Step 1 Launch Google Earth.

Step 2 In the Places page on the left sidebar menu, choose My Places or Temporary Places.

Step 3 Right-click Temporary Places and select Add > Folder from the drop-down lists.

Step 4 Enter the required information.

If you specify View coordinates (latitude, longitude, range, heading, and tilt), this information is used to "fly" or advance to the correct location when Google Earth is first loaded. If you do not specify View coordinates, the latitude and longitude information is derived using the minimum and maximum latitude and longitude of all access points within the specified group or folder.

Step 5 Click OK.

After the folder is created, you can select it from the Places page to create Placemarks.

Create Placemarks for KML Files Used in Wireless Site Maps

To create Placemarks, follow these steps:

Step 1 Launch Google Earth.

Step 2 In the Places page on the left sidebar, select My Places or Temporary Places.

Step 3 Select the folder that you previously created.

Step 4 Right-click your created folder and select Add > Placemark from the drop-down lists.

Step 5 Complete the required fields. For more information regarding Google Earth, see the Google Earth online help.

The Placemark name must contain the name, MAC address (the radio MAC not Ethernet MAC), or IP address of the appropriate access point.

Step 6 Click Snapshot current view or click Reset to return the coordinates to the original settings.

Step 7 Click OK.

Step 8 Repeat these steps for all placemarks you want to add.

Step 9 When all placemarks are created, save the folder as a .kmz file (KML Zip file) or as a .kml file. You can import both .kmz and .kml files into Prime Infrastructure.

Create CSV Files to Import Geographical Coordinates Into Wireless Site Maps

You can create a CSV file that contains the required access point geographical coordinates, and then import the CSV file into Prime Infrastructure.

Step 1 Using a text editor, create a new file that provides the necessary fields, separated by commas, as described in the following table.

Table 25: Sample Fields for Geographical Coordinates CSV File

“FolderName”	“Value Optional”	Max Length: 32
“FolderState”	“Value Optional”	Permitted Values: true/false
“FolderLongitude”	“Value Optional”	Range: 0 to ±180
“FolderLatitude”	“Value Optional”	Range: 0 to ±90
“FolderAltitude”	“Value Optional”	Range: 0 to 99999
“FolderRange”	“Value Optional”	Range: 0 to 99999
“FolderTilt”	“Value Optional”	Range: 0 to 90
“FolderHeading”	“Value Optional”	Range: 0 to ±180
“FolderGeoAddress”	“Value Optional”	Max Length: 128
“FolderGeoCity”	“Value Optional”	Max Length: 64
“FolderGeoState”	“Value Optional”	Max Length: 40
“FolderGeoZip”	“Value Optional”	Max Length: 12
“FolderGeoCountry”	“Value Optional”	Max Length: 64
“AP_Name”	“Value Required”	Max Length: 32
“AP_Longitude”	“Value Required”	Range: 0 to ±180
“AP_Latitude”	“Value Required”	Range: 0 to ±90

Step 2 Save the file with CSV filename extension and then copy it to a location accessible from your browser.

Import Geographical Coordinate Files to Create Outdoor Locations in Wireless Site Maps

To group access points together into outdoor locations, use the Latitude/Longitude geographical coordinates for each access point. You first need to create the required access point geographical coordinate files, which you can then import into Prime Infrastructure. You can import either a Google KML or a CSV file containing access point geographical coordinates into Prime Infrastructure.

Step 1 Choose Maps > Google Earth.

Step 2 Choose Select a command > Import Google KML > Go (or, if you are importing a CSV file, choose Select a command > Import CSV > Go.

Step 3 Navigate to the KML, KMZ, or CSV file, then click Next.

The input file is parsed and validated for the following:

- Access points specified in the uploaded file are validated (the specified access points must be available within Prime Infrastructure).
- Range validations are performed for tilt, heading, range, and other geographical coordinates fields.If longitude and latitudeare provided, range validations are performed; if not, the value is defaulted to 0.

Step 4 After the files pass all validation checks, review the file details and click Save.

If the uploaded information was previously saved, the information is overwritten as follows:

- If the folder was uploaded previously, the coordinates are updated for the folder.
- If access points were uploaded previously, the coordinates are updated for the access points.
- Existing access points in the folder are not removed.
- New folders are created as needed and access points are placed accordingly.

Add Google Earth Location Launch Points to Access Point Details

You can expand the number of Google Earth Location launch points within Prime Infrastructure by adding launch points to the Access Point summary and detail pages.

Step 1 Choose Monitor > Wireless Technologies > Access Point Radios.

Step 2 In the Access Point summary page, click the Edit View link next to page heading.

Step 3 In the Edit View page, highlight Google Earth Location in the left-hand column, then click Show.

The Google Earth Location column heading moves into the View Information column.

Step 4 To change the display order of the columns, highlight the Google Earth Location entry and click the Up and Down buttons as needed, then click Submit.

You are returned to the Access Points summary page, and a Google Earth launch link appears. The launch link also appears in the general summary page of the Access Points details page (Monitor > Wireless Technologies > Access Point Radios > AP Name).

Configure Your Google Earth Map Preferences

You can configure access point settings for the Google Earth Maps feature:

Step 1 Choose Maps > Google Earth.

Step 2 Configure the following parameters:

- Refresh Settings—Select the Refresh from Network check box to enable on-demand refresh. This option is applied only once and then disabled. Based on the number of access points in your network, the refresh can take a long period of time.
- Layers—Layer filters for access points, access point heat maps, and access point mesh information can be selected and saved. Select the check box to activate the applicable layer and click > to open the filter page. These settings apply when Google Earth sends the request for the next refresh.
  - Access Points—From the AP Filter drop-down list, choose to display channels, Tx power level, coverage holes, MAC addresses, names, controller IP, utilization, profiles, or clients.

    If the access point layer is not checked, no data is returned, and an error message is returned to Google Earth as a Placemark without an icon.
  - AP Heatmap—From the Protocol drop-down list, choose 802.11a/n, 802.11b/g/n, 802.11a/n & 802.11b/g/n, or None. Select the cutoff from the RSSI Cutoff drop-down list (- 60 to - 90 dBm).

    If you chose both 802.11a/n and 802.11b/g/n, the heat maps are generated for both and overlaid on top of each other. The order cannot be defined. To prevent this overlay, you must turn off individual overlay in Google Earth or change it in the Google Earth Settings in Prime Infrastructure.
  - AP Mesh Info—Choose Link SNR, Packet Error Rate, or none. Choose Link SNR or Packet Error Rate from the Link Color drop-down list. When you select AP Mesh Info, Mesh Links are also automatically shown.

Step 3 Click Save Settings to confirm these changes or Cancel to close the page without saving the changes.

Monitor Mesh Access Points Using Maps

You can view summary information for a mesh access point (AP) from a mesh network map. This information is in addition to the information shown for all APs (MAC address, AP model, controller IP address, location, height of AP, AP uptime, and LWAPP uptime).

To view summary and detailed configuration information for a mesh AP from a mesh network map, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Select the campus, building, floor area, basement level or outdoor area containing the AP you want to monitor.

Step 3 To view summary configuration information for an AP, hover your mouse cursor over the AP that you want to monitor. A dialog box appears with configuration information for the selected AP.

Step 4 To view detailed configuration information for an AP, double-click the AP appearing on the map. The configuration details for the AP appear.

If the AP has an IP address, a Run Ping Test link is also visible at the bottom of the mesh AP dialog box.

View Mesh Access Point Configurations Using Wireless Site Maps

To view detailed configuration information for a mesh access point (AP) from a mesh network map, follow these steps:

Step 1 Choose Maps > Site Maps.

Step 2 Select the campus, building, floor area, basement level or outdoor area containing the AP you want to monitor.

Step 3 Double-click the AP for which you want to view detailed configuration information.

Step 4 Click any of the following tabs to get the required information:

- General—Displays the overall configuration of the mesh AP such as the AP name, MAC address, AP Up time, associated controllers (registered and primary) operational status, and software version.

  The software version for mesh APs is appended with the letter m and the word mesh appears in parentheses.

- Interface—Displays configuration details for the interfaces supported on the mesh AP. Interface options are radio and Ethernet.

- Mesh Links—Displays parent and neighbor details (name, MAC address, packet error rate, and link details) for the mesh AP. You can also initiate link tests from this page.

- Mesh Links—Displays parent and neighbor details (name, MAC address, packet error rate, and link details) for the mesh AP. You can also initiate link tests from this page.

View Device Details on Wireless Site Maps

Hover your cursor over any device icon in a map to view details about that device.

Monitor mode access points are shown with gray labels to distinguish them from other access points.

What Is a Wireless Network Site Map?

A wireless network site map is a representation within Prime Infrastructure of the physical placement of access points throughout your facilities, as well as the facilities themselves. A hierarchy of a single physical campus, the buildings that comprise that campus, and the floors of each building, together with the physical location of access points in that hierarchy, constitutes a single wireless network map.

Create a Simple Wireless Network Site Map

After access points have been installed and have joined a controller, and you've configured Prime Infrastructure to manage the controllers, you can create a network design.

The location appliance must be set to poll the controllers in that network, as well as be configured to synchronize with that specific network design, to track devices in that environment. The concept and steps to perform synchronization between Prime Infrastructure and the mobility services engine are explained in the Cisco Mobility Services Engine Configuration Guide.

Step 1 Log in to Prime Infrastructure with SuperUser, Admin, or ConfigManager access privileges.

Step 2 Choose Maps > Site Maps.

Step 3 Create a new campus and at least one building.

Step 4 Create a new floor area in one of the buildings.

Step 5 Select the access points to be placed on the floor area.

Each access point you add to the floor area is represented by a gray circle (labeled with the access point name or MAC address) and is lined up in the upper left part of the floor map.

Step 6 Drag each access point to the appropriate location. (Access points turn blue when you click them to relocate them.) The small black arrow at the side of each access point represents Side A of each access point, and each arrow of the access point must correspond with the direction in which the access points were installed. (Side A is clearly noted on each 1000 series access point and has no relevance to the 802.11a/n radio.)

Step 7 To adjust an access point's directional arrow, choose the appropriate orientation on the Antenna Angle drop-down list.

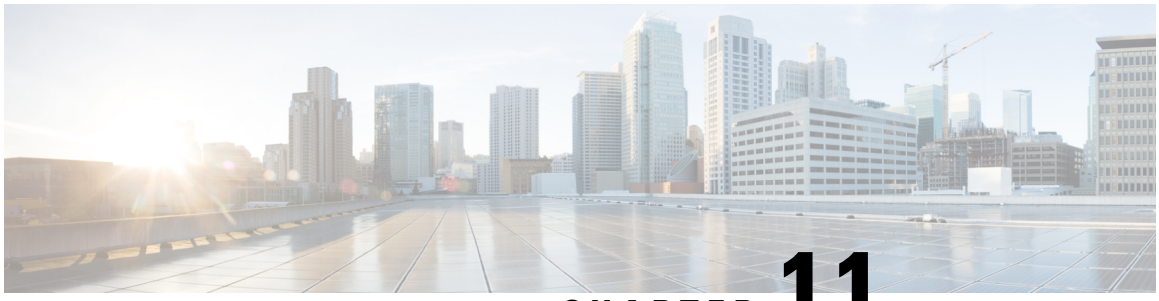
Access point placement and direction must directly reflect the actual access point deployment or the system cannot pinpoint the device location.

Step 8 Click Save when you are finished placing and adjusting each direction of the access point.

Step 9 Repeat these steps to create additional campuses, buildings, and floors until each device location is properly detailed in the network design.

PART IV

Monitor the Network



CHAPTER 11

Set Up Network Monitoring

Set Up Port and Interface Monitoring

To monitor your device ports, you can create a port group and then display monitoring information on dashboards. Port groups are logical groupings of interfaces that allow you to monitor device ports by the function they serve. For example, you can create a port group for the WAN ports and create another port group for the internal distribution ports on the same router.

After you create groups, you can create an interface health monitoring policy on those ports as explained in the following steps:

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies.

Step 2 Click My Policies.

Step 3 Click Add.

Step 4 Choose Interface Health under Policy Types.

Step 5 From the Device Selection drop-down list, choose Port Group.

Step 6 Choose the User Defined group and click OK.

Step 7 Enter the policy name.

Step 8 Select required the Parameters and Threshold and complete the required fields.

Step 9 Click OK.

Step 10 Click Save and Activate.

Step 11 To display the results, choose Dashboards > Overview > Network Interface, and view the Top N Interface Utilization dashlet.

Step 12 Edit the Top N Interface Utilization dashlet and add the port group that you previously created.

Set Up WAN Interface Monitoring

Creating a WAN interface port group allows you to efficiently monitor all WAN interfaces in a specific port group. For example, if you have many small branch offices that have low bandwidth issues, you can create a port group that includes all WAN interfaces from each branch office, and then monitor this port group for issues.

By default, provides a static WAN Interfaces port group on which health monitoring is automatically deployed. The following procedure shows you how to:

1. Add interfaces to the WAN Interfaces port group.
2. Verify the utilization and availability of the WAN interfaces from the Site dashboard.

Step 1 To add interfaces to the WAN Interfaces port group:

a) Choose Inventory > Group Management > Port Groups.
b) From the menu on the left, choose System Defined > WAN Interfaces.
c) Select the device, then click Add to Group.

Step 2 To display the results:

a) Choose Dashboard Overview Add Dashlets.
b) Click either of the following:

- Top N WAN Interfaces by Utilization
- Top N WAN Interfaces with Issues

Set Up Enhanced Wireless Client Monitoring Using Cisco ISE

manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, collects additional information about these clients from Cisco ISE and provides all client relevant information to to be visible in a single console.

When posture profiling is enforced in the network, communicates with Cisco ISE to get the posture data for the clients and displays it along with other client attributes. When Cisco ISE is used to profile the clients or an endpoint in the network, collects the profiled data to determine what type of client it is, whether it is an iPhone, iPad, an Android device, or any other device.

You can get enhanced information about managed clients using the Cisco ISE server.

If is integrated with an ISE server (to access endpoint information), you can:

- Check an End User's Network Session Status.
- Using the User 360° View, you can identify possible problems with the end user's authentication and authorization for network access.
- Troubleshoot the User Application and Site Bandwidth Utilization.

displays ISE Profiling attributes only for authenticated endpoints.

Add Cisco Identity Service Engines

A maximum of two ISEs can be added to . If you add two ISEs, one should be primary and the other should be standby. When you are adding a standalone node, you can add only one standalone node and cannot add a second node.

To add an Identity Services Engine, follow these steps:

Step 1 Choose Administration > Servers > ISE Servers.

Step 2 From the Select a command drop-down list, choose Add ISE Server, then click Go.

Step 3 Complete the required fields, then click Save.

The credentials should be superuser credentials local to ISE. Otherwise, ISE integration does not work.

Set Up NAM and NetFlow Data Collection for Performance Monitoring

If your implementation includes Assurance licenses, you must enable data collection via NAMs and NetFlow configurations. This is necessary to populate the additional dashlets, reports, and other features supplied with Assurance.

Enable NAM Data Collection

To ensure that you can collect data from your Network Analysis Modules (NAMs), you must enable NAM data collection. You can do this for each discovered or added NAM, or for all NAMs at the same time.

Before you begin

You must specify the HTTP/HTTPS credentials for each NAM. See "Adding NAM HTTP/HTTPS Credentials."

Step 1 Choose Services > Application Visibility & Control > Data Sources.

Step 2 In the NAM Data Collector section, select the required NAM datasources for which you want to enable data collection.

Step 3 Click Enable.

Note After enabling the NAM Polling, you can verify the NAM data Top N Application dashlet from Application dashboard.

To disable NAM Data collection, select the required(enabled) NAM or NAM datasources from the NAM Data Collector section and click Disable.

Define NAM Polling Parameters

You can specify data that is collected from NAMs.

Step 1 Choose Monitor > Monitoring Policies.

Step 2 Click Add, then select NAM Health under the Policy Types list from the left sidebar menu.

Step 3 Select the NAM devices from which you want to collect data, then complete the required fields.

Step 4 Under Parameters and Thresholds, specify the parameters you want to poll from the NAM devices and threshold conditions.

Step 5 Click Save and Activate.

Enable NetFlow Data Collection

To start collecting NetFlow and Flexible NetFlow data, you must configure your NetFlow-enabled switches, routers, and other devices (ISR/ASR) to export this data to . The following table shows the various device types that support NetFlow and the ways to configure devices to export NetFlow data to .

The following table gives the detailed information of NetFlow support summary.

Table 26: NetFlow Support Summary

Device Type	IOS Versions Supporting NetFlow	Supported NetFlow Export Types	NetFlow Configuration in	Template Naming Convention
Cisco ASR	IOS XE 3.11 to 15.4(1) S, and later Easy PerfMon based configuration (EzPM)	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility Application Traffic Stats	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Traffic-Voice-Video- Netflow-URL- Netflow-Aggregated-Traffic-Stats-
	IOS XE 3.9, 3.10	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility AVC Troubleshooting	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Host- Netflow-App-Traffic- Netflow-Voice-Video- Netflow-URL- Netflow-AVC-Troubleshooting-

Device Type	IOS Versions Supporting NetFlow	Supported NetFlow Export Types	NetFlow Configuration in	Template Naming Convention
Cisco ISR	15.1(3) T	TCP/UDP conversation traffic Voice & Video	TCP/UDP: Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Collecting Traffic Statistics Voice Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI >Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-Voice-Video-
	IOS XE 3.11 to 15.4(1) S, and later Easy PerfMon based config (EzPM)	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility Application Traffic Stats	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Traffic-Voice-Video- Netflow-URL- Netflow-Aggregated-Traffic-Stats-
	IOS XE 3.9, 3.10	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility AVC Troubleshooting	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Host- Netflow-App-Traffic- Netflow-Voice-Video- Netflow-URL- Netflow-AVC-Troubleshooting-

Device Type	IOS Versions Supporting NetFlow	Supported NetFlow Export Types	NetFlow Configuration in	Template Naming Convention
Cisco ISR G2	15.1(4) M and 15.2(1) T	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video	TCP/UDP, ART: Create a CLI template. See "Configure NetFlow on ISR Devices" Voice & Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI >Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Voice-Video-
	15.2(4) M and 15.3(1)T	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video	Choose: Services > Application Visibility & Control >Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Voice-Video-
	15.4(1)T and later Easy PerfMon based configuration (EzPM)	TCP/UDP conversation traffic Application Response Time (ART) Voice & Video HTTP URL visibility	Choose Services > Application Visibility & Control > Interfaces Configuration Format: V9 and IPFIX	Netflow-Traffic-Conv- Netflow-App-Traffic- Netflow-Traffic-Voice-Video- Netflow-App-Traffic-URL-
Cisco Catalyst 2000	15.0(2) UCP and later	TCP/UDP conversation traffic	Create a custom CLI template. See "Configuring NetFlow Export on Catalyst 2000 Switches". Format: V5, V9	Netflow-Traffic-Conv-
Cisco Catalyst 3750-X, 3560-X	15.0(1)SE IP base or IP services feature set and equipped with the network services module.	TCP/UDP conversation traffic	Create a custom CLI template. See "Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches." Format: V9	Netflow-Traffic-Conv-

Device Type	IOS Versions Supporting NetFlow	Supported NetFlow Export Types	NetFlow Configuration in	Template Naming Convention
Cisco Catalyst 3850 (wired)	15.0(1)EX and later	TCP/UDP conversation traffic Voice & Video	TCP/UDP: Create a custom CLI template. Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches." Voice & Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI >Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-Voice-Video-
Cisco Catalyst 3850 (wireless)	Cisco IOS XE Release 3SE (Edison)	TCP/UDP conversation traffic	See "Configuring Flexible NetFlow." Format: V9	Netflow-Traffic-Conv-
Cisco CT5760 Controller (Wireless)	Katana 5760	TCP/UDP conversation traffic	See "Application Visibility and Flexible Netflow." Format: V9	Netflow-Traffic-Conv-
Cisco Catalyst 4500	15.0(1)XO and 15.0(2)SG onwards	TCP/UDP conversation traffic Voice & Video	TCP/UDP: Create a custom CLI template. See" Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches." Voice & Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI >Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-Voice-Video-
Cisco Catalyst 6500	15.1(1)SY and later	TCP /UDP conversation traffic Voice & Video	TCP/UDP: Create a custom CLI template. See" Configuring NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches." Voice & Video: Use Medianet Perfmon CLI template. Choose Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI >Medianet – PerfMon Format: V9	Netflow-Traffic-Conv- Netflow-Voice-Video-

Configure NetFlow Export on Catalyst 2000 Switches

To manually configure NetFlow export on Catalyst 2000 devices, create a user-defined CLI template as shown in the following steps.

Step 1 Choose Configuration > Templates > Features & Technologies > CLI Templates > CLI.

Step 2 Hover your mouse cursor over the information icon and click New to create a new CLI template.

Step 3 Enter a name for the new CLI template (for example, “Prime_NF_CFG_CAT2K).

Step 4 From the Device Type list, choose Switches and Hubs.

Step 5 In the Template Detail > CLI Content text box, enter the following commands, modifying them as needed for your network (note that these commands are only an example):

```
flow record PrimeNFRec

 match ipv4 protocol

 match ipv4 source address

 match ipv4 destination address

 match interface input

 match transport source-port

 match transport destination-port

 collect counter bytes long

 collect counter packets long

!

!

flow exporter PrimeNFExp

 destination 172.18.54.93

 transport udp 9991

 option exporter-stats timeout 20

!

!

flow monitor PrimeNFMon
```

```
 record PrimeNFRec

 exporter PrimeNFExp


interface GigabitEthernet3/0/1

  ip flow monitor PrimeNFMon input
```

Step 6 Click Save as New Template. After you save the template, deploy it to your devices. See " Ways to Create Configuration Templates Using Prime Infrastructure, on page 384."

Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches

To manually configure NetFlow to export TCP and UDP traffic on Catalyst 3000, 4000, or 6000 devices, create a user-defined CLI template as shown in the following steps.

Step 1 Choose Configuration > Templates > Features & Technologies > CLI Templates > CLI.

Step 2 Hover your mouse cursor over the information icon and click New to create a new CLI template.

Step 3 Enter a name for the new CLI template (for example, "Prime_NF_CFG_CAT3K_4K").

Step 4 From the Device Type list, choose Switches and Hubs.

Step 5 In the Template Detail > CLI Content text box, enter the following commands, modifying them as needed for your network (note that these commands are only an example):

```
flow record PrimeNFRec

 match ipv4 protocol

 match ipv4 source address

 match ipv4 destination address

 match interface input

 match transport source-port

 match transport destination-port

 collect counter bytes long

 collect counter packets long


flow exporter PrimeNFExp
```

```
 destination 172.18.54.93

 transport udp 9991

 option exporter-stats timeout 20



flow monitor PrimeNFMon

 record PrimeNFRec

 exporter PrimeNFExp


interface GigabitEthernet3/0/1

  ip flow monitor PrimeNFMon input
```

Step 6 Click Save as New Template. After you save the template, deploy it to your devices See " Ways to Create Configuration Templates Using Prime Infrastructure, on page 384."

Configure NetFlow on ISR Devices

To manually configure NetFlow to export ART traffic on an ISR device, use the following steps to create a user-defined CLI template:

Step 1 Choose Configuration > Templates > Features & Technologies > CLI Templates > CLI.

Step 2 Hover your mouse cursor over the information icon and click New to create a new CLI template.

Step 3 Enter a name for the new CLI template (for example, "Prime_NF_CFG_TEMPLATE").

Step 4 From the Device Type list, choose Routers.

Step 5 In the Template Detail > CLI Content text box, enter the following commands, modifying them as needed for your network (note that these commands are only an example).

```
flow record NFARecord
 match ipv4 source address
 match ipv4 destination address
 match ipv4 protocol
 match transport source-port
 match transport destination-port
 match application name
 match interface input
 collect interface output
 collect ipv4 source mask
 collect ipv4 destination prefix
 collect ipv4 destination mask
 collect counter bytes long
```

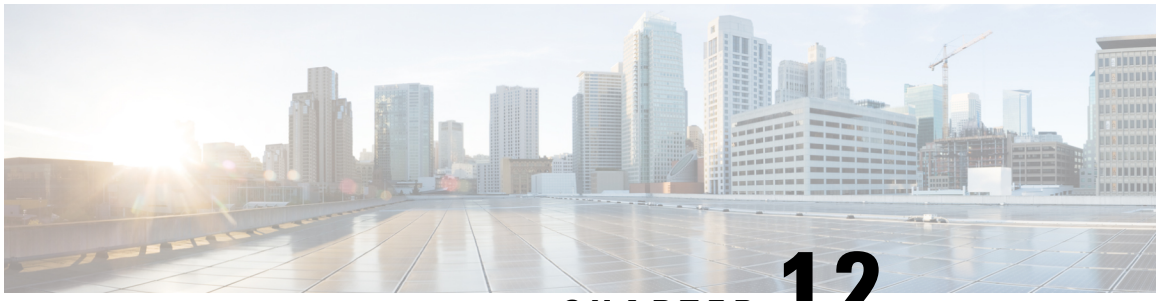
```
 collect counter packets long
 collect timestamp sys-uptime first
 collect timestamp sys-uptime last
!

flow exporter NFAExporter
 destination <Prime server ip address>
 source <Any L3 interface or the device>
 transport udp 9991
 template data timeout 60
 option application-table timeout 60
 option application-attributes timeout 300
!

flow monitor NFAMonitor
 exporter NFAExporter
 cache timeout active 60
 record NFARecord
!

interface <L3 interface provided in exporter:source section>
 ip flow monitor NFAMonitor input
!
```

Step 6 Click Save as New Template. After you save the template, deploy it to your devices. See " Ways to Create Configuration Templates Using Prime Infrastructure, on page 384."



CHAPTER 12

Monitoring Devices

Set Up Packet Capture to Monitor Network Traffic

In addition to aggregating data from multiple NAMs, Prime Infrastructure makes it easy to actively manage and troubleshoot network problems using multiple NAMs and ASRs.

Note This feature is supported for NAMs and ASRs. For more information on minimum Cisco IOS XE version supported on ASRs, see the Cisco ASR 1000 Series Aggregation Services Routers Release Notes.

In the following workflow, a network operator needs to troubleshoot a set of similar authentication violations taking place at multiple branches. Because the operator suspects that the authentication problems are due to a network attack in progress, the operator runs the Packet Capture feature against the NAMs or ASRs for each branch, then runs the Packet Decoder to inspect the suspicious traffic.

Note The legacy cipher, which helps you to perform the Copy To or Merge functionalities in the Packet Capture screen, in the Prime Infrastructure server is enabled by default.

In case the Copy To/Merge functionalities do not work, you must enable it manually by entering the following command in the Prime Infrastructure's CLI.

#admin ncs run ssh-server-security-legacy-algorithms enable

You must disable it after performing these actions. Enter the following command to disable.

admin# ncs run ssh-server-legacy-algorithms disable

Step 1 Create a capture session definition:

a) Choose Monitor > Tools > Packet Capture to create a new capture session definition.

b) Complete the General section as needed. Give the session definition a unique name and specify how you want to file the captured data. To capture the full packet, enter 0 in the Packet Slice Size.

c) If you want to restrict the captured traffic to particular source or destination IPs, VLANs, applications, or ports, click Add in the Software Filters section and create filters as needed. If you do not create a software filter, it captures everything.
d) In the Devices area, you can select: A NAM and its data ports. You can create one capture session per NAM only, whether the capture session is running or not. An ASR and its interfaces.
e) Click Create and Start All Sessions. Prime Infrastructure saves the new session definition, then runs separate capture sessions on each of the devices you specified. It stores the sessions as files on the device and displays the list of packet capture files in the Capture Files area.

Step 2 To decode a packet capture file:

a) Choose Monitor > Tools > Packet Capture
b) Select a PCAP file in a NAM or ASR device.
c) Select Copy To to copy the PCAP file to the PI server (the decode operation only runs on files in the PI server).
d) Click View Jobs to confirm that the copy job completed successfully.
e) Open the localhost folder, select the check box for the new capture file, then click Decode. The decoded data appears in the bottom pane.
f) A TCP Stream displays the data as the application layer sees it. To view the TCP Stream for a decoded file, select a TCP packet from the Packet List, then click TCP Stream. You can view the data as ASCII text or in a HEX dump.

Step 3 To run a packet capture session again, select the session definition in the Capture Sessions area and click Start.

Manage Jobs Using the Jobs Dashboard

If you have the appropriate user account privileges, you can manage jobs using the Jobs dashboard. To view the Jobs dashboard, choose Administration > Dashboards > Job Dashboard. From here, you can quickly see if a job was successful, partially successful, or failed.

If too many jobs are already running, will hold other jobs in the queue until resources are available. If this delays a scheduled job past its normal starting time, the job will not run. You will have to run it manually.

Some jobs may require approval. If this is the case, sends an email to users with Administrator privileges notifying them that a job was scheduled and needs approval. The job will only run after it is approved.

The following table describes the buttons displayed in the Jobs dashboard.

Table 27: Jobs Dashboard Buttons

Button	Description
Delete Job	Removes a job from the Jobs dashboard.
Edit Job	Edit the settings configured for the selected job.
Edit Schedule	Displays the series schedule and lets you edit it (start time, interval, and end time). **Note** Editing the schedule of an already-scheduled job will change the status of that job to Pending for Approval since each edit requires an approval from the user who created the job.
Run	Runs a new instance of the selected job. Use this to rerun partially successful or failed jobs; the job will only run for the failed or partially successful components.

Button	Description
Abort	Stops a currently-running job, but allows you to rerun it later. Not all jobs can be aborted; will indicate when this is the case.
Cancel Series	Stops a currently-running job and does not allow anyone to rerun it. If the job is part of a series, future runs are not affected.
Pause Series	Pauses a scheduled job series. When a series is paused, you cannot run any instances of that series (using Run).
Resume Series	Resumes a scheduled job series that has been paused.

Note The Delete Job, Abort, and Cancel Series buttons are not available for system and poller jobs.

To view the details of a job, follow these steps:

Step 1 Choose Administration > Dashboards > Job Dashboard.

Step 2 From the Jobs pane, choose a job series to get basic information (such as job type, status, job duration, and next start time).

Step 3 To view the job interval, click a job instance hyperlink.

At the top of the job page, the Recurrence field indicates how often the job recurs. Job interval details will be added for every jobs that triggers.

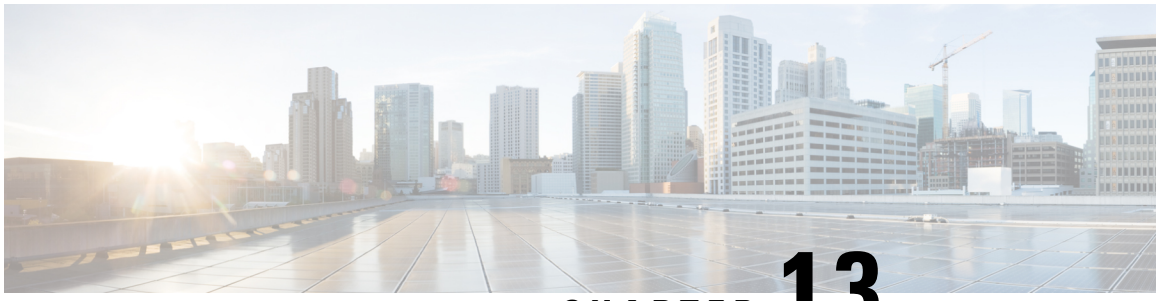
Step 4 To get details about a failed or partially successful job, click the job instance hyperlink and expand the entries provided on the resulting page.

This is especially helpful for inventory-related jobs. For example, if a user imported devices using a CSV file (a bulk import), the job will be listed in the Jobs sidebar menu under User Jobs > Device Bulk Import. The job details will list the devices that were successfully added and the devices that were not.

Example

To troubleshoot a failed software image import job:

1. Choose User Jobs > Software Image Import from the Jobs sidebar menu.
2. Locate the failed job in the table and then click its hyperlink.
3. Expand the job's details (if not already expanded) to view the list of devices associated with the job and the status of the image import for each device.
4. To view the import details for a specific device, click that device's i (information) icon in the Status column. This opens an Image Management Job Results pop-up window.
5. Examine each step and its status. For example, the Collecting image with Protocol: SFTP column might report that SFTP is not supported on the device.



CHAPTER 13

Monitor Wireless Devices

Monitor Controllers

Choose Monitor > Managed Elements > Network Devices , then select Device Type > Wireless Controller to view all the wireless controllers.

Related Topics

Monitor System Parameters, on page 225

Monitor System Parameters

Choose Monitor > Managed Elements > Network Devices, then select Device Type > Wireless Controllerto view all the wireless controllers. Click a Device name to view its details.

From Release 3.2 onwards, for the following Monitor pages under Device Details > System, by default the data is fetched from the Prime Infrastructure database. There is an option to refresh from device by clicking the Refresh from Device link in the upper right corner of the page. It also shows the date and time when the data was last refreshed on the Prime Infrastructure.

- Summary
- CDP Neighbors
- WLANs

From Release 3.2 onwards, for the following Monitor pages under Device Details > System, the data is fetched directly from the device.

- CLI Sessions
- DHCP Statistics

Table 28: Monitor Network Devices Wireless Controller Details

To View ...	Select This Menu ...
System Information	System > Summary under Device Details tab
Summary information such as IP address, device type, location, reachability status, description, and total device count	
CLI session details	System > CLI Sessions under Device Details tab
DHCP statistics (for version 5.0.6.0 controllers or later) such as packets sent and received, DHCP server response information, and the last request time stamp	System > DHCP Statistics under Device Details tab
Multicast information	System > Multicast under Configuration tab
Stack information such as MAC address, role, and state	System > Stacks under Device Details tab
STP statistics	System > Spanning Tree Protocol under Configuration tab
Information about any user-defined fields	System > User Defined Field under Device Details tab
Wireless local access networks (WLANs) configured on a controller	System >WLANs under Device Details tab
Mobility	Mobility > Mobility Stats under Device Details tab
Statistics for mobility group events such as receive and transmit errors, and handoff request	
Ports	Ports > General under Configuration tab
Information regarding physical ports on the selected controller	
CDP Interfaces	Ports > CDP Interface Neighbors under Configuration tab
Security	Security > RADIUS Accounting under Device Details tab
RADIUS accounting server information and statistics	
RADIUS authentication server information	Security > RADIUS Authentication under Device Details tab
Information about network access control lists	System > Security > Network Access Control
Guest access deployment and network users	Security > Guest Users under Device Details tab
Management Frame Protection (MFP) summary information	System > Security > Management Frame Protection under Device Details tab
List of all rogue access point rules currently applied to a controller.	System > Security > Rogue AP Rules under Device Details tab

To View ...	Select This Menu ...
List of sleeping clients, which are clients with guest access that have had successful web authentication that are allowed to sleep and wake up without having to go through another authentication process through the login page	Security > Sleeping Clients under Device Details tab
IPv6	IPv6 > Neighbor Binding Timers under Configuration tab
Statistics for the number of messages exchanged between the host or client and the router to generate and acquire IPv6 addresses, link, and MTU	
Redundancy	System > Redundancy Summary under Device Details tab
Redundancy information	
mDNS	mDNS > mDNS Service Provider under Device Details tab
List of mDNS services and service provider information	

Related Topics

What is Spanning Tree Protocol, on page 227
What is Management Frame Protection, on page 227
What are Rogue Access Points Rules, on page 228

What is Spanning Tree Protocol

The Spanning Tree Protocol (STP) is a link management protocol. Cisco WLAN Solution implements the IEEE 802.1D standard for media access control bridges.

The spanning tree algorithm provides redundancy while preventing undesirable loops in a network that are created by multiple active paths between stations. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail.

The following controllers do not support Spanning Tree Protocol: WISM, 2500, 5500, 7500 and SMWLC.

What is Management Frame Protection

Management Frame Protection (MFP) provides the authentication of 802.11 management frames. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

If one or more of the WLANs for the controller has MFP enabled, the controller sends each registered access point a unique key for each BSSID the access point uses for those WLANs. Management frames sent by the access point over the MFP enabled WLANs is signed with a Frame Protection Information Element (IE). Any attempt to alter the frame invalidates the message causing the receiving access point configured to detect MFP frames to report the discrepancy to the WLAN controller.

What are Rogue Access Points Rules

Rogue Access Points rules automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. applies the rogue access point classification rules to the controllers and respective access points.

These rules can limit a rogue appearance on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Rogue Access Points Rules also help reduce false alarms.

Rogue classes include the following types:

- Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly Access Points category.
- Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
- Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

Related Topics

Monitor System Parameters, on page 225

View System Details About Third-Party Controllers

Choose Monitor > Managed Elements > Network Devices> Third Party Wireless Controllers to view the detailed information about the third party (non-Cisco) controllers that are managed by .

View System Details About Switch Controllers and Configure the Switch List

Choose Monitor > Managed Elements > Network Devices > Switches and Hubsto view the following detailed information about the switches:

- Searching Switches

Use the search feature to find specific switches or to create and save custom searches.

- Viewing the Switches

Configure the Switch List Page

The Edit View page allows you to add, remove, or reorder columns in the Switches table.

To edit the available columns in the table, follow these steps:

Step 1 Choose Monitor > Managed Elements > Network Devices > Switches and Hubs.

Step 2 Click the Edit View link.

Step 3 To add an additional column to the table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.

Step 6 Click Reset to restore the default view.

Step 7 Click Submit to confirm the changes.

Monitor Access Points

This section describes access to the controller access points summary details. Use the main date area to access the respective access point details.

Choose Monitor > Wireless Technologies> Access Point Radios to access this page.

Related Topics

View Access Points, on page 229
View System Details About Access Points, on page 231

View Access Points

Choose Monitor > Wireless Technologies > Access Point Radios or perform an access point search to view the summary of access points including the default information.

Related Topics

Types of Reports for Access Points, on page 229
View System Details About Switch Controllers and Configure the Switch List, on page 228

Types of Reports for Access Points

The following reports can be generated for Access Points. These reports cannot be customized.

- Load—Traffic Load is the total amount of bandwidth used for transmitting and receiving traffic. This enables WLAN managers to track network growth and plan network growth ahead of client demand.
- Dynamic Power Control—Generates a report with Dynamic Power Control information.
- Noise—Generates a report with Noise information. The Noise report displays a bar graph of noise (RSSI in dBm) for each channel for the selected access points.
- Interference—The Interference report displays a bar graph of interference (RSSI in dBm) for each channel:
  - High interference—40 to 0 dBm
  - Marginal interference—100 to -40 dBm
  - Low interference—110 to -100 dBm
- Coverage (RSSI)—The Coverage (RSSI) report displays a bar graph of client distribution by received signal strength showing the number of clients versus RSSI in dBm.
- Coverage (SNR)—The Access Points Coverage (SNR) report displays a bar graph of client distribution by signal-to-noise ratio showing the number of clients versus SNR.
- Up/Down Statistics—The Up/Down Statistics report displays a line graph of access point up time graphed against time. Time in days, hours and minutes since the last reboot.
- Network Airtime Fairness Statistics—Network Airtime Fairness Statistics is a tabular representation of Average Airtime used across different WLAN profiles in the selected interval of time.

- Voice Statistics—Generates a report for selected access points showing radio utilization by voice traffic. The Voice Statistics report displays the following radio utilization statistics by voice traffic:
  - Access Points Name
  - Radio
  - Calls in Progress
  - Roaming Calls in Progress
  - Bandwidth in Use

Voice Statistics reports are only applicable for CAC/WMM clients.

- Voice TSM Table—The Voice Traffic Stream Metrics Table is generated for the selected access points and radio, organized by client device showing QoS status, PLR, and latency of its voice traffic stream.
- Voice TSM Reports—The Voice Traffic Stream Metrics Table report displays a graphical representation of the Voice Traffic Stream Metrics Table except that metrics from the clients that are averaged together on the graphs for the selected access point.
- 802.11 Counters—The 8o2.11 Counters report displays counters for access points at the MAC layer. Statistics such as error frames, fragment counts, RTS/CTS frame count, and retried frames are generated based on the filtering criteria and can help interpret performance (and problems, if any) at the MAC layer.
- Access Points Profile Status—The Access Points Profile Status displays access point load, noise, interference, and coverage profile status.
- Air Quality vs. Time—The Radio Utilization Report displays the utilization trends of the access point radios based on the filtering criteria used when the report was generated. It helps to identify current network performance and capacity planning for future scalability needs. The Radio Utilization Report displays the air quality index of the wireless network during the configured time duration.
- Traffic Stream Metrics—The Traffic Stream Metrics Report is useful in determining the current and historical quality of service (QoS) for given clients at the radio level. It also displays uplink and downlink statistics such as packet loss rate, average queuing delay, distribution of delayed packets, and roaming delays.
- Tx Power and Channel—The Tx Power and Channel report displays the channel plan assignment and transmit power level trends of devices based on the filtering criteria used when the report was generated. It can help identify unexpected behavior or issues with network performance.

The Current Tx Power Level setting controls the maximum conducted transmit power. The maximum available transmit power varies according to the configured channel, individual country regulation, and access point capability. See the Product Guide or data sheet at for each specific model to determine the access point capability.

The Current Tx Power Level setting of 1 represents the maximum conducted power setting for the access point. Each subsequent power level (for example. 2, 3, 4, and so on.) represents approximately a 50% (or 3dBm) reduction in transmit power from the previous power level. The actual power reduction might vary slightly for different models of access points.

Based on the configured antenna gain, the configured channel, and the configured power level, the actual transmit power at the access point can be reduced so that the specific country regulations are not exceeded.

Irrespective of whether you choose Global or Custom assignment method, the actual conducted transmit power at the access point is verified such that country specific regulations are not exceeded.

The following command buttons are available to configure the transmission levels:

- Save—Save the current settings.
- Audit—Discover the present status of this access point.

- VoIP Calls Graph—VoIP Calls Graph analyzes wireless network usage from a voice perspective by providing details such as the number and duration of VoIP calls (per radio) on the network over time. VoIP snooping must be enabled on the WLAN to be able to gather useful data from this report. This report displays information in a graph.
- VoIP Calls Table—VoIP Calls Table provides the same information as the VoIP Calls Graph report but in table form.
- Voice Statistics—Voice Statistics Report analyzes wireless network usage from a voice perspective by providing details such as percentage of bandwidth used by voice clients, voice calls, roaming calls, and rejected calls (per radio) on the network. To be able to gather useful data from this report, make sure call admission control (CAC) is supported on voice clients.
- Worst Air Quality APs—Provides a high-level, easy-to- understand metric to facilitate understanding of where interference problems are impacting the network. Air Quality (AQ) is reported at a channel, floor, and system level and it supports AQ alerts, so that you can be automatically notified when AQ falls below a desired threshold.

View System Details About Access Points

The Access Points Details page enables you to view access point information for a single Access Point.

Choose Monitor > Wireless Technologies > Access Point Radios and click the access point name in the AP Name column to access this page. Depending on the type of access point, the following tabs are displayed:

- General Tab

The General tab fields differ between lightweight and autonomous access points.

For autonomous clients, only collects client counts. The client counts in the Monitor page and reports have autonomous clients included. Client search, client traffic graphs, or other client reports (such as Unique Clients, Busiest Clients, Client Association) do not include clients from autonomous access points.

- Interfaces Tab
- CDP Neighbors Tab

This tab is visible only when CDP is enabled.

- Current Associated Clients Tab

This tab is visible only when there are clients associated to the Access Point (CAPWAP or Autonomous Access Point).

- SSID Tab

This tab is visible only when the access point is an Autonomous Access Point and there are SSIDs configured on the Access Point

- Clients Over Time Tab

This tab displays the following charts:

- Client Count on Access Point—Displays the total number of clients currently associated with an access point over time.
- Client Traffic on Access Point—Displays the traffic generated by the client connected in the Access Point distribution over time.

The information that appears in these charts is presented in a time-based graph. Time-based graphs have a link bar at the top of the graph page that displays 6h, 1d, 1w, 2w, 4w, 3m, 6m, 1y, and Custom. When selected, the data for that time frame is retrieved and the corresponding graph is displayed.

Related Topics

Types of Reports for Access Points, on page 229

View Access Point Radio Air Time Fairness Information

Cisco Air Time Fairness (ATF) for High Density Experience (HDX) allows network administrators to group devices of a defined category and enables some groups to receive traffic from the WLAN more frequently than other groups. Therefore, some groups are entitled to more air time than other groups.

Cisco ATF has the following capabilities:

- Allocates Wi-Fi air time for user groups or device categories
- Air time fairness is defined by the network administrator and not by the network
- Provides a simplified mechanism for allocating air time
- Dynamically adapts to changing conditions in a WLAN
- Enables a more efficient fulfillment of service-level agreements
- Augments standards-based Wi-Fi QoS mechanisms

To monitor the ATF Statistics:

Step 1 Choose Monitor > Wireless Technologies > Access Point Radios.

Step 2 Click the desired radio name in the Radio column.

Depending on the type of access point, different tabs are displayed.

Step 3 In the Access Point Radio Details, choose the Air Time Fairness tab.

The following charts are displayed:

- Air Time Usage Absolute—This chart represents the percent Air Time Usage by a WLAN on a Radio during the measured interval of time.
  - Click the calendar icon to choose the start date and year and end date and year or choose a preset value. The presets available are 1h, 6h, 1d, 1w, 2w, 4w, 3m, 6m, and 1y.
- Air Time Usage Relative—This chart displays the percent Air Time usage by a WLAN across all WLAN s on a radio.
- Click the calendar icon to choose the start date and year and end date and year or choose a preset value. The presets available are 1h, 6h, 1d, 1w, 2w, 4w, 3m, 6m, and 1y.

What is a Rogue Access Point

A rogue device is an unknown access point or client that is detected by managed access points in your network. Rogue access points can disrupt wireless LAN operations by hijacking legitimate clients and using plain-text or other denial of service or man-in-the-middle attacks. That is, a hacker can use a rogue access point to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of clear-to-send (CTS) frames. This action mimics an access point informing a particular client to transmit and instructing all others to wait, which results in legitimate clients being unable to access network resources.

Therefore, wireless LAN service providers have a strong interest in banning rogue access points from the air space.

Since rogue access points are inexpensive and readily available, employees sometimes plug unauthorized rogue access points into existing LANs and build ad-hoc wireless networks without IT department knowledge or consent. These rogue access points can be a serious breach of network security as they can be plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on the rogue access point, it is easy for unauthorized users to use the access point to intercept network traffic and hijack client sessions. Even more alarming, wireless users frequently publish insecure access point locations, increasing the odds of having enterprise security breached.

Related Topics

How Detects Rogue Access Points, on page 233
How Rogue Access Point States Are Determined, on page 233
View Rogue Access Point Alarms, on page 236
What is an Ad hoc Rogue, on page 238
View Rogue Access Point Clients , on page 237
How Locates, Tags, and Contains Rogue Access Points , on page 238

How Detects Rogue Access Points

Controllers continuously monitor all nearby access points and automatically discover and collect information on rogue access points and clients. When a controller discovers a rogue access point, it uses the Rogue Location Discovery Protocol (RLDP) to determine if the rogue is attached to your network. consolidates all of the controllers rogue access point data.

You can configure controllers to use RLDP on all access points or only on access points configured for monitor (listen-only) mode. The latter option facilitates automated rogue access point detection in a crowded RF space, allowing monitoring without creating unnecessary interference and without affecting regular data access point functionality. If you configure a controller to use RLDP on all access points, the controller always chooses the monitor access point for RLDP operation if a monitor access point and a local (data) access point are both nearby. If RLDP determines that the rogue is on your network, you can choose to either manually or automatically contain the detected rogue.

Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

Related Topics

What is a Rogue Access Point, on page 232
How Rogue Access Point States Are Determined, on page 233
View Rogue Access Point Alarms, on page 236
View Ad Hoc Rogue Access Point Alarms, on page 238

How Rogue Access Point States Are Determined

Classification and reporting of rogue access points occurs through the use of rogue states and user-defined classification rules that enable rogues to automatically move between states. You can create rules that enable the controller to organize and display rogue access points as Friendly, Malicious, or Unclassified.

By default, none of the classification rules are enabled. Therefore, all unknown access points are categorized as Unclassified. When you create a rule, configure conditions for it, and enable the rule, the unclassified access points are reclassified. Whenever you change a rule, it is applied to all access points (friendly, malicious, and unclassified) in the Alert state only. Rule-based rogue classification does not apply to ad-hoc rogues and rogue clients.

The 5500 series controllers support up to 2000 rogues (including acknowledged rogues); the 4400 series controllers, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch support up to 625 rogues; and the 2100 series controllers and Controller Network Module for Integrated Services Routers support up to 125 rogues. Each controller limits the number of rogue containments to three per radio (or six per radio for access points in monitor mode).

When the controller receives a rogue report from one of its managed access points, it responds as follows:

1. The controller verifies whether the unknown access point is in the friendly MAC address list. If it is, the controller classifies the access point as Friendly.
2. If the unknown access point is not in the friendly MAC address list, the controller starts applying rogue classification rules.
3. If the rogue is already classified as Malicious, Alert or Friendly, Internal or External, the controller does not reclassify it automatically. If the rogue is classified differently, the controller reclassifies it automatically only if the rogue is in the Alert state.
4. The controller applies the first rule based on priority. If the rogue access point matches the criteria specified by the rule, the controller classifies the rogue according to the classification type configured for the rule.
5. If the rogue access point does not match any of the configured rules, the controller classifies the rogue as Unclassified.
6. The controller repeats the previous steps for all rogue access points.
7. If RLDP determines that the rogue access point is on the network, the controller marks the rogue state as Threat and classifies it as Malicious automatically, even if no rules are configured. You can then manually contain the rogue (unless you have configured RLDP to automatically contain the rogue), which would change the rogue state to Contained. If the rogue access point is not on the network, the controller marks the rogue state as Alert, and you can manually contain the rogue.
8. If desired, you can manually move the access point to a different classification type and rogue state.

As mentioned previously, the controller can automatically change the classification type and rogue state of an unknown access point based on user-defined rules, or you can manually move the unknown access point to a different classification type and rogue state.

Related Topics

What is a Rogue Access Point, on page 232
How Detects Rogue Access Points, on page 233
How Rogue Access Points are Classified, on page 234

How Rogue Access Points are Classified

The following table shows the allowable classification types and rogue states from and to which an unknown access point can be configured.

Table 29: Allowable Classification Type and Rogue State Transitions

From	To
Friendly (Internal, External, Alert)	Malicious (Alert)

From	To
Friendly (Internal, External, Alert)	Unclassified (Alert)
Friendly (Alert)	Friendly (Internal, External)
Malicious (Alert, Threat)	Friendly (Internal, External)
Malicious (Contained, Contained Pending)	Malicious (Alert)
Unclassified (Alert, Threat)	Friendly (Internal, External)
Unclassified (Contained, Contained Pending)	Unclassified (Alert)
Unclassified (Alert)	Malicious (Alert)

If the rogue state is Contained, you have to uncontain the rogue access point before you can change the classification type. If you want to move a rogue access point from Malicious to Unclassified, you must delete the access point and allow the controller to reclassify it.

Malicious Rogue APs

Malicious rogue access points are detected but untrusted or unknown access points with a malicious intent within the system. They also refer to access points that fit the user-defined malicious rules or have been manually moved from the friendly access point classification.

The Security dashboard of home page displays the number of malicious rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active malicious rogue access points.

Malicious rogue access point states include:

- Alert—Indicates that the access point is not on the neighbor list or part of the user-configured Friendly Access Point list.
- Contained—The unknown access point is contained.
- Threat—The unknown access point is found to be on the network and poses a threat to WLAN security.
- Contained Pending—Indicates that the containment action is delayed due to unavailable resources.
- Removed—This unknown access point was seen earlier but is not seen now.

Click an underlined number in any of the time period categories for detailed information regarding the malicious rogue access points.

Friendly Rogue APs

Friendly rogue access points are known, acknowledged or trusted access points. They also refer to access points that fit the user-defined friendly rogue access point rules. Friendly rogue access points cannot be contained.

Only users can add a rogue access point MAC address to the Friendly Access Point list. does not apply the Friendly Access Point MAC address to controllers.

The Security dashboard of home page displays the number of friendly rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active friendly rogue access points.

Friendly rogue access point states include the following:

- Internal—If the unknown access point is inside the network and poses no threat to WLAN security, you would manually configure it as Friendly, Internal. For example, the access points in your lab network.
- External—If the unknown access point is outside the network and poses no threat to WLAN security, you would manually configure it as Friendly, External. For example, the access points belonging to a neighboring coffee shop.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly Access Point list.

Click an underlined number in any of the time period categories for detailed information regarding the friendly rogue access points.

To delete a rogue access point from the Friendly Access Point list, ensure that both and controller remove the rogue access point from the Friendly Access Point list. Change the rogue access point from Friendly Access Point Internal or External to Unclassified or Malicious Alert.

Unclassified Rogue APs

A rogue access point is called unclassified, if it is not classified as either malicious or friendly. These access points can be contained and can be moved manually to the friendly rogue access point list.

The Security dashboard of the home page displays the number of unclassified rogue access points for each applicable state for the past hour, the past 24 hours, and the total number of active unclassified rogue access points.

Unclassified rogue access point states include:

- Pending—On first detection, the unknown access point is put in the Pending state for 3 minutes. During this time, the managed access points determine if the unknown access point is a neighbor access point.
- Alert—The unknown access point is not on the neighbor list or part of the user-configured Friendly Access Point list.
- Contained—The unknown access point is contained.
- Contained Pending—The unknown access point is marked Contained, but the action is delayed due to unavailable resources.

Click an underlined number in any of the time period categories for further information.

Related Topics

What is a Rogue Access Point, on page 232
How Detects Rogue Access Points, on page 233

View Rogue Access Point Alarms

Rogue access point radios are unauthorized access points detected by one or more Cisco 1000 series lightweight access points. To open the Rogue Access Point Alarms page, do one of the following:

- Search for rogue APs.
- Navigate to Dashboard > Wireless > Security. This page displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the AP number link in the Alarm Summary.

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use it to view additional alarms.

Rogue access point partitions are associated with one of the detecting access points (the one with the latest or strongest RSSI value). If there is detecting access point information, uses the detecting controller. If the rogue access point is detected by two controllers which are in different partitions, the rogue access point partition might be changed at any time.

When polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Alarm event details for each rogue access point are available in the Rogue Access Point Alarms list page.

To view alarm events for a rogue access point radio, select Monitor > Monitoring Tools > Alarms and Events, and click the arrow icon in a row to view Rogue Access Point Alarm Details page.

All Alarm Details page fields (except No. of Rogue Clients) are populated through polling and are updated every two hours. The number of rogue clients is a real-time number and is updated each time you access the Alarm Details page for a rogue access point alarm.

When a controller (version 7.4 or 7.5) sends custom rogue Access Point alarm, shows it as unclassified rogue alarm. This is because does not support custom rogue Access Point alarm.

When polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

View Rogue Access Point Clients

You can view a list of rogue clients in several ways:

- Perform a search for rogue clients using feature.
- View the list of rogue clients for a specific rogue access point from the Alarm Details page for the applicable rogue access point. Click the Rogue MAC address for the applicable rogue client to view the Rogue Client details page.
- In the Alarms Details page of a rogue access point, choose Rogue Clients from the Select a command drop-down list.

The Rogue Clients page displays the Client MAC address, when it was last heard, its current status, its controller, and the associated rogue access point.

Rogue client statuses include: Contained (the controller contains the offending device so that its signals no longer interfere with authorized clients); Alert (the controller forwards an immediate alert to the system administrator for further action); and Threat (the rogue is a known threat). The higher the threat of the rogue access point, the higher the containment required.

Click the Client MAC Address for the rogue client to view the Rogue Client details page.

Related Topics

What is a Rogue Access Point, on page 232
View Rogue Access Point Alarms, on page 236
View Ad Hoc Rogue Access Point Alarms, on page 238

What is an Ad hoc Rogue

If the MAC address of a mobile client operating in a ad hoc network is not in the authorized MAC address list, then it is identified as an ad hoc rogue.

Related Topics

View Ad Hoc Rogue Access Point Alarms, on page 238
View Rogue Access Point Clients , on page 237

View Ad Hoc Rogue Access Point Alarms

The Adhoc Rogue Alarms page displays alarm events for ad hoc rogues. To access the Adhoc Rogue Alarms page, do one of the following:

- Perform a search for ad hoc rogue alarms.
- Navigate to Dashboard > Wireless > Security. This page displays all the ad hoc rogues detected in the past hour and the past 24 hours. Click the ad hoc rogue number to view the ad hoc rogue alarms.

If there are multiple alarm pages, the page numbers are displayed at the top of the page with a scroll arrow on each side. Use this to view additional alarms.

When polls, some data might change or get updated. Because of this, some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Alarm event details for each ad hoc rogue is available on the Adhoc Rogue Alarms page. Rogue access point radios are unauthorized access points detected by Cisco 1000 Series Lightweight APs.

To view alarm events for an ad hoc rogue radio, click the applicable Rogue MAC address in the Adhoc Rogue Alarms page.

When polls, some data might change or get updated. Hence some of the displayed rogue data (including Strongest AP RSSI, No. of Rogue Clients, Channel, SSID, and Radio Types) can change during the life of the rogue.

Alarms will not be triggered if a rogue is discovered using switch port tracing as switch port tracing does not update any of the rogue attributes such as severity, state, and so on.

How Locates, Tags, and Contains Rogue Access Points

generates the flags as rogue access point traps and displays the known rogue access points by MAC address Cisco Unified Network Solution is monitoring it.

The operator displays a map showing the location of the access points closest to each rogue access point. These access points are classified as:

- Known or Acknowledged rogue access points (no further action)
- Alert rogue access points (watch for and notify when active)
- Contained rogue access points

This built-in detection, tagging, monitoring, and containment capability enables system administrators to take appropriate action:

- Locate rogue access points.

- Receive new rogue access point notifications, eliminating hallway scans.
- Monitor unknown rogue access points until they are eliminated or acknowledged.
- Determine the closest authorized access point, making directed scans faster and more effective.
- Contain rogue access points by sending their clients deauthenticate and disassociate messages from one to four access points. This containment can be done for individual rogue access points by MAC address or can be mandated for all rogue access points connected to the enterprise subnet.
- Tag rogue access points:
  - Acknowledge rogue access points when they are outside of the LAN and do not compromise the LAN or WLAN security
  - Accept rogue access points when they do not compromise the LAN or WLAN security
  - Tag rogue access points as unknown until they are eliminated or acknowledged
- Tag rogue access points as contained and discourage clients from associating with the rogue access points by having between one and four access points transmit deauthenticate and disassociate messages to all rogue access point clients. This function applies to all active channels on the same rogue access point.

Related Topics

Identify the Lightweight Access Points That Detect Rogue Access Points, on page 239

Identify the Lightweight Access Points That Detect Rogue Access Points

Use the Detecting Access Points feature to view information about the Cisco Lightweight APs that are detecting a rogue access point.

To access the Rogue Access Point Alarms details page, follow these steps:

Step 1 To display the Rogue Access Point Alarms page, do one of the following:

- Perform a search for rogue Access Points
- Navigate to Dashboard > Wireless > Security. This dashboard displays all the rogue access points detected in the past hour and the past 24 hours. Click the rogue access point number to view the rogue access point alarms.
- Click the Malicious AP number link in the Alarm Summary box.

Step 2 In the Rogue Access Point Alarms page, click the Rogue MAC Address for the applicable rogue access point. The Rogue Access Point Alarms details page appears.

Step 3 From the Select a command drop-down list, choose Detecting APs.

Step 4 Click Go.

Click a list item to display data about that item.

Related Topics

How Locates, Tags, and Contains Rogue Access Points , on page 238

View Access Points Interference Information from Spectrum Experts

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to . This feature allows to collect, archive and monitor detailed interferer and air quality data from Spectrum Experts in the network.

To access the Monitor Spectrum Experts page, follow these steps:

Choose Services > Mobility Services > Spectrum Experts.

From the left sidebar menu, you can access the Spectrum Experts Summary page.

Monitor WiFi TDOA Receivers

The WiFi TDOA receiver is an external system designed to receive signals transmitted from a tagged, tracked asset. These signals are then forwarded to the mobility services engine to aid in the location calculation of the asset.

Related Topics

Enhance Tag Location Reporting with WiFi TDOA Receivers, on page 329
Add WiFi TDOA Receivers to and Maps, on page 330

View RF Performance Using Radio Resource Management Dashboard

The Radio Resource Management (RRM), built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment. receives traps whenever a change in the transmit power in the access point or channel occurred. These trap events or similar events such as RF regrouping are logged into and are maintained by the event dispatcher.

RRM automatically detects and configures new controllers and lightweight access points as they are added to the network. It automatically adjusts associated and nearby lightweight access points to optimize coverage and capacity. Lightweight access points can simultaneously scan all valid 802.11b/g channels for the country of operation as well as for channels available in other locations. The access points go off-channel for a period not greater than 60 ms to monitor these channels for noise and interference. Packets collected during this time are analyzed to detect rogue access points, rogue clients, ad-hoc clients, and interfering access points.

The following notifications are sent to RRM dashboard:

- Channel change notifications are sent when a channel change occurs. Channel change depends on the Dynamic Channel Assignment (DCA) configuration.
- Transmission power change notifications are sent when transmission power changes occur. The reason code is factored and equated to one irrespective of the number of reasons for the event to occur.

- RF grouping notifications are sent when there is a RF grouping content change and automatic grouping is enabled.

To view the RRM dashboard information choose Monitor > Wireless Technologies > Radio Resource Management.

View Access Points Alarms and Events

To monitor the Access Point alarms on your network:

Step 1 Perform an advanced search for the following:
a) Performance alarms
b) CleanAir Security alarms
c) wIPS DoS alarms

Step 2 Select the check box next to the alarm and modify the required fields in the Alarm Browser toolbar.

View Access Points Failure Objects

To monitor failure objects, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Alarms and Events, then click the Events tab.

Step 2 Click the expand icon to the left of the Description column. Depending on the type of event you selected, the associated details vary.

View Access Points Rogue Access Points

To monitor events for rogue access points:

Step 1 Choose Monitor > Monitoring Tools > Alarms and Events, then click the Events tab.

Step 2 Use the Quick Filter or Advanced Filter feature to monitor the Rogue APs.

Step 3 Click the expand icon to view alarm events for a rogue access point radio.

View Access Points Ad Hoc Rogues

To monitor events for ad hoc rogues:

Procedure

	Command or Action	Purpose
Step 1	Choose Monitor > Monitoring Tools > Alarms and Events, then click the Events tab.	
Step 2	Use the Quick Filter or Advanced Filter feature to monitor the events for Ad hoc Rogue APs.	
Step 3	Click the expand icon to view alarm events for an ad hoc rogue access point.	

Related Topics

What is a Rogue Access Point, on page 232

View Access Points Adaptive wIPS Events

To monitor Cisco adaptive wIPS events:

Step 1 Choose Monitor > Monitoring Tools > Alarms and Events, then click the Events tab.

Step 2 Use the Quick Filter or Advanced Filter feature to narrow down the search results to monitor wIPS events. One or more events might generate an abnormal state or alarm. The alarm can be cleared, but the event remains.

View Access Points CleanAir Air Quality Events

To view the events generated on CleanAir air quality of the wireless network:

Perform an advanced search for Performance event.

The Search Results page contains information about severity, failure Source, and date and time.

What to do next

To view air quality event details click an expand icon adjacent to Severity column in the Air Quality Events page.

View Access Points Interferer Security Risk Events

To monitor interferer security risk events:

To view the security risk event generated on your wireless network, perform an advanced search for Security event.

The Search Results page contains the following CleanAir air quality events information about severity, failure Source, and date and time.

What to do next

To view interferer security event details, click an expand icon adjacent to Severity column to access the alarm details page.

View Access Points Health Monitor Events

To view the health monitor events:

Perform an advanced search for event.

The Search Results page contains information about severity, failure Source, messages and date and time.

View Health Monitor Event Details

To view health monitor event details click an expand icon adjacent to Severity column to access the alarm details page.

Related Topics

View Access Points Health Monitor Events, on page 243

Using Telemetry

This section describes how telemetry is used in Cisco Prime Infrastructure.

Devices that Support Telemetry

In Cisco Prime Infrastructure, telemetry supports the following devices:

- Cisco Catalyst 9800-40 Wireless Controller
- Cisco Catalyst 9800-80 Wireless Controller
- Cisco Catalyst 9800-L-F Wireless Controller
- Cisco Catalyst 9800-CL Wireless Controller for Cloud

Prerequisites for Using Telemetry

- You must enable NETCONF configuration on the Catalyst 9800 WLC.
- You must integrate Coral with the Cisco Prime Infrastructure server.

About Telemetry

Telemetry polls the device and collects telemetry data such as any change on the device like addition or removal of APs and clients.

Ports Used by Telemetry

- Prime Infrastructure to WLC: TCP port 830

  This is used by Cisco Prime Infrastructure to push the telemetry configuration to the 9800 devices using NETCONF.

- WLC to Prime Infrastructure: TCP port 20828 (for IOS-XE 16.10 and 16.11, Cisco PI 3.5 to 3.7).

  or

  TCP port 20830 (for IOS-XE 16.12,17.x and later, Cisco PI 3.8 onwards).

Note In case there is a firewall between Cisco Prime Infrastructure and Catalyst 9800, be sure to open these ports to establish communication

Difference Between Telemetry and SNMP in Cisco Prime Infrastructure

In SNMP, Cisco PI fetches the data from the device. It will also use SNMP to push configuration templates as well as support traps for AP and client events.

In telemetry, Cisco PI registers itself as a receiver to receive telemetry data and PI keeps listening to the device. The device is responsible for sending data such as discovery data and association and disassociation data of APs and clients. Telemetry does not fetch configuration data as in SNMP.

Verify Telemetry Status

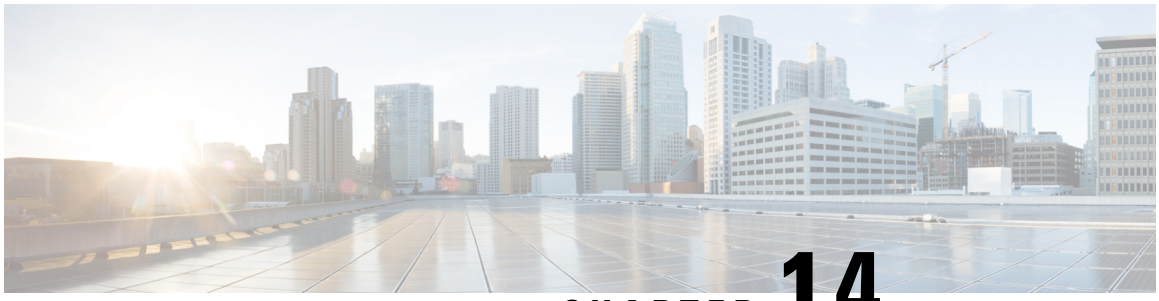
To verify the telemetry connection to Prime from the C9800, use the show telemetry internal connection command.

```
#show telemetry internal connection
Telemetry connection

Address Port Transport State Profile
------------------------------------------------------------------
x.x.x.x 20828 cntp-tcp Active
```

If you have any issues with telemetry, you must collect the prime coral logs such as “Prime_TDL_collector_R0-”* logs.

For more information on telemetry on Cisco PI, see Managing Catalyst 9800 Wireless Controller Series with Prime Infrastructure using SNMP v2 and SNMP v3 and NetCONF.



CHAPTER 14

Monitor Device and Network Health and Performance

This chapter contains the following topics:

How Device Health and Performance Is Monitored: Monitoring Policies

Monitoring policies control how monitors your network by controlling the following:

- What is monitored—The network and device attributes monitors.
- How often it is monitored—The rate at which parameters are polled.
- When to indicate a problem—Acceptable values for the polled attributes.
- How to indicate a problem—Whether should generate an alarm if a threshold is surpassed, and what the alarm severity should be.

Monitoring policies are important because apart from controlling what is monitored, they determine what data can be displayed in reports, dashboards, and other areas of . Monitoring policies do not make any changes on devices.

Only device health monitoring (that is, the Device Health monitoring policy) is enabled by default. Interface Health monitoring is not enabled by default to protect system performance in large deployments.

These steps summarize how you can configure a monitoring policy.

1. Use a monitoring policy type as a template for your monitoring policy, and give the policy a name that is meaningful to you. Policy types are packaged with and make it easy for you to start monitoring different technologies and services.
2. Adjust your policy's polling frequencies or disable polling altogether for specific parameters.
3. Specify the threshold crossing alarms (TCAs) you want to generate if a parameter's threshold is surpassed. Some TCAs are configured by default; you can adjust or disable them, and configure new TCAs.
4. Specify the devices you want your policy to monitor. Devices are filtered depending on the policy type.
5. Activate your policy. The polled data will be displayed in dashboards, reports, the Alarms and Events table, and other areas of the web GUI.

To view and administer monitoring policies, choose Monitor > Monitoring Tools > Monitoring Policies.

Navigation	Description
Automonitoring	Lists the policies that are enabled by default in . Only the Device Health monitoring policy is enabled by default. You can adjust the settings for this policy.
My Policies	The policy you create is listed here. When you choose a policy from My Policies, you can view the policy's details.

Set Up Basic Device Health Monitoring

The Device Health monitoring policy is enabled by default. It monitors both Cisco devices and third-party devices. For Cisco devices, the device health monitoring checks managed devices for CPU utilization, memory pool utilization, environment temperature, and device availability. For third party devices, the device health monitoring checks managed devices for device availability only. This policy also specifies thresholds for utilization and temperature which, if surpassed, trigger alarms that are displayed in the GUI client.

To view the current settings for this policy, choose Monitor > Monitoring Tools > Monitoring Policies, then select Automonitoring from the list on the left. You can also adjust the polling frequency and threshold for the different parameters. To adjust a polling frequency or threshold, use the drop-down lists that are provided in the GUI client.

You might also want to create a device health monitoring policy that monitors specific devices—for example, devices of a certain type or in a certain geographical location. For instructions on how to do this, see Adjust What Is Being Monitored, on page 253.

Set Up Basic Interface Monitoring

Interfaces are not monitored by default. This protects system performance for networks with large numbers of interfaces.

Use this procedure to set up basic interface monitoring.

To set up and enable interface monitoring:

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies, then select My Policies from the list on the left.

Step 2 Click Add to create a new policy.

Step 3 Choose Interface Health for generic interface monitoring.

When you select a policy, populates the window with the policy settings.

Step 4 Enter a meaningful name and description.

Step 5 From the Device Selection drop-down list, click the appropriate radio button and then select the devices or device groups you want to monitor. If you chose the Interface Health monitoring policy, you can also select port groups.

only lists the devices or ports applicable to the policy you selected in Step 3.

Note the following:

- If you want to use the default settings for polling and thresholds, proceed to Step 8.
- Due to a limitation in the current release of , the Interface Health monitoring policy polls all of the interfaces in your network for cyclic redundancy check (CRC) error data, not just the ones associated with the selected port group. Keep this in mind whenever you view CRC error data.

Step 6 To adjust how often the interface is polled, select a value from the Polling Frequency drop-down list. Some policies allow you to set polling frequencies for different parameters, while other policies have only one polling frequency that is applied to all parameters.

Step 7 If the policy supports TCA customization, you can adjust the thresholds. See Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 260.

Step 8 Click:

- Save and Activate to start monitoring immediately
- Save and Close to save the policy and activate it at a later time

Default Monitoring Policies

Prime Infrastructure polls SNMP objects to gather monitoring information for the following health monitoring policies under Monitor > Monitoring Tools > Monitoring Policies > Automonitoring:

- Device Parameters—The table Device Parameter Automonitoring Metrics describes the device health parameters that are polled.
- Interface Parameters—The table Interface Parameter Automonitoring Metrics describes the interface parameters that are polled for:
  - Trunk and Link Ports
  - WAN Interfaces

For the following monitoring policies that provide assurance information, data is collected through NetFlow or NAMs:

- Application Response Time

- NAM Health
- Traffic Analysis
- Voice Video Data
- Voice Video Signaling

Table 30: Device Parameter Automonitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
Device Availability	All SNMP devices, Third Party devices	SNMPv2-MIB	sysUpTime
CPU Utilization	Cisco IOS devices, All Supported Nexus devices, Cisco UCS devices	CISCO-PROCESS-MIB	cpmCPUTotalPhysicalIndex cpmCPUTotal1minRev
	Cisco ASR device	CISCO-ENTITY-QFP-MIB	
Memory Pool Utilization	Cisco IOS devices, ISR devices.	CISCO-MEMORY-POOL-MIB	ciscoMemoryPoolName ciscoMemoryPoolType ciscoMemoryPoolUsed ciscoMemoryPoolFree
	All supported Cisco Nexus devices, Cisco UCS devices and Cisco IOS XE devices	CISCO-PROCESS-MIB	cpmCPUTotalIndexcpmCPUMemoryUsedcpmCPUMemoryFree
	Cisco ASA devices, IOS XR and Edison devices	CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTypecempMemPoolNamecempMemPoolUsedcempMemPoolFree
	Cisco IOS ASR devices	CISCO-ENTITY-QFP-MIB	ceqfpMemoryResTypeceqfpMemoryResInUseceqfpMemoryResFree
Environment Temp[1]	ASR, All Supported Nexus devices, Cisco UCS devices	CISCO-ENVMON-MIB	entSensorValue
	Catalyst 2000, 3000, 4000, 6000, ISR	CISCO-ENVMON-MIB	ciscoEnvMonTemperatureStatusValue

[1] For stacked switch devices, the Environment Temp displays the temperature of each stacked instance.

Table 31: Interface Parameter Automonitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
Interface Availability	Cisco IOS devices, All Supported Nexus devices, and Third Party devices	IF-MIB	ifOperStatus

Metric	Devices Polled	MIB	MIB Objects Included
Input Utilization	Cisco IOS devices, Third Party devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifInErrors, ifInDiscards, ifInUnknownProtos ifHCInBroadcastPkts, ifHCInMulticastPkts, locIfInputQueueDrops
Output Utilization	Cisco IOS devices, Third Party devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCOutBroadcastPkts, ifHCOutMulticastPkts, ifHCOutUcastPkts, ifOutDiscards, ifOutUnknownProtos, locIfOutputQueueDrops
Percent Drop per QoS Class	Cisco IOS devices	IF-MIB, Old-CISCO-Interface-MIB	cbQosCMDropBitRate,cbQosCMPrePolicyBitRate

Note locIfIn, outQueueDrops, and QOS monitoring are not supported for third party devices.

Table 32: Class-Based, QoS, Health-Monitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
QOS calculation	Cisco IOS devices	CISCO-CLASS-BASED-QOS-MIB	cbQosCMDropByte64 cbQosCMPostPolicyByte64 cbQosCMPrePolicyByte64
Interface Inbound Errors	Cisco IOS devices, Third party devices	IF-MIB	ifInErrors
Interface Outbound Errors	Cisco IOS devices, Third party devices	IF-MIB	ifOutErrors
Interface Inbound Discards	Cisco IOS devices, Third party devices	IF-MIB	ifInDiscards
Interface Outbound Discards	Cisco IOS devices, Third party devices	IF-MIB	ifOutDiscards

Modify Default Monitoring Policies

Prime Infrastructure monitoring policies monitor network device metrics and alert you of changing conditions before the issues impact their operation. By default, Prime Infrastructure polls device health metrics on supported routers, switches and hubs and third party devices, and interface health metrics on WAN interfaces, links, and trunk ports. It is not polled on storage devices, and UCS series devices. If a the threshold is violated three times, Prime Infrastructure generates a critical alarm, which is displayed on the Monitor > Monitoring Tools > Alarms and Events page.

To modify or disable the polling frequency and the threshold parameters, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies > Automonitoring.

Step 2 Select Device Health, then modify the polling frequencies and thresholds as desired.

Step 3 Click:

- Save and Activate to save and activate the policy immediately on the selected devices.
- Save and Close to save the policy and activate it at a later time.

Use the Dashboards To Check Network and Device Health

provides a variety of dashboards for monitoring your devices and network. The following are some examples of what dashboards can provide:

- Network-wide real-time status information, such as unreachable devices, interfaces that are down, and the most recent alarms.
- Summarized historical information, such as the most frequently-occurring alarms, and the devices and interfaces with the highest memory and CPU utilization.
- Device-specific information, such as a device's availability history, utilization, interface statistics, and alarms.
- Technology-specific information.

For information on dashboards, see Set Up and Use the Dashboards, on page 6.

Check What Is Monitoring

This topic explains how to get the following information:

- Which policies are activated, their status, and their history.
- The specific parameters that is polling, the frequency at which they are polled, and their threshold crossing alarm (TCA) settings.
- Who created the policy and which policy type they used as its basis.

To find out what a policy polls, when the policy last ran, and whether the policy is currently active, choose Monitor > Monitoring Tools > Monitoring Policies, then choose My Policies. lists the monitoring policies you created or have access to, with the following information.

Policy Field	Description
Name	Policy name (specified by the policy creator). To find out who created a policy, see the instructions that follow this table.
	Policy description (specified by the policy creator).

Policy Field	Description
Type	Template (policy type) used to create this policy. For information on the policy types, see How Device Health and Performance Is Monitored: Monitoring Policies, on page 245.
Status	Active or Inactive.
Threshold	Whether the policy monitors parameter thresholds and generates TCAs. If Yes is displayed, you can check the TCA settings using the instructions that follow this table.
Activation History	Active monitoring policy—Displays the number of times the policy was activated, and provides a hyperlink to an Activation History popup window that tells you: • When the policy was activated. • Which devices were polled at each policy run. If the list is very long, hover your mouse cursor over the list in the Activated for column to launch a popup window. Inactive monitoring policy—Displays Not Available.
Collection Status	Active monitoring policy—Provides a hyperlink to a Collection Status popup window that tells you: • Which parameters were polled at each policy run. If the list is very long, hover your mouse cursor over the list in the Parameters column to launch a popup window. Inactive monitoring policy—Displays Not Available.

To view polling frequencies and TCA details, from My Policies, select a policy from the list on the left. Depending on the policy type, the following information is displayed.

Policy Field	Description
General Information	Name, description, creator, status, policy type (Feature Category). For information on the policy types, see How Device Health and Performance Is Monitored: Monitoring Policies, on page 245.
Device Selection	Devices which the policy is monitoring.
Polling Frequency	How often polls the device parameters.

Policy Field	Description
Parameters and Thresholds	Which parameters are polled and their TCA settings, if any. To view the TCA settings, click the arrow next to the parameter name. For more information about viewing the parameters polled by the various policy types, see Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 252.

Check Which Parameters and Counters Are Polled By a Monitoring Policy

Check What Is Monitoring, on page 250 explains how to find out which monitoring policies are currently activated. To find out which parameters are being polled by a policy, follow this procedure.

You can use this procedure to check:

- Parameters polled by existing policies (regardless of whether a policy is active or inactive).
- Parameters used by a policy type. This is useful if you want to check what a new policy will poll before creating the policy.

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies, then choose My Policies. The web GUI lists the existing active and inactive monitoring policies.

Step 2 To check the parameters used by an existing policy:

- To view parameters that were polled most recently, locate the policy in the window on the right, then click Details in the Collection Status column. In the Collection Data dialog box, hover your mouse over the text in the Parameter column to list the polled parameters.
- To view the parameters along with their polling settings, expand My Policies in the navigation area on the left, then choose the policy you want to check. The window on the right displays the parameters and their polling settings.

Step 3 To check the parameters used by a specific policy type:

a) Click Edit. The supported policy types are listed in the navigation area on the left.
b) Choose a policy type. The window on the right displays the parameters polled by that policy, along with default polling and TCA settings. (These settings can be customized when a monitoring policy is created.)

Check a Monitoring Policy's Device, Polling, Threshold, and Alarm Settings

To check a monitoring policy's threshold and alarm settings:

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies, then choose My Policies.

Step 2 Select the monitoring policy and click Edit to open the policy details.

Step 3 To find out which devices the policy is monitoring, click the Device Selection drop-down list. Devices that are monitored are indicated with a check mark. To add or remove devices, see Change the Device Set a Policy is Monitoring, on page 259.

Step 4 To find out the polling interval the policy is using, check the Polling Interval setting. For per-parameter polling, you must expand the individual parameters to see the setting. To adjust the polling settings, see Change the Polling for a Monitoring Policy, on page 260.

Step 5 To find out the thresholds and alarm settings the policy is using, expand the parameter in the Polling and Thresholds area. To change the threshold and alarm settings, see Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 260.

Adjust What Is Being Monitored

To make adjustments to what is monitoring, use the guidance in the following table to find the best method for your needs.

If:		See:
is collecting the data you need, and...	... you want to change the polling frequency	Change the Polling for a Monitoring Policy, on page 260
	... you want to adjust the alarm behavior	Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 260
	... you want to adjust which devices are monitored	Change the Device Set a Policy is Monitoring, on page 259
is not collecting the data you need, and...	... a similar monitoring policy already exists	Create a New Monitoring Policy Based On An Existing Policy, on page 253
	... no similar monitoring policies exist, but one of the policy types contains the parameters you want to monitor	Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 254
	... no similar monitoring policies exist, and none of the policy types contain the parameters you want to monitor	Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 258
	... you want it to monitor unsupported or third-party devices	

Create a New Monitoring Policy Based On An Existing Policy

Step 1 Check what is currently being monitored to verify that you need to create a new policy. See Check What Is Monitoring, on page 250.

Step 2 Create the duplicate.

a) Choose Monitor > Monitoring Tools > Monitoring Policies, then click My Policies from the list on the left.

b) Locate the policy you want to duplicate.

c) Select the policy, then click Duplicate.
d) In the Duplicate Policy Creation dialog, choose the parent folder, enter a policy name and description, then click OK.

Step 3 Make your changes to the duplicate.

a) Locate the policy under My Policies.
b) Select the policy and click Edit.
c) Make your changes as needed. See:

- Change the Device Set a Policy is Monitoring, on page 259
- Change the Polling for a Monitoring Policy, on page 260
- Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 260

Step 4 Click:

- Save and Activate to save and activate the policy immediately on the selected devices.
- Save and Close to save the policy and activate it at a later time.

Create a New Monitoring Policy Using Out-of-the-Box Policy Types

Step 1 Check what is currently being monitored. See Check What Is Monitoring, on page 250.

Step 2 Choose Monitor > Monitoring Tools > Monitoring Policies, then click Add.

Step 3 Select the policy type template you want to use from the Policy Types menu.

Step 4 Configure the new policy:

a) Select the devices, device groups, or port groups from the Device Selection drop-down list. (Not all monitoring types can be applied to port groups.)
b) Enter a name and contact, and edit the description.
c) Under Parameters and Thresholds, configure the polling settings, parameter values, and alarm conditions. See Change the Polling for a Monitoring Policy, on page 260 and Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 260.

Step 5 Click:

- Save and Activate to save and activate the policy immediately on the selected devices.
- Save and Close to save the policy and activate it at a later time.

GETVPN Monitoring Policies

For the GETVPN policy type, Prime Infrastructure uses metrics described in the following table.

Table 33:

GETVPN Monitoring Parameters	MIB	MIB Objects Included
Group Name Group ID Group ID Type Group ID Length Key Server ID Group Member ID Device Type Device ID Device ID Type Device ID length Registered Key Server ID Registered Key Server ID Type Registered Key Server ID Length	CISCO-GDOI-MIB	gmGdoiGroupTable cgmGdoiGroupName, cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGroupIdLength cgmGdoiKeyServerTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiKeyServerIdValue, cgmGdoiKeyServerIdType, cgmGdoiKeyServerIdLength, cgmGdoiKeyServerActiveKEK, cgmGdoiKeyServerRekeysPushed cgmGdoiKsKekTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiKeyServerIdValue, cgmGdoiKeyServerIdType, cgmGdoiKsKekIndex, cgmGdoiKsKekSPI, cgmGdoiKsKekSrcIdValue, cgmGdoiKsKekSrcIdType, cgmGdoiKsKekSrcIdLength, cgmGdoiKsKekDstIdValue, cgmGdoiKsKekDstIdType, cgmGdoiKsKekDstIdLength, cgmGdoiKsKekOriginalLifetime, cgmGdoiKsKekRemainingLifetime

GETVPN Monitoring Parameters	MIB	MIB Objects Included
Active KEK Rekeys Count KEK Index KEK SPI KEK Source ID KEK Source ID Type KEK Source ID Length KEK Destination ID KEK Destination ID Type KEK Destination ID Length KEK Original Lifetime KEK Remaining LIfetime TEK Selector Index TEK Source ID TEK Source ID Type TEK Source ID Length TEK Destination ID TEK Destination ID Type TEK Destination ID Length TEK Policy Index TEK SPI TEK Original Lifetime TEK Remaining Lifetime TEK Window Size	CISCO-GDOI-MIB	cgmGdoiKsTekSelectorTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiKeyServerIdValue, cgmGdoiKeyServerIdType, cgmGdoiKsTekSelectorIndex, cgmGdoiKsTekSrcIdValue, cgmGdoiKsTekSrcIdType, cgmGdoiKsTekSrcIdLength, cgmGdoiKsTekDstIdValue, cgmGdoiKsTekDstIdType, cgmGdoiKsTekDstIdLength cgmGdoiKsTekPolicyTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiKeyServerIdValue, cgmGdoiKeyServerIdType, cgmGdoiKsTekPolicyIndex, cgmGdoiKsTekSPI, cgmGdoiKsTekOriginalLifetime, cgmGdoiKsTekRemainingLifetime, cgmGdoiKsTekWindowSize cgmGdoiGmTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmIdLength, cgmGdoiGmRegKeyServerIdValue, cgmGdoiGmRegKeyServerIdType, cgmGdoiGmRegKeyServerIdLength, cgmGdoiGmActiveKEK, cgmGdoiGmRekeysReceived cgmGdoiGmKekTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmKekIndex, cgmGdoiGmKekSPI, cgmGdoiGmKekSrcIdValue, cgmGdoiGmKekSrcIdType, cgmGdoiGmKekSrcIdLength, cgmGdoiGmKekDstIdValue, cgmGdoiGmKekDstIdType, cgmGdoiGmKekDstIdLength, cgmGdoiGmKekOriginalLifetime, cgmGdoiGmKekRemainingLifetime cgmGdoiGmTekSelectorTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmTekSelectorIndex, cgmGdoiGmTekSrcIdValue, cgmGdoiGmTekSrcIdType, cgmGdoiGmTekSrcIdLength, cgmGdoiGmTekDstIdValue, cgmGdoiGmTekDstIdType, cgmGdoiGmTekDstIdLength cgmGdoiGmTekPolicyTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmTekPolicyIndex, cgmGdoiGmTekSPI, cgmGdoiGmTekOriginalLifetime, cgmGdoiGmTekRemainingLifetime, cgmGdoiGmTekWindowSize

DMVPN Monitoring Policies

For the DMVPN policy type, Prime Infrastructure uses metrics described in the following table.

Table 34: Monitor > Monitoring Tools > Monitoring Policies > DMVPN Metrics

DMVPN Monitoring Parameters	MIB	MIB Objects Included
Remote Peer Physical IP Decrypted Byte Count Encrypted Byte Count Remote Tunnel IP NHRP Expiration Remote Subnet IP Remote Subnet Mask	CISCO-IPSEC-FLOW-MONITOR-MIB	cipSecTunnelTable cipSecTunRemoteAddr, cipSecTunInOctets, cipSecTunOutOctets
	NHRP-MIB	nhrpCacheTable nhrpCacheInternetworkAddr, nhrpCacheHoldingTime, nhrpCacheNbmaAddr, nhrpCacheType
	IP-FORWARD-MIB	pCidrRouteTable ipCidrRouteNextHop, ipCidrRouteDest, ipCidrRouteMask

LISP Monitoring Policy

For the LISP monitoring policy type, <Product Name> uses the metrics shown in the following table.

Table 35: Monitor > Monitoring Tools > Monitoring Policies > LISP Monitoring

LISP Monitoring Parameters	MIB	MIB Objects Included
LISP Map Cache Size	LISP-MIB	lispFeaturesMapCacheSize
LISP Map Cache Limit	LISP-MIB	lispFeaturesMapCacheLimit

You can view the polled data in the Device Lisp Map Cache Entries dashlet under Device dashboard and in the Top N Lisp Map Cache Entries dashlet under the Network Devices dashboard.

Nexus Virtual Port Channel (VPC) Health Monitoring Policy

The Nexus VPC health monitoring policy periodically fetches the configuration parameters from the primary VPC configured Nexus Switch and looks for any discrepancies in the configuration that can lead to inconsistencies, by correlating with the secondary VPC configured Nexus Switch. If inconsistencies are detected the monitoring policy generates an alarm and captures the details of the inconsistency at global level and VPC level. The following table describes the Nexus VPC Health Monitoring policy parameters.

Table 36: Monitor > Monitoring Tools > Monitoring Policies > Nexus VPC Health

Category	Nexus VPC Monitoring Parameters
Global Fault	stpModestp, Disabled, stpMstRegionName, stpMstRegionRevision, stpMstRegionVlanMap, stpLoopguard, stpBridgeAssurance, stpEdgePortType, bpduFilterGuard, stpMstSimulatePvst, passVlans
VPC Fault	VpcCardType, OperationalPortMode, Mode, LacpMode, InterfaceType, AdminPortMode, Speed, Duplex, Mtu, NativeVlan,StpPortType, StpPortGuard, StpMstSimulatePvst

Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices

You can design custom MIB polling policies to monitor third-party or Cisco devices and device groups. You can also create custom MIB policies to monitor device features for which doesn't provide default policies. Using this feature, you can:

- Upload the SNMP MIB for the device type, then choose devices and attributes to poll and the polling frequency.
- Upload a single MIB definition file or a group of MIBs with their dependencies as a ZIP file.
- Display the results as a line chart or a table.

This feature allows you to easily repeat polling for the same devices and attributes and customize the way Cisco devices are polled using SNMP.

You can create a maximum of 25 custom MIB polling policies.

To create a custom MIB polling policies, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies, then choose My Policies and click Add.

Step 2 From the Policy Types menu, select Custom MIB Polling.

Step 3 Enter a name for the policy.

Step 4 Under the MIB Selection tab, specify the polling frequency and enter the MIB information.

- If does not list the MIB you want to monitor in the MIBs drop-down list, download the MIBs you want to monitor from the following URL: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2
- To upload a MIB, specify a filename extension only if you are uploading a ZIP file.
- If you are uploading a ZIP file, ensure that all dependent MIB files are either included in the ZIP or already present in the system.
- Ensure your upload file and the MIB definition have the same name. If you are uploading a ZIP file, you may name it as you please, but the MIB files packaged inside it must also follow the same convention (for example: MyMibs.zip is acceptable, as long as all MIB files in the ZIP match their MIB names).

Step 5 To test the policy you created on a device before activating it, click the Test tab and select a device on which to test the new policy.

Step 6 Click Save and Activate to immediately activate the policy on the devices specified.

Step 7 To view the MIB polling data, create a generic dashlet on the Performance dashboard using the name of the policy that you created.

Note To view the SNMP polling date for Cisco ASR devices, you should use the show platform hardware qfp active datapath utilization | inc Processing command for CPU utilization and show platform hardware qfp active infrastructure exmem statistics | sec DRAM command for memory utilization.

Example: Monitor IP SLA

You can create a monitoring policy to view IP service levels for network-based applications and services. There are approximately seven IP SLA-related MIBs. In this example, the video MIB only is monitored.

Step 1 Download the IP SLA video MIB from the following URL: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2

Step 2 ChooseMonitor > Monitoring Policies > My Policies, then click Add.

Step 3 Click Custom MIB Polling.

Step 4 Enter a name for the policy.

Step 5 Under the MIB Selection tab, click Upload MIB and navigate to the MIB that you uploaded in Step 1.

Step 6 From the Tables pulldown menu, select a table, then select the specific metrics to monitor.

Step 7 To test the policy you created on a device before activating it, click the Test tab and select a device on which to test the new policy.

Step 8 Select the devices for which you want to monitor IP SLA metrics.

Step 9 Click Save and Activate to immediately activate the policy on the devices specified.

Step 10 To monitor this information from a dashboard, you need to create a generic dashlet. See Add a Predefined Dashlet To a Dashboard, on page 10 for more information.

Check the Status of Past Monitoring Policy Data Collections

To check a monitoring policy's past data collection:

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies, then click My Policies.

Step 2 Locate the policy, and under the Collection Status, click Details to open the Collection Data dialog. To see which parameters were polled for a device, hover your mouse over the text in the Parameter column.

Change the Device Set a Policy is Monitoring

You can customize how often monitoring information is gathered (polling interval). Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1 Choose Monitor > Monitoring Policies > My Policies and select the policy you want to edit.

Step 2 Check the policy you want to edit and click Edit.

Step 3 Click the Device Selection drop-down list.

Step 4 Select and deselect devices as needed.

Step 5 Click Save and Activate to save and activate the policy immediately on the selected devices.

Change the Polling for a Monitoring Policy

You can customize how often monitoring information is gathered (polling interval). Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies, then click My Policies.

Step 2 Select the policy you want to edit and click Edit.

Step 3 Adjust the polling frequency. How to adjust polling depends on the monitoring policy type.

Step 4 Click Save and Activate to save and activate the policy immediately on the selected devices.

Change Thresholds and Alarm Behavior for a Monitoring Policy

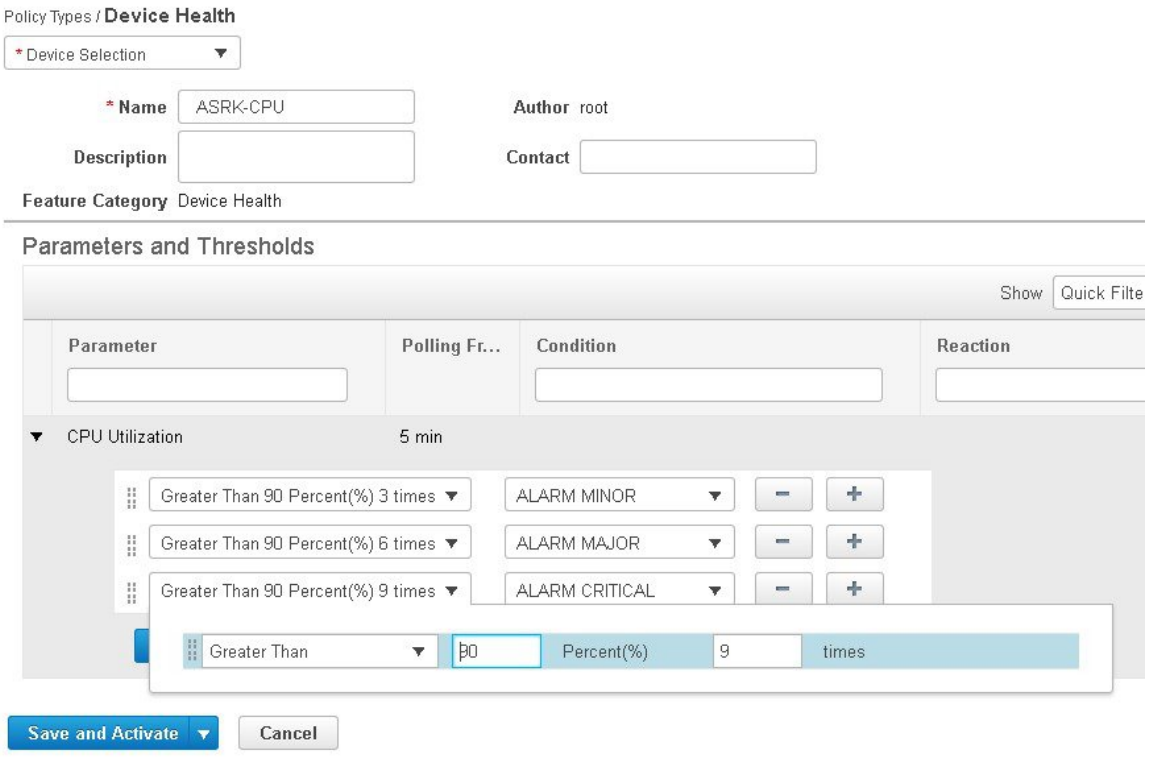
You can customize the threshold value that indicates a problem and whether should generate an informational event or an alarm (of any severity) when a problem is detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies, then choose My Policies.

Step 2 Select the policy you want to edit and click Edit.

Step 3 Locate the parameter you want to change.

Step 4 Expand the parameter. You can change an existing condition or add new conditions, as in the following figure, which specifies thresholds and alarms for CPU utilization on Cisco ASR 9000 devices.



Note You can have only total of 50 thresholds for each metrics as given in the below tables.

Step 5 When you are done, click Save and Activate to save and activate the policy immediately on the selected devices.

Metrics	Parameters
CPU	CPU Utilization
MEMORY	Memory Pool Utilization
ENVTEMP	Environment Temperature
INTERFACE	Interface Inbound Errors, Interface Outbound Errors, Interface Inbound Discards, Interface Outbound Discards, Input Utilization, Output Utilization, Input Packet Broadcast Percent, Percentage drops in input queue, Percentage drops in output queue
QOS	Percent Drop per QoS Class

Policy Name	Parameters
Traffic Analysis	In Bytes, In Packets, Out Bytes, Out Packets
Traffic Analysis	Total Bytes, Total Packets, In Bytes, In Packets, Out Bytes, Out Packets

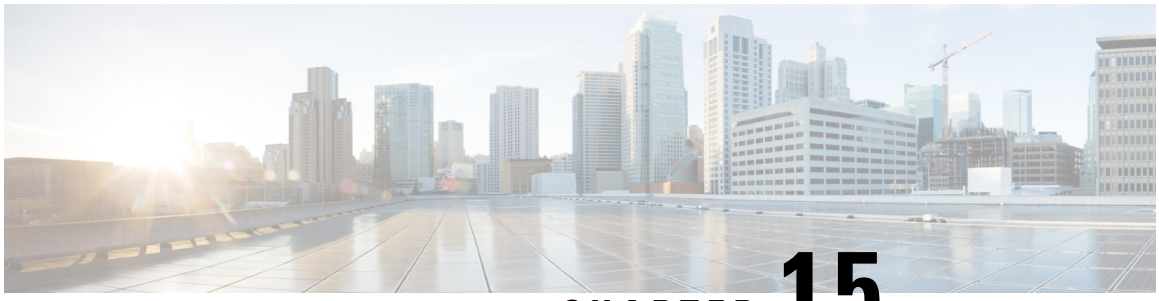
Policy Name	Parameters
Application Response Time	Average Network Time, Average Client Network Time, Average Server Network Time, Average Transaction Time, Average Server Response Time, Maximal Network Time, Maximal Client Network Time, Maximal Server Network Time, Maximal Transaction Time
Voice Video Data	Average MOS, Worst MOS, Jitter, Actual Packet Loss, Adjusted Packet Loss

Monitor Network Performance Using Reports

provides a variety of reports to help you monitor your network's performance. The following are some examples:

- Environmental temperature, CPU and memory utilization
- Interface errors and discards

When you run a performance report, retrieves historical data that has been saved in the database. Reports can only display data that has been configured to collect—in other words, data that is collected and monitored using monitoring policies. (No monitoring policies have to be enabled for event and alarm-related reports; that data is collected automatically.) .



CHAPTER 15

Monitor Alarms and Events

This chapter contains the following topics:

What Are Alarms and Events?

An event is a distinct incident that occurs at a specific point in time, such as a port status change, or a device becoming unreachable. Events can indicate an errors, failures, or exceptional conditions in the network. Events can also indicate the clearing of those errors, failures, or conditions.

An alarm is a response to one or more related events. Only certain events generate alarms. Alarms have a state (cleared or not cleared) and a severity (Critical, Major, Minor, and so forth). An alarm inherits the severity of its most recent event. Alarms remain open until a clearing event is generated (or if the alarm is manually cleared).

Related Topics

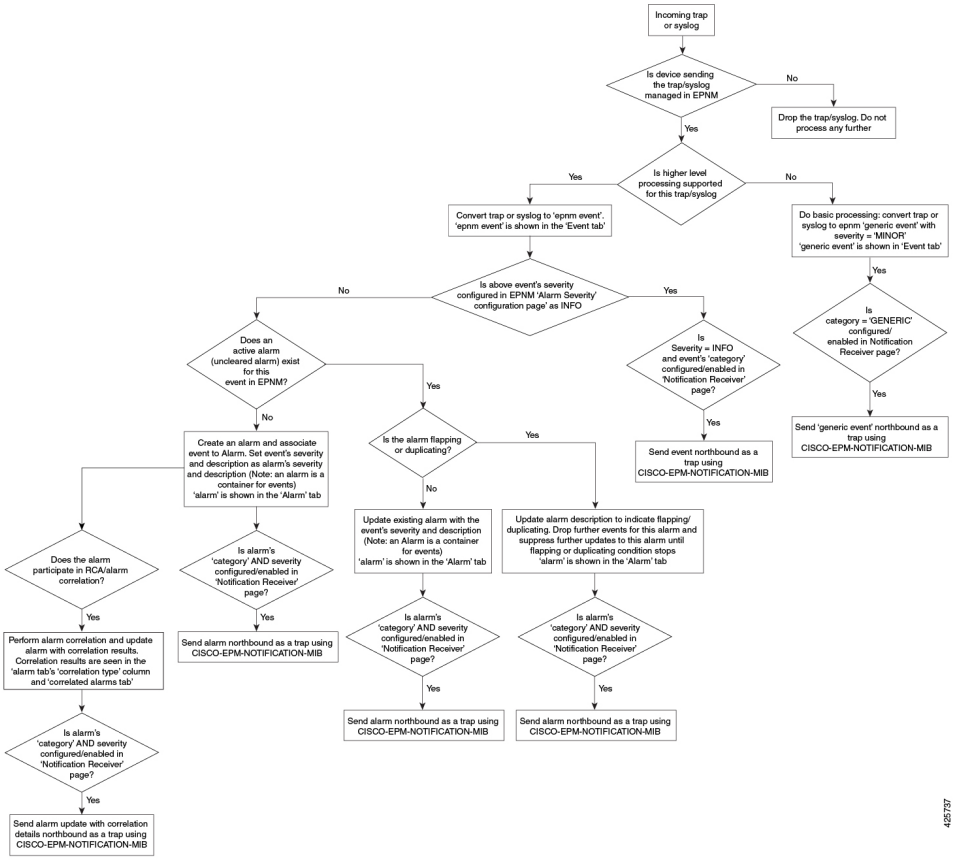
How are Alarms and Events Created and Updated?, on page 264

Acknowledge and Clear Alarms, on page 270
Interpret Event and Alarm Badges and Colors, on page 269

How are Alarms and Events Created and Updated?

The processes SNMP traps, syslogs, and TL1 messages from both IPv4 and IPv6 devices. It maintains an event catalog that determines how it should respond to these events. The flowchart below represents the manner in which these alarms and events are processed:

Figure 7: Alarm processing flowchart



performs the following general steps when it processes an event:

1. Identifies the device and device component that is causing the event (localizes the event).
2. Checks whether the supported event triggers inventory collection.

   Some events have specific rules that instruct what information it should collect.

3. Checks whether the event severity is INFO or CLEARED.
   - If it is INFO or CLEARED, saves the event and displays it in the GUI.
   - If it is any other severity, evaluates whether a new alarm should be opened (next step).

4. Checks whether an alarm already exists or a new alarm should be created.

- If an alarm does exist, associates the event to the existing alarm. The alarm severity is changed to match the severity of the new event, and the alarm time stamp is updated. If it is a clearing event (for example, a link up event), the alarm will be cleared.

Note In some cases, a device may not generate a clearing alarm. The administrator should set the alarm auto-clearing interval.

- If an alarm does not exist, creates a new alarm and assigns it the same severity as the event.

Link Up/Down Flapping

Flapping is a flood of consecutive transitions from link down to link up (or visa versa) for the same interface on a device. It can occur when a fault causes repeated event notifications (for example, a cable with a loosely fitting connector). will mark an alarm as flapping if there are five occurrences of link up/down transitions within 60 seconds. The five occurrences could be of a sequence such as, Interface Down, Interface Up, Interface Down, Interface Up, Interface Down, and so on.

The alarm marked as flapping is either cleared or marked back as a link down when there is no occurrence of any link up/down transition for 60 seconds. The alarm will be updated based on the last non-flapping event received (up or down). This helps control the flow of events and constant updating of the alarm state and the associated notifications (display, emails, northbound traps).

Find and View Alarms

To view alarms, choose Monitor > Monitoring Tools > Alarms and Events. The alarms are classified into four categories and displayed in separate tabs in the Alarms table as given below:

- Network Health—Shows the controller, switches, and router category alarms.
- Rogue AP—Shows the Rogue AP and Adhoc Rogue category alarms.
- Security—Shows the security category alarms.
- System—Shows the system category alarms.

To populate the Rogue AP data in the report, you must set the Rogue AP severity to Minor or Major. If the Rogue AP severity is set to Information, the Rogue AP report won't populate the Rogue AP data.

The count next to each tab name indicates the total number of alarms in that specific alarm category.

Show Active Alarms—You can search for specific alarms and also create and save customized (preset) filters as described in the procedure that follows the table - By default, the Alarms and Events page shows the latest 4000 active alarms excluding the cleared alarms. The active alarms are automatically refreshed based on the settings chosen in My Preferences page. For more details, see Set Up Your Alarm and Event Display Preferences, on page 267. You can temporarily disable the automatic refreshing of alarms by clicking the Pause Auto-Refresh button.

Show Alarm History—Click Show Alarm History in the Alarms and Events page to view up to 20,000 alarms. If you want to view the cleared alarms, see Cleared , on page 271. The alarms are not refreshed automatically in the Show Alarm History mode. But, you can manually refresh the alarms by clicking the Refresh icon in the Alarms and Events table.

The following table describes the alarm viewing options available in the show drop-down filter list.

To find these alarms:	Choose Monitor > Monitoring Tools > Alarms and Events and:
Alarms generated by specific device	For active alarms, click the "I" icon next to the device name to open the Device 360 view, then click the Alarms tab. For cleared alarms, refer to the Alarms and Events table. For certain devices, you can also use the Chassis View to check device alarms.
Alarms assigned to you	Click the Show drop-down filter list and choose Alarms assigned to me. You can also use this filter for cleared and correlated alarms.
Unassigned alarms	Click the Show drop-down filter list and choose Unassigned Alarms. You can also use this filter for cleared and correlated alarms.
Latest alarms according to the timestamp	For active alarms: • Alarms in the last 30 minutes—Click the Show drop-down filter and choose the last 5, 15, or 30 minutes (PI timestamp). • Alarms in the last 24 hours—Click the Show drop-down filter and choose the last 1, 8, or 24 hours (PI timestamp). • Alarms in the last 7 days—Click the Show drop-down filter and choose the last 7 days (PI timestamp).
Latest Alarms according to the device timestamp	Follow the same instructions as in the previous row, but choose the filters with the suffix (Device timestamp)
All alarms generated by a device group, series, or type	Choose a group from the navigation pane on the left. You can also use this filter for cleared and correlated alarms.
Alarms using customized filters	Create and save the advanced filter (see the procedure that follows this table).

Set Alarm and Event Management Preferences

Note Advanced users can also use the Representational State Transfer (REST) API to access device fault information. For information on the API, click ⚙ at the top right of the window and choose .

Set Up Your Alarm and Event Display Preferences

Note The list of 4000 alarms and events also includes cleared alarms which are not displayed. Click Show All to see all the open alarms.

You can customize the following alarm and event display by clicking at the top right of the window and choosing My Preferences. After you make your changes, click Save to apply your new settings. Other settings, such as whether acknowledged, cleared, and assigned alarms are displayed, are controlled globally by the administrator.

User Preference Setting	Description
Automatically refresh Alarms & Events page	Enables or disables automatically refreshing of the Alarms and Events page. If enabled, the page is refreshed according to the setting in Refresh Alarm count in the Alarm Summary.
Refresh Alarm count in the Alarm Summary every ___ minutes/seconds	Sets the refresh interval for the alarm count in the Alarm Summary (1 minute by default) (see Customize the Alarm Summary, on page 268).
Enable Alarm Badging on Alarms & Events page	When user enables Alarm Badging, alarm severity icons are displayed next to the device groups on the Monitor > Monitoring Tools > Alarms & Events page.
Disable Alarm Acknowledge Warning Message	**Note** This setting is only configurable if Hide Acknowledged Alarms is also enabled; that setting is disabled by default (see the previous table). Disables the following message from displaying when user selects an alarm and chooses Change Status > Acknowledge: Warning: This alarm will not be generated, if the original event recurs again, within next 7 days, as it is acknowledged now. Clearing the alarm instead of acknowledging will cause the alarm to be generated if the event recurs again. Proceed with alarm acknowledgment?
Disable confirmation prompt for “Clear all of this condition”	Disables the following message from displaying when user selects an alarm and chooses Change Status > Clear all of this condition: Are you sure you want to clear all alarms of this condition? (Disabled by default)

User Preference Setting	Description
Disable “Set severity to information” prompt for “Clear all of this condition”	Disables the following message which is displayed when user selects an alarm and chooses Change Status > Clear all of this condition: Do you want to set the severity for the selected alarm's condition to Information? WARNING: This is a system-wide change that will prevent creation of future alarms of this condition. You can undo this change on the Severity Configuration page under System Settings. (Disabled by default) **Note** Users with sufficient privileges can reset the severity to its original value.
Select alarm categories for Alarm Summary Toolbar	Controls what is displayed in the Alarm Summary (see Customize the Alarm Summary, on page 268).
When clearing all alarms of a condition, always set the condition's severity to Information	When user selects and alarm and chooses Change Status > Clear all of this condition. (Disabled by default)
Enable New Critical Alarm Count Notifications	Enables the notification pop-up that displays the count of critical alarms.The count gets updated once the alarm interval is refreshed depending on the interval set in Refresh Alarm count in the Alarm Summary (see Customize the Alarm Summary, on page 268). Only the outstanding critical alarms are displayed.

Customize the Alarm Summary

You can specify what alarm categories are displayed:

- In the title bar alarm count (bell). This gives you a quick visual count of alarms you are interested in.
- In the Alarm Summary pop-up window that is launched when you click the alarm count. The pop-up window gives you a quick look at alarm counts with their severity, as shown in the following figure.

To customize this information:

Step 1 Click Edit at the top left of the Alarm Summary pop-up window. This opens your My Preferences page. You can also open this page by clicking ⚙ at the top right of web GUI window and choosing My Preferences.

Step 2 Click the Alarms & Events tab.

Step 3 To change the Alarm Summary refresh interval, select a number from the Refresh Alarms & Events page and Alarm count in the Alarm Summary every drop-down list.

Step 4 To specify what is included in the Alarm Summary, Go to the Alarm Categories area. Select Alarm Summary from the Default category to displaydrop-down list. Enable or disable the required Alarm Category by selecting or deselecting the corresponding checkbox.

Step 5 Click Save to confirm the changes made in the My Preferences window.

Interpret Event and Alarm Badges and Colors

When there is a problem in the network, flags the problem by displaying an alarm or event icon with the element that is experiencing the problem. Alarm Severity Icons, on page 269 lists the icons and their colors.

Alarm Severity Icons

The table below lists the alarm colors and their respective severity levels for the icons displayed in various parts of the web GUI.

Severity Icon	Description	Color
	Critical alarm	Red
	Major alarm	Orange
	Minor alarm	Yellow
	Warning alarm	Light Blue
	Alarm cleared; normal, OK	Green
	Informational alarm	Medium Blue
	Indeterminate alarm	Dark Blue

Get Troubleshooting and Detailed Alarm Information

- View an Alarm's Details, on page 269
- Find Troubleshooting Information for an Active Alarm, on page 270
- Find Out Which Events Are Associated With An Alarm, on page 270

View an Alarm's Details

To get more details about an alarm, expand it. You can do this from the Alarms list (by choosing Monitor > Monitoring Tools > Alarms and Events, or by clicking Details in the Alarm Summary pop-up).

General Information—When alarm was found and last updated, current and last severity, and how it was detected	Device Details—Managed device name, address, uptime, reachability status, collection status, and so forth

Messages—Trap, syslog, or TL1 message	Device Events—Recent device events from past hour (of any type, in chronological order)

Find Troubleshooting Information for an Active Alarm

Use this procedure to get an explanation for why an active alarm occurred, and the recommended response to the alarm.

Note Not all alarms have this information. Users with sufficient privileges can add or change the information that is displayed in the popup window.

Step 1 Choose Monitor > Monitoring Tools > Alarms and Events, then click the Alarms tab. (For interface alarms, you can also get this information from the Interface 360 view under the Alarms tab.)

Step 2 Locate the alarm, then click the "i" icon in the Severity column to open the popup window that provides the explanation and the recommended action that can be taken to troubleshoot the alarm.

If you take any actions, we recommend you document your actions. Choose the alarm, click Annotation.

Find Out Which Events Are Associated With An Alarm

To view the events that have been correlated to an alarm, from the Alarms table, click the “i” icon next to the Severity.

Acknowledge and Clear Alarms

An alarm can have a status of Not Acknowledged, Acknowledged, or Cleared.

Not Acknowledged

Not Acknowledged means the problem is not being worked on. It could indicate that a new fault condition in the network, or that a cleared fault condition that has recurred. Not Acknowledged alarms are not removed from the Alarms and Events tables until they are either acknowledged or cleared.

Acknowledged

Acknowledged means a fault condition has either been recognized and is being worked on, or it can be ignored. Moving an alarm to the acknowledged status is a manual operation and changes the alarm Status to Acknowledged. An acknowledged event is still considered to be open (that is, not cleared), so if any related events recur, the events are added to the alarm.

By default, acknowledged alarms are not removed from the Alarms list. This behavior depends on the Hide Acknowledge Alarms setting that is controlled by the Administrator.

Acknowledged alarms can be moved back to the Not Acknowledged status (for example, if you acknowledged the wrong alarm).

Cleared

Cleared means the fault condition no longer exists. If an alarm is cleared but an associated event recurs, opens a new alarm.

By default, cleared alarms will not be shown in the Alarms and Events page. To view the cleared alarms in the Alarms History table in the Alarms and Events page:

Note When FRU alarms are generated, if inventory lacks location parameters then, generated alarms will not have location parameters. When the FRU alarms are cleared, the alarms may not have inventory location parameters.

- Choose Administration > Settings > System settings, then choose Alarms and Events.
- Under Alarm Display Options, uncheck the Hide cleared Alarms check box.

To change the status of an alarm:

Step 1 Choose Monitor > Monitoring Tools > Alarms & Events.

Step 2 Select an alarm, then choose Change Status and the appropriate status (Acknowledge, Unacknowledge, Clear, Clear all of this Condition).

Note Clear all of this Condition triggers a clearing event for all alarms with the same condition as the alarm you selected. When you choose this status, displays a dialog asking if you want to change the severity for the selected alarm condition to Information. This prevents from issuing alarms for the specified condition. To later reset the condition's severity, choose Administration > System Settings > Severity Configuration and modify the severity.

Step 3 Click Yes to confirm that you want to clear all alarms of the specified condition.

Add Notes To an Alarm

The annotation feature allows you to add free-form text to the alarm, which is displayed in the Messages area of the alarm details. To add text to an alarm, choose the alarm in the Alarms and Events table, click Annotation, and enter your text. As with acknowledging, when you annotate an alarm, adds your user name and the annotation time stamp to the Messages area of the alarm details.

Manage How Alarms are Triggered (Alarm Thresholds)

You can customize how often information is gathered (polling interval), the threshold value that indicates a problem, and whether should generate an informational event or an alarm (of an severity) when a problem is detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies > My Policies and select the policy you want to edit.

Step 2 Locate the parameter you want to change. You can search for the parameter by entering a string in the Parameter text box.

Step 3 To adjust the polling interval, select the new interval from the Polling Frequency drop-down list. To disable polling, choose No Polling. Note that some polling frequencies are applied to groups of parameters. Changing the group interval will change the polling for all settings in the group. If a policy does not have any thresholds or events associated with it, prompts you to save the changes.

Step 4 To change a threshold value, expand the parameter and choose a value from the parameter's drop-down list.

Step 5 To specify what should do when the threshold is surpassed, choose an alarm value from the parameter's drop-down list. You can configure to generate an alarm of a specified severity, generate an informational event, or do nothing (if no reaction is configured).

Step 6 Click:

- Save and Activate to save and activate the policy immediately on the selected devices.
- Save and Close to save the policy and activate it at a later time.

Which Events Are Supported?

View Events

To view alarms, choose Monitor > Monitoring Tools > Alarms and Events, and then click the Events tab.

Show Active Events—By default, the Alarms and Events page shows the latest 4000 active events including the cleared events. The active events are automatically refreshed based on the settings chosen in My Preferences page. For more details, see Set Up Your Alarm and Event Display Preferences, on page 267. You can temporarily disable the automatic refreshing of events by clicking the Pause Auto-Refresh button.

Show Event History—Click Show Event History in the Alarms and Events page to view up to 20,000 events. The events are not refreshed automatically in the Show Event History mode. But, you can manually refresh the events by clicking the Refresh icon in the Alarms and Events table.

The Events tab provides a variety of filters that you can use to find the information you are looking for. You can also create and save customized (preset) filters using the same procedure described in Find and View Alarms, on page 265. The following table lists some of the ways you can filter events.

Click the Take Snapshot tab to view the paged events. You can view up to 20,000 paged events. The tab name gets changed as Snapshot of current date and time. By defalut 50 events will be displayed per page. You can vary thePage Size from 50 to 200.

To find these events:	Select Monitor > Monitoring Tools > Alarms and Events, click the Events tab, and:
All events generated by a device group, series, type, location group, or user-defined group	Choose a group from the left sidebar menu
Events in last x minutes, hours, or days	Click the Show drop-down filter list and choose the appropriate filter
Non-informational events generated in the last hour	From the Show drop-down filter list, choose Non-info events in last hour
Events using customized filters	Create and save an advanced filter (see Find and View Alarms, on page 265)

View Syslog Policies

To view the Syslog policy, do the following:

Step 1 Choose Monitor > Monitoring Tools > Syslog Policies. All the syslog policies are listed in the Syslog Policies page.

Step 2 Click the Expand icon to view the policy details.

Related Topics

Create a New Syslog Policy, on page 273
Edit a Syslog Policy, on page 274
Change Syslog Policy Ranks, on page 275
Change Syslog Policy Ranks

Create a New Syslog Policy

To create a new Syslog policy, do the following:

Step 1 Choose Monitor > Monitoring Tools > Syslog Policies.

Step 2 Click the Add icon. The Create New Syslog Policy window appears.

Step 3 In the Policy Attributes page, enter the unique Name, Description (optional), and choose the desired type of action that the policy will perform.

Step 4 Click Next.

Step 5 You will view the Send Email option or Run Script option based on the policy action chosen in the Policy Attributes window.

- Send Email Option
  - Click Create New Email Recipient and enter the Name and Email Address to create new recipient.
  - Alternatively, select a recipient and notification time range from the drop-down list.
  - Click the Add icon to specify multiple recipients. Send Email will notify one or more recipients by email when matching syslogs are received during corresponding certain times period.
- Run Script Option
  - Click the Upload scripts button to upload a new script from your system. Prime Infrastructure accepts all types of syslog scripts and parameters. Hence, you can upload scripts of any type and provide parameters pertaining to those scripts. The scripts that you upload will be listed in the Script file drop-down list. You can select any one of the uploaded scripts from the drop-down list and create a new syslog policy.

By default Run Script option is disabled. To enable Run Script option, go to Administration > Settings > System Settings > Alarms and Events > Syslog Policies. You must have Syslog Policies Settings access privilege to access the Syslog Policies system settings page.

Step 6 Click Next.

Step 7 In the Device Groups window, choose the Device Groups to which you want to apply the syslog policy. If you do not select any device groups the policy will be applied to all the devices.

Step 8 In the Syslog Fields window, configure the following filters for the syslog fields

- All Messages - The policy will activate for any syslog that meets its other conditions (such as device groups). The content of the syslog message will not affect whether the policy is activated or not.
- Message Types: - The policy will apply only for syslogs that match certain message types such as specific combinations of facility, severity, and mnemonic fields.
- Advanced Filters - To create more complex filters on the facility, severity, and mnemonic fields.
  - Choose a field (facility, severity, or mnemonic).
  - Chose a filter operation. Most filters will also require a value. The “Match” radio buttons above the list of filters determines whether all given conditions must be true, or if at least one must be true.

Step 9 Click Summary to view the details of the syslog policy. If you wish to change the settings, navigate to the respective window and do the necessary changes.

Step 10 Click Finish.

Edit a Syslog Policy

To edit a new Syslog policy, do the following:

Step 1 Choose Monitor > Monitoring Tools > Syslog Policies.

Step 2 Choose the policy and then click the Edit icon. The Edit Syslog policy wizard appears.

Step 3 In the Policy Attributes window, check and modify the Description if required.

Note The policies name and action type cannot be changed after the policy is created.

Step 4 To make desired changes in the Edit Syslog Policy wizard follow the same as the steps in Create a New Syslog Policy Wizard.

Step 5 Click Finish to save the changes or click Cancel to discard.

Delete Syslog Policy

To delete a Syslog Policy, do the following :

Step 1 Choose Monitor > Monitoring Tools > Syslog Policies.

Step 2 Choose the syslog policy which you want to delete and click the Delete icon.

Step 3 Click yes in the Delete Confirmation dialog box to delete, or No to cancel.

Change Syslog Policy Ranks

To change an existing syslog policy rank, do the following :

Step 1 Choose Monitor > Monitoring Tools > Syslog Policies.

Step 2 Choose the syslog policy which you want to change the rank.

Step 3 Click Move Up or Move Down button to increase or decrease the rank of the selected policy. Click Move Up or Move Down button to increase or decrease the rank of the selected policy. Or

Step 4 Click Move To button. You can enter the desired ranks in the drop-down box and click enter to save the changes.

View Syslogs

logs all syslogs from severity 0 through 7 (emergency through debugging messages) generated by all devices that are managed by . Syslogs from devices that are not managed are not logged or displayed. also logs all SNMP messages.

stores a maximum of 2,000,000 syslogs with the following display limits:

- Live syslog streaming—Latest 2,000 syslogs

Step 1 To view syslogs, choose Monitor > Monitoring Tools > Syslog Viewer.

Use the filters to locate different syslogs. You can enter regular expressions in the fields; for example:

```
^Auth, V|violation|$,^Sec*V|violation$
```

Step 2 To view live syslogs, click the Live tab. If the data is excessive, click the Pause icon. You can click the Resume arrow at any time.

Step 3 If you do not want to see duplicates of a syslog, click Deduplicate. will aggregate the syslogs of that type into one line item and display the count in the Count field.

Step 4 To view older syslogs (syslogs that were received before you clicked the Live tab), click the Historic tab. Click the Create Syslog Policy button to create a new syslog policy.

Export Alarms, Events or Syslogs to a CSV or PDF File

Use this procedure to save alarms, events or syslogs as a CSV or PDF file.

Step 1 Navigate to the data you want to export.

Step 2 If you have a very large amount of data, apply a filter; otherwise the export process may take some time.

Step 3 Click  at the top right of the table to open the Export dialog box.

Step 4 Choose CSV or PDF, click OK, and save the file.

Working with Alarms, Events and Syslog Reports

This section describes how to create, schedule and run a alarms, events and syslog reports.

Related Topics

Create a New Alarm Report, on page 276
Create a New Events Report, on page 277
Create a New Syslog Report, on page 278

Create a New Alarm Report

You can create an alarm report by performing the following steps.

Step 1 Navigate to Report > Report Launch Pad > Fault > Alarm Reports.

Step 2 Click the New button. The New Alarm Reports page appears.

Step 3 Select the Create the report in the current virtual domain and each of its sub-domains check box, if you wish to create alarm reports for both the main domain and sub-domains.

Step 4 Enter the title of the report in the Report Title text box.

Step 5 Select an option from the Report By list box.

Step 6 Click the Edit button adjacent to the Report Criteria field to modify the criterion.

Step 7 Select a severity level of the report from the Severity list box. The available options are cleared, critical, information, major, minor, and warning.

Step 8 Select any of the options from the Alarm Category list box.

Step 9 Select a Reporting Period. You can either select an option from the list box or specify the From and To period.

Step 10 Click the Customize button to customize the report.

Step 11 Select the Enable check box to allow scheduling.

Step 12 Select a format in which the report must be exported from the Export Format list box. The available formats are CSV and PDF.

Step 13 Enter the destination to which the report must be delivered. It can either be an email ID or an SFTP server name.

Step 14 Set the date and time by clicking the calendar icon in the Start Date/Time text box. It displays the current date and time, by default.

Step 15 Set a desired Recurrence period.

Step 16 Click the save icon adjacent to the Report Run Result label to launch the Run History page.

Step 17 Click the Run button to generate the report.

Step 18 Click the Save button to save the report.

Step 19 Click the Run and Save button to generate the report and save it for later use.

Step 20 Click the Save and Export button to save the report parameters and export it as a CSV or PDF file.

Step 21 Click the Save and Email button to save the report parameters and send it through email.

Step 22 Click the Cancel button to discard the changes.

Create a New Events Report

You can create an events report by performing the following steps.

Step 1 Navigate to Report > Report Launch Pad > Fault > Events Reports.

Step 2 Click the New button. The New Events Reports page appears.

Step 3 Select the Create the report in the current virtual domain and each of its sub-domains check box, if you wish to create events reports for both the main domain and sub-domains.

Step 4 Enter the title of the report in the Report Title text box.

Step 5 Select an option from the Report By list box.

Step 6 Click the Edit button adjacent to the Report Criteria field to modify the criterion.

Step 7 Select a severity level of the report from the Severity list box. The available options are cleared, critical, information, major, minor, and warning.

Step 8 Select any of the options from the Event Category list box.

Step 9 Select a Reporting Period. You can either select an option from the list box or specify the From and To period.

Step 10 Click the Customize button to customize the report.

Step 11 Select the Enable check box to allow scheduling.

Step 12 Select a format in which the report must be exported from the Export Format list box. The available formats are CSV and PDF.

Step 13 Enter the destination to which the report must be delivered. It can either be an email ID or an SFTP server name.

Step 14 Set the date and time by clicking the calendar icon in the Start Date/Time text box. It displays the current date and time, by default.

Step 15 Set a desired Recurrence period.

Step 16 Click the save icon adjacent to the Report Run Result label to launch the Run History page.

Step 17 Click the Run button to generate the report.

Step 18 Click the Save button to save the report.

Step 19 Click the Run and Save button to generate the report and save it for later use.

Step 20 Click the Save and Export button to save the report parameters and export it as a CSV or PDF file.

Step 21 Click the Save and Email button to save the report parameters and send it through email.

Step 22 Click the Cancel button to discard the changes.

Create a New Syslog Report

You can create a syslog report by performing the following steps.

Step 1 Navigate to Report > Report Launch Pad > Fault > Syslog Reports.

Step 2 Click the New button. The New Syslog Reports page appears.

Step 3 Select the Create the report in the current virtual domain and each of its sub-domains check box, if you wish to create syslog reports for both the main domain and sub-domains.

Step 4 Enter the title of the report in the Report Title text box.

Step 5 Select an option from the Report By list box.

Step 6 Click the Edit button adjacent to the Report Criteria field to modify the criterion.

Step 7 Select a severity level of the report from the Severity list box. The available options are Alert, Critical, Debug, Emergency, Error, Informational, Notice, and Warning.

Step 8 Select a Reporting Period. You can either select an option from the list box or specify the From and To period.

Step 9 Click the Customize button to customize the report.

Step 10 Select the Enable check box to allow scheduling.

Step 11 Select a format in which the report must be exported from the Export Format list box. The available formats are CSV and PDF.

Step 12 Enter the destination to which the report must be delivered. It can either be an email ID or an SFTP server name.

Step 13 Set the date and time by clicking the calendar icon in the Start Date/Time text box. It displays the current date and time, by default.

Step 14 Set a desired Recurrence period.

Step 15 Click the save icon adjacent to the Report Run Result label to launch the Run History page.

Step 16 Click the Run button to generate the report.

Step 17 Click the Save button to save the report.

Step 18 Click the Run and Save button to generate the report and save it for later use.

Step 19 Click the Save and Export button to save the report parameters and export it as a CSV or PDF file.

Step 20 Click the Save and Email button to save the report parameters and send it through email.

Step 21 Click the Cancel button to discard the changes.

Get Support from Cisco

If you receive an alarm in Monitor > Monitoring Tools > Alarms and Events for which you cannot find a resolution in the Cisco Support Community (click an alarm, then choose Troubleshoot > Support Forum.), you can use to open a support request (click an alarm, then choose Troubleshoot > Support Case).

Respond to Problems Within

generates internal SNMP traps to monitor its own functions—such as server CPU and disk utilization, fan and power supply failures, and high availability (HA) state changes.

What is an Alarm Policy?

An Alarm Policy is a filtering method that allows you to control the alarms on network conditions, thereby reducing noise in the system. Choose Monitor > Monitoring Tools > Alarm Policies to view the alarm policies. You can create, edit, delete, and rank the alarm policies. Alarm policy includes one or more conditions, and an action that is applied to any events/alarms that meet all the defined conditions.

The new alarm policies will not be applicable for the alarms already generated by . You must delete or clear the existing alarms for the alarm policy to be effective in .

Note When restarting the Server, all the alarm policies will be suspended. Once the server is up and running, all policies will be enforced.

You can create alarm policies to perform the following actions:

- Suppress alarms—Does not generate alarms for the selected events. But, events will be created and saved normally.
- Suppress events and alarms—Does not create events and alarms.
- Change alarm severities—Overrides the system-wide default severity for the alarms/events that meet the conditions set in the policy.
- Create disassociation threshold alarm—Generates an alarm when a certain percentage of access points across one or more device groups are disassociated from their controllers.
- Configure AP Disassociated alarm suppression—Suppress the alarms with the condition “AP disassociated from controller” either permanently or temporarily.

Related Topics

Create a New Alarm Policy, on page 281
Types of Alarm Policies, on page 280
Edit an Existing Alarm Policy, on page 282
Alarm Policy Ranks, on page 280

Types of Alarm Policies

The table below shows the alarm policy types and the various alarm actions available for each alarm policy type.

Policy Type	Available Action Options
Access Point	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
AP Disassociation	• Create Disassociation Threshold Alarm • Configure Suppression for AP Disassociated Alarm
Controller	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
Interface	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
Layer 2 Switch	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
System	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities
Wired Infrastructure	• Suppress Alarms • Suppress Alarms and Events • Change Alarm Severities

Alarm Policy Ranks

Rank determines the priority or execution order of the alarm policy whenever two or more policies are applied to the same alarm or event. By default, the alarm policies will be ranked in the order they are created.

Points to be remembered while ranking the alarm policies:

1. A lower rank number indicates higher priority
2. A policy with highest rank is applied first, then next highest rank, and so on
3. A high-ranked policy may affect the behavior of a lower-ranked policy or may override the lower-ranked policy entirely.
    - Suppress Alarms will not be applied if a higher-rank alarm suppression policy has already been applied to the event.
    - Suppress Alarms and Events will not be applied if either:
        - A higher-rank suppression policy has already been applied to the event.
        - The event indicates an AP has been disassociated for a sustained period of time.
    - Change Alarm Severities will not be applied if a higher-rank severity change policy has already been applied to the event or alarm.
    - Create Disassociation Threshold Alarm—Does not count AP disassociated alarms that are suppressed by a higher-rank suppression policy. If the AP disassociated alarms are temporarily suppressed, they will be counted once their suppression time expires.
    - Configure AP Disassociated Alarm—Suppression will not be applied if a higher-ranked suppression policy has already been applied to the alarm.

To change the ranking of alarm policies, do the following:

Step 1 Choose Monitor > Monitoring Tools > Alarm Policies.

All the alarm policies are listed in the order they are created.

Step 2 Choose the alarm policy which you want to change the order.

Step 3 Click the Move To icon and enter the ranking number in the Row field or click the Move up icon or Move down icon and change the ranking order.

View Alarm Policies

Step 1 Choose Monitor > Monitoring Tools > Alarm Policies.

All the alarm polices are listed in the Alarm Policies page.

Step 2 Click the Expand icon to view the policy details.

Create a New Alarm Policy

To create a new Alarm Policy, do the following:

Step 1 Choose Monitor > Monitoring Tools > Alarm Policies.

Step 2 Click the Add icon and choose the policy type from the Select A Policy Type window.

The Create a New Alarm Policy wizard appears.

Step 3 In the Policy Attributes page, enter the Name, Description (optional), and choose the type of action you want to perform.

The type of action displayed here is based on the chosen policy in the previous step. See, Types of Alarm Policies in Related Links.

Step 4 For Access Point, Controller, Interface, Layer 2 Switch, unclassified, and Wired Infrastructure policy types, do the following:

a) Choose the Device groups.

If you do not select any device the policy will apply to all devices.

b) (Only for Interface policies) Choose the Port groups.

If you do not select any port the policy will apply to all the port groups.

c) Choose the alarms/events that you want to suppress or the alarms/events that you want to change the severity based on the action chosen in the Policy Attributes page.

d) Click Summary to view the details of the policy. If you wish to change the settings, navigate to the respective page and do the necessary changes.

e) Click Finish.

Step 5 For AP Disassociation policy type, do the following:

Note The AP disassociation alarm policy will be applied only to the leaf nodes.

a) Choose the Device groups.

This is a mandatory step, if you have chosen Create Diassociation Threshold Alarm action in the Policy Attributes page. If you do not select any device for Configure Suppression for AP Disassociated Alarms action, the policy will be applied to all the devices.

b) For Create Diassociation Threshold Alarm action, choose the desired dissociation threshold percentage.

c) For Configure Suppression for AP Disassociated Alarms action, click Suppress Permanently if you want to permanently suppress the alarm or click Display if the condition persists for this duration and select a suppression duration using the slider.

d) Click Summary to view the details of the policy. If you wish to change the settings, navigate to the respective page and do the necessary changes.

e) Click Finish.

Related Topics

Types of Alarm Policies, on page 280
Edit an Existing Alarm Policy, on page 282

Edit an Existing Alarm Policy

To edit the Alarm Policy, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Alarm Policies.

Step 2 Choose the policy and then click the Edit icon.

The Edit Alarm Policy wizard appears.

Step 3 In the Policy Attributes page, check and modify the Description if required.

You cannot edit the policy name and action chosen while creating the policy.

Step 4 The remaining steps in the Edit Alarm Policy wizard are same as the steps in Create a New Alarm Policy wizard. See, Create a New Alarm Policy, on page 281.

Step 5 Click Finish to save the changes or click Cancel to discard.

Related Topics

What is an Alarm Policy?, on page 279
Create a New Alarm Policy, on page 281

Delete Alarm Policy

To delete the alarm policy, do the following;

Step 1 Choose Monitor > Monitoring Tools > Alarm Policies.

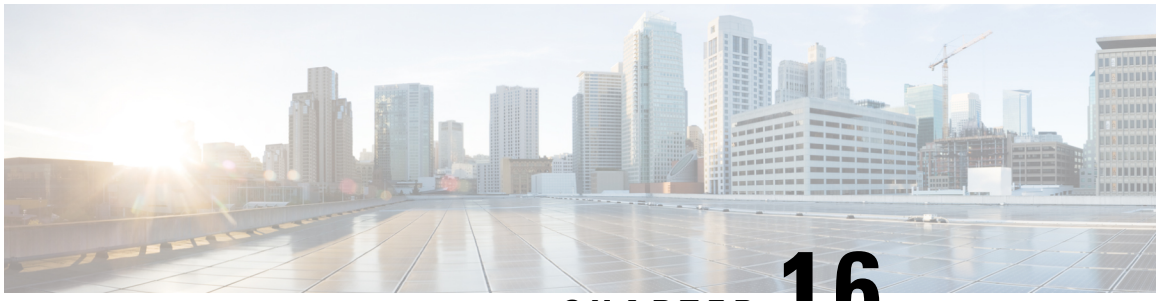
Step 2 Choose the alarm policy which you want to delete and click the Delete icon.

Step 3 Click yes in the Delete Confirmation dialog box to delete, or No to cancel.

Alarms and Events Notification Policies

You can create policies for sending notifications on specific alarms of interest that are generated from particular device groups, to specific recipient groups.

For more information see the section Event Receiving, Forwarding, and Notifications in the chapter Fault Management Administration Tasks in the Cisco Prime Infrastructure Administrator Guide.



CHAPTER 16

Monitor Network Clients and Users

What is a Network Wired/Wireless Client

A client is a device that is connected to an access point or a switch. supports both wired and wireless clients. After you add controllers and switches to , the client discovery process starts. Wireless clients are discovered from managed controllers or autonomous access points. The controllers are polled during regular client status poll. The wireless client count includes autonomous clients as well. In the case of switches, polls for clients immediately after the device is added and updates the device information in the database. For wired clients, the client status polling to discover client associations occurs every two hours (by default). A complete polling happens twice every day to poll complete information of all wired clients connected to all switches.

uses background tasks to perform the data polling operations. There are three tasks associated with clients:

1. Autonomous AP Client Status
2. Lightweight Client Status
3. Wired Client Status

You can refresh the data collection tasks (such as polling interval) from the Administration > Settings > Background Tasks page. See Managing Data Collection and Retention

Client status (applicable only for wired clients) is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the SNMP connection to the wired switch is lost.

For the clients of autonomous access point managed by and for the clients authenticated using Local Extensible Authentication Protocol (LEAP), the username is not registered and is displayed as unknown.

supports both identity and non-identity wired clients. The support for wired clients is based on the identity service. The identity service provides secure network access to users and devices and it also enables the network administrators to provision services and resources to the users based on their job functions.

do not poll end hosts connected through VLAN 1000-1024.

does not support VRF. Therefore, if a client is connected to a VRF-configured device, you cannot view client information.

Note If Prime Infrastructure is unable to retrieve information about wired devices with SNMPv3, apply SNMPv2.

Related Topics

Find Out When Network Clients Connect, on page 299

Monitor Network Users and Clients Using Client Summary Dashboard

You can monitor the network users and clients using the Client Summary Dashboard.

Client Summary Dashboard

The Client dashboard (Dashboard > Overview > Client Summary) page displays the client-related dashlets. These dashlets enable you to monitor the clients on the network. The data for graphs is also polled/updated periodically and stored in database. On the other hand, most of the information in the Client Details page are polled directly from the controller/switch.

When you log into , the Client Summary dashboard displays a few client-related dashlets.

- Client Count By Association/Authentication—Displays the total number of clients by Association and authentication in over the selected period of time.
  - Associated client—All clients connected regardless of whether it is authenticated or not.
  - Authenticated client—All clients connected and passed authentication, authorization and other policies, and ready to use the network.
- Client Distribution—Shows the count of client based on current distribution, such as protocol, EAP type used, and authentication type.

- Client Count By Wireless/Wired—Displays the total number of wired and wireless clients in over the selected period of time.
- Client Traffic—Shows traffic for wired and wireless clients over a period of time.
- Client Posture Status—Shows client count for each postrure status.

Related Topics

Interactive Graphs, on page 869
Add Dashlets to Dashboards

How Do I View Network Clients and Users

Choose Monitor > Monitoring Tools > Clients and Users to view all the wired and wireless clients in your network. In addition, you can view the client association history and statistical information. These tools are useful when users complain of network performance as they move throughout a building with their laptop computers. The information might help you assess what areas experience inconsistent coverage and which areas have the potential to drop coverage.

Access the Client Detail page by clicking on a MAC Address to help you identify, diagnose, and resolve client issues.

Filtering Clients and Users

The Monitor > Monitoring Tools > Clients and Users page lists all associated clients by default. There are preset filters that allow you to view a subset of clients.

The WGB, Wired Guest, and Office Extended Access Point 600 (OEAP 600) are tracked as wireless clients. only remembers sorting column which is indexed including MAC Address, IP Address, Username, AP MAC Address and SSID. Sorting on non-indexed column causes serious performance issue when loading the client list page.You can still sort the table by any column. But after you leave this page, will not remember the last used sorting column if it is not indexed.

In addition, you can use the filter icon  to filter the records that match the filter rules. If you want to specify a filter rule, chooseAll from the Show drop-down list before you click  .

When you select a preset filter and click the filter icon, the filter criteria is dimmed. You can only see the filter criteria but cannot change it. When the All option is selected to view all the entries, clicking the filter icon shows the quick filter options, where you can filter the data using the filterable fields. You can also enter text in the free form text box for table filtering.

You can use the advanced search feature to narrow the client list based on specific categories and filters.

Filtering on IP Addresses

When you perform advanced client filtering on IPv6 addresses, each octet that you specify must be a complete octet. If you specify a partial octet, the filtering might not show correct results.

The following example shows how the advanced client filtering works on IPv6 addresses. This example assumes that you have the following IP addresses in the system: 10.10.40.110.10.40.210.10.40.310.10.240.1Fec0::40:20Fe80::240:20. If you search for all IP addresses containing 40, you get the following result: 10.10.40.110.10.40.210.10.40.3Fec0::40:20. The IP addresses that contain 240 are not filtered because the filtering feature expects you to enter a complete octet.

Viewing Clients and Users

To view complete details in the Monitor > Monitoring Tools > Clients and Users page and to perform operations such as Radio Measurement, users in User Defined groups should have the required permission before they access the Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location pages.

The following attributes are populated only when the ISE is added to :

- ISE
- Endpoint Type
- Posture
- Authorization Profile Name

queries the ISE for client authentication records for the last 24 hours to populate this data. If the client is connected to the network 24 hours before it is discovered in , you might not see the ISE-related data in the table. You might see the data in client details page. To work around this, reconnect the client to the network. The ISE information is shown in the table after the next client background task run.

To view clients and users, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Clients and Users to view both wired and wireless clients information. The Clients and Users page appears.

The Clients and Users table displays a few columns by default. If you want display the additional columns that are available, click  , and then click Columns. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

Note The user name of the client will not be displayed when the client is roaming and if the selected Protocol is "Mobile".

Step 2 Choose a client or user. The following information appears depending on the selected client/user.

- Client Attributes
- Client Statistics
- Client Statistics.
- Client Association History
- Client Event Information
- Client Location Information
- Wired Location History
- Client CCXv5 Information

Related Topics

Search Methods, on page 877
Customize the Controller Client and Users Page , on page 303

Export the List of Network Clients and Users to CSV Files

You can quickly export your clients and users list into a CSV file (spreadsheet format with comma-separated values).

The columns that are shown in the Clients and Users table are only exported to the CSV file.

To export the clients and users list, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Click the export icon on the toolbar. A dialog box appears.
3. In the File Download dialog box, click Save.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Click the export icon on the toolbar. A dialog box appears.

Step 3 In the File Download dialog box, click Save.

Related Topics

How Do I View Network Clients and Users, on page 287
Customize the Controller Client and Users Page , on page 303

Launch the Network Client Troubleshooting Tool

You can launch the Client Troubleshooting tool for any client from the Clients and Users page.

Step 1 Choose Monitor > Monitoring Tools > Clients and Users. The Clients and Users page lists all the clients the system knows (including those not currently associated).

Step 2 Click the MAC Address for the client having connection problems that you want to troubleshoot.

You may find it handy to narrow the client list first, by using the Search feature.

Step 3 Click Troubleshoot and Debug.

Related Topics

How the Client Troubleshooting Tool Gives Advice, on page 291

About the Client Troubleshooting Page

The Client Troubleshooting page provides:

- Details on the current or last session for a selected wired or wireless client.
- The client's current/last connection status, shown as a series of graphic icons.
- If connection problems are detected:
  - The nature of the connection problem (also indicated by graphic icons).
  - Advice on how to troubleshoot that problems.

Note If a client is connected to a switch through Port Channel, interprets the MAC Address of the port channel as VLAN or normal port. Hence the Client Troubleshooting page may not display the correct switch information.

By default the client data is fetched from the Prime Infrastructure database. There is an option to refresh from device by clicking the Refresh from Device link in the upper right corner of the page. It also shows the date and time when the data was last refreshed on the Prime Infrastructure. If the Auto Refresh is turned on, then the Refresh from Devices option is disabled.

By default, the Auto Refresh is enabled. The device automatically refreshes every minute to collect the live data. It also shows when the client was discovered. You can disable this by clicking the Auto Refresh button in the upper right corner of the page.

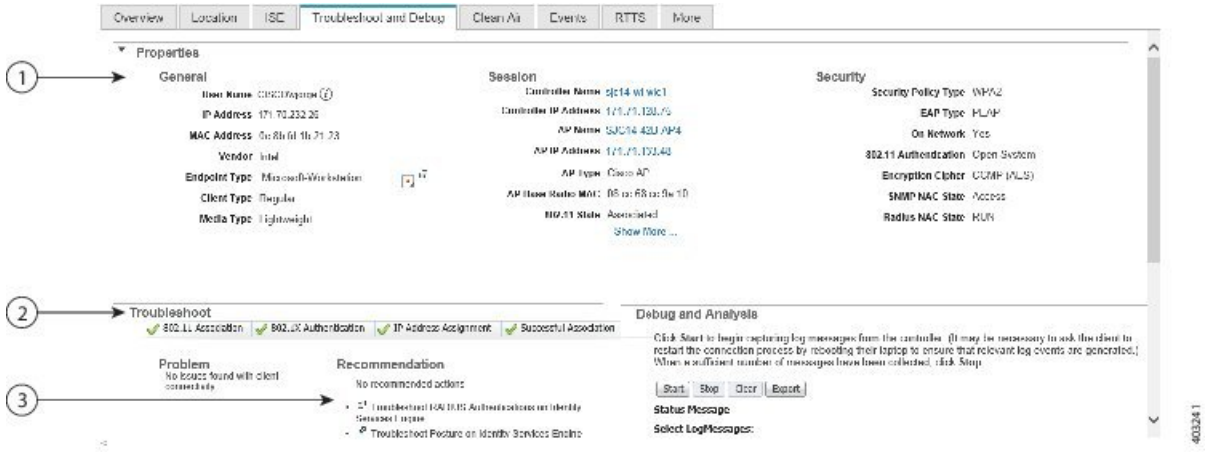
The Client Troubleshooting page provides:

The following figure shows the complete Client Troubleshooting page for a wireless client that has connected successfully. The upper Properties section of the page provides the same session details for a successfully connected client that you would see on the Clients and Users page.

Also note that, as this is a successful connection, the lower Troubleshoot section shows green check marks as the status for each stage of the wireless connection process, and provides no advice on troubleshooting the connection.

Note Troubleshooting is not supported for clients connected to the Wireless Controllers of Cisco Catalyst 9800 Series.

Figure 8: Client Troubleshooting page for Successful Wireless Client



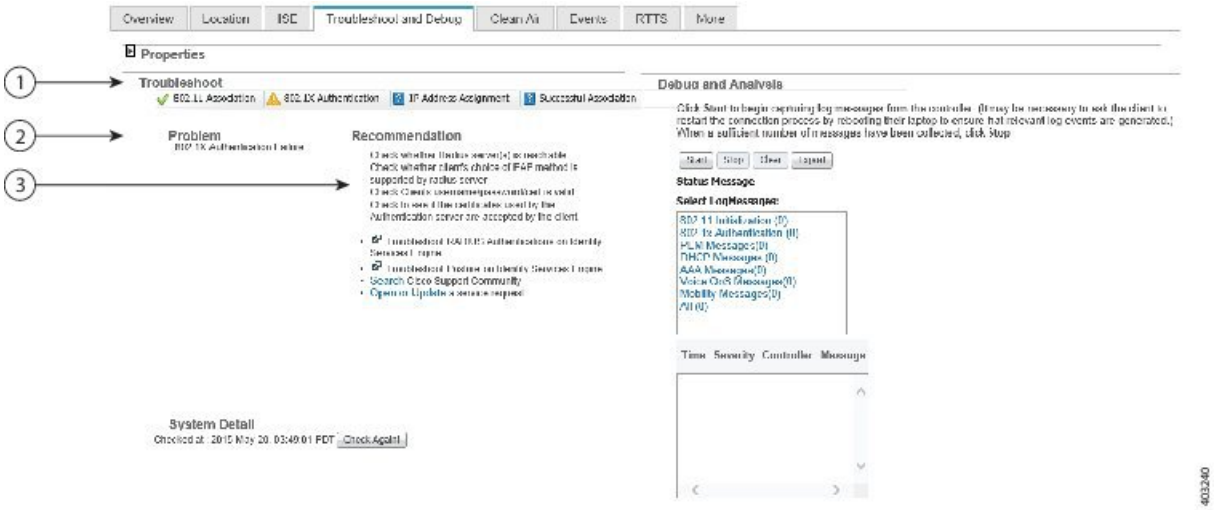
1	Properties
2	Troubleshoot
3	Recommendation

The following figure shows the Troubleshoot section of the Client Troubleshooting page for a different wireless client (for simplicity, we have collapsed the Properties section by clicking on the section's right arrow icon).

This client had trouble connecting. As you can see, there is an alert on the 802.1X Authentication portion of the connection process and a list of steps to try to determine exactly why this was a problem.

This number and type of connection status icons, and advice in the Troubleshoot section, will vary according to the kind of client, the stage of the connection process that had problems, and the likely sources of the problem. For more information, see "How the Client Troubleshooting Tool Gives Advice" in Related Topics.

Figure 9: Client Troubleshooting page for Unsuccessful Wireless Client



1	Troubleshoot
2	Problem
3	Recommendation

Related Topics

Launch the Network Client Troubleshooting Tool, on page 289
How the Client Troubleshooting Tool Gives Advice, on page 291

How the Client Troubleshooting Tool Gives Advice

determines the number of connection areas and the type of troubleshooting advice to present on the Client Troubleshooting page based on the stages the client passes through when establishing connection and connectivity protocols involved at each stage. The following table summarizes these stages and protocols involved at each stage.

Table 37: Client Connection Stages and Protocols

Connection Stage	Link Connectivity	802.1X Authentication	MAC Authentication	Web Authentication	IP Connectivity	Authorization
802.1X	X	X	–	–	X	X

Connection Stage	Link Connectivity	802.1X Authentication	MAC Authentication	Web Authentication	IP Connectivity	Authorization
MAC Authentication	X	–	X	–	X	X
Web Authentication	X	–	–	X	X	X

The following table details the troubleshooting advice presented for each kind of problem detected during the stages of connection building.

Table 38: Troubleshooting Advice for Each Connection Stage and Problem

Client State	Problem	Suggested Action
Link Connectivity	Cannot find the client in the network	• Check whether the client cable is plugged into the network. • Check whether the client is using the proper cable to connect to the network. • Ensure that the port to which the client is connected is not disabled administratively. • Ensure that the port to which the client is connected is not error disabled. • Check whether the speed and duplex are set to Auto on the port to which the client is connected.

	Authentication in progress	• If the client has been in this state for a long time, check the following:
		  • Check whether the supplicant on the client is configured properly as required.
		  • Modify the timers related to the authentication method and try again.
		  • Use the fall back authentication feature if you are not sure which authentication method works with the client.
		  • Try disconnecting and reconnecting.

802.1X Authentication	802.1X Authentication Failure	• Check whether the RADIUS server(s) is reachable from the switch. • Check whether the client choice of EAP is supported by the RADIUS server(s). • Check whether the username/password/certificate of the client is valid. • Ensure that the certificates used by the RADIUS server are accepted by the client.
MAC Authentication	MAC Authentication Failure	• Check whether the RADIUS server(s) is reachable from the switch. • Check whether the MAC address of the client is in the list of known clients on the RADIUS server. • Check whether the MAC address of the client is not in the list of excluded clients.

Client State	Problem	Suggested Action
Web Authentication	Client could not be authenticated through web/guest interface	• Check whether the guest credentials are valid and have not expired. • Check whether the client can be redirected to the login page. • Check whether the RADIUS server is reachable. • Ensure that pop-ups are not blocked. • Check whether the DNS resolution on the client is working. • Ensure that the client is not using any proxy settings. • Check whether the client can access https://<virtual-ip>/login.html • Check whether the browser of the client accepts the self-signed certificate offered by the controller.
IP Connectivity	Client could not complete DHCP interaction	• Check whether the DHCP server is reachable. • Check whether the DHCP server is configured to serve the WLAN. • Check whether the DHCP scope is exhausted. • Check whether multiple DHCP servers are configured with overlapping scopes. • Check whether the local DHCP server is present. If the DHCP bridging mode is enabled (move it to second), the client is configured to get the address from the DHCP server. • Check if the client has the static IP configured and ensure that the client generates IP traffic.
Authorization	Authorization Failure	• Ensure that the VLAN defined for authorization is available on the switch. • Ensure that the default port ACL is configured for ACL authorization.
Successful Connection	None	None. This indicates that all previous stages were completed successfully.

Related Topics

How To Use the Network Client Troubleshooting Tool, on page 293
Launch the Network Client Troubleshooting Tool, on page 289

How To Use the Network Client Troubleshooting Tool

Launch the Client Troubleshooting Tool for the client you want to analyze. See "Launch the Network Client Troubleshooting Tool" in Related Topics. The following table explains the usage of the troubleshooting tabs in the Client Troubleshooting page.

Task	Action
Analyzing client connection logs	• Click the Log Analysis tab to view log messages logged against the client. • Click Start to begin capturing log messages about the client from the controller. • Click Stop to stop log message capture. • Click Clear to clear all log messages. Log messages are captured for ten minutes and then automatically stopped. Click Start to continue. • Click one of the links under Select Log Messages to display log messages (the number between parentheses indicates the number of messages)

Task	Action
Viewing Client Event History and Event Logs	• Click the Events tab to display the event history of a client. • Click the Event Log tab to view the event log. • Click Start to begin capturing log messages from the client. • Click Stop when a sufficient number of messages have been collected. • The Client Troubleshooting Event log and Messaging features are available to CCX Version 6 clients only if the Management Service version is 2 and later.
Checking Client ISE Authentication History and Identity Services	• Click the Identity Services Engine tab to view information about ISE authentication. • Enter the date and time ranges to retrieve historical authentication and authorization information, and then click Submit. The results of the query are displayed in the Authentication Records portion of the page. • Click the Identity Services Engine tab to view information about the identity services parameters. You must configure the Identity Services Engine (ISE) before you access this tab. • If the ISE is not configured, it provides a link to add an ISE to . The ISE provides authentication records to via REST API. The network administrator can choose a time period for retrieving authentication records from the ISE.
Checking Client Clean Air Environment	• Click the CleanAir tab to view information about the air quality parameters and active interferer for the CleanAir-enabled access point. • Click CleanAir Details to know more about the air quality index.

Task	Action
Running Diagnostic Tests on Problem Clients	• Click the Test Analysis tab if Cisco-compatible Extension Version 5 or Version 6 clients are available. • Check the check box for the applicable diagnostic test, enter any appropriate input information, and click Start. The Test Analysis tab allows you to run a variety of diagnostic tests on the client. The following diagnostic tests are available on the Test Analysis tab: • DHCP—Executes a complete DHCP Discover/Offer/Request/ACK exchange to determine that the DHCP is operating properly between the controller and client. • IP Connectivity—Causes the client to execute a ping test of the default gateway obtained in the DHCP test to verify that IP connectivity exists on the local subnet. • DNS Ping—Causes the client to execute a ping test of the DNS server obtained in the DHCP test to verify that IP connectivity exists to the DNS server. • DNS Resolution—Causes the DNS client to attempt to resolve a network name known to be resolvable to verify that name resolution is functioning correctly. • 802.11 Association—Directs an association to be completed with a specific access point to verify that the client is able to associate properly with a designated WLAN. • 802.1X Authentication—Directs an association and 802.1X authentication to be completed with a specific access point to verify that the client is able to properly complete an 802.1x authentication. • Profile Redirect—At any time, the diagnostic system might direct the client to activate one of the configured WLAN profiles and to continue operation under that profile. • To run the profile diagnostic test, the client must be on the diagnostic channel. This test uses the profile number as the input. To indicate a wildcard redirect, enter 0. With this redirect, the client is asked to disassociate from the diagnostic channel and associate with any profile. You can also enter a valid profile ID. Because the client is on the diagnostic channel when the test is run, only one profile is returned in the profile list. You should use this profile ID in the profile redirect test (when wildcard redirecting is not desired).
Pinging Problem Clients with Text Messages	For Cisco-compatible Extension Version 5 or Version 6 clients, a Messaging tab will appear which can be used to send an instant text message to the user of this client. From the Message Category drop-down list, choose a message, and click Send.

Task	Action
Viewing Real Time Troubleshooting (RTTS) Details	Click the RTTS tab to view the Real Time Troubleshooting (RTTS) details. Select modules to debug and debug level. Click Run. The RTTS manager executes a set of commands in the controllers connected to the client based on the selected debug modules and debug level and displays the RTTS details. Click the Filter tab to filter the RTTS details based on debug time, controller name, controller IP, severity, and debug message. Click the Export tab to export the debug details as a csv file. You can also debug other controllers based on the selected debug modules and debug levels by using the Choose different controllers option. The RTTS Manager supports five concurrent RTTS debug sessions and each debug session is limited to five devices.

Task	Action
Viewing Voice Metrics for a Client	To view traffic stream metrics for this client, follow these steps: • Choose Monitor > Monitoring Tools > Clients and Users. • Select a client. • From the More drop-down list, choose Voice Metrics. • Click Go. The following information appears: • Time—Time that the statistics were gathered from the access point(s). • QoS • AP Ethernet MAC Radio • QoS • AP Ethernet MAC • Radio • Time—Time that the statistics were gathered from the access point(s). • QoS • AP Ethernet MA • QoS • Radio • AP Ethernet MAC • Radio • % PLR (Downlink)—Percentage of packets lost on the downlink (access point to client) during the 90 second interval. • % PLR (Uplink)—Percentage of packets lost on the uplink (client to access point) during the 90 second interval. • Avg Queuing Delay (ms) (Uplink)—Average queuing delay in milliseconds for the uplink. Average packet queuing delay is the average delay of voice packets traversing the voice queue. Packet queue delay is measured beginning when a packet is queued for transmission and ending when the packet is successfully transmitted. It includes time for re-tries, if needed. • % Packets > 40 ms Queuing Delay (Downlink)—Percentage of queuing delay packets greater than 40 ms. • % Packets 20ms—40ms Queuing Delay (Downlink)—Percentage of queuing delay packets greater than 20 ms. • Roaming Delay—Roaming delay in milliseconds. Roaming delay, which is measured by clients, is measured beginning when the last packet is received from the old access point and ending when the first packet is received from the new access point after a successful roam.

Related Topics

Launch the Network Client Troubleshooting Tool, on page 289
Debug Commands for RTTS, on page 298

Debug Commands for RTTS

The following table contains the list of debug commands for Legacy controllers and Converged Access Controllers 5760/3850/3650 Wireless LAN Controllers (WLCs).

Table 39: List of Debug Commands for Legacy Controllers and NGWC Controllers

Controller	Modules to Debug	Debug Level	Commands
Legacy	All		debug capwap info enable debug dot1x all enable debug mobility directory enable
	Dot1.x	Detail	debug dot1x all enable
		Error	debug dot1x events enable
		High Level	debug dot1x states enable
Legacy	Mobility	Detail	debug mobility packet enable debug mobility keepalive enable
		Error	debug mobility directory enable debug mobility config enable
		High Level	debug mobility handoff enable
	Wireless Client Join	Detail	debug client <macAddress> debug aaa all enable debug dot1x all enable
		Error	debug client <macAddress>
		High Level	debug client <macAddress>
NGWC	All		debug capwap ap error debug dot1x events debug capwap ios detail

Controller	Modules to Debug	Debug Level	Commands
Dot1.x	Detail	debug wcm-dot1x detail debug wcm-dot1x all debug dot1x all	
	Error	debug wcm-dot1x errors debug dot1x errors	
	High Level	debug wcm-dot1x trace debug wcm-dot1x event debug wcm-dot1x error debug client mac-address <macAddress>	
Mobility	Detail	debug mobility all	
	Error	debug mobility error	
	High Level	debug mobility handoff	
Wireless Client Join	Detail	debug wcdb error debug wcdb event debug wcdb db debug ip dhcp snooping events debug ip dhcp server events debug client mac <macAddress>	
	Error	debug client mac <macAddress>	
	High Level	debug client mac <macAddress>	

Related Topics

Launch the Network Client Troubleshooting Tool, on page 289

Find Out When Network Clients Connect

This feature enables you to track clients and be notified when they connect to a network.

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.
3. Click Add to track a single client, and then enter the following parameters:
4. If you have a long list of clients, click Import to track multiple clients. This allows you to import a client list from a CSV file. Enter the MAC address and username.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.

This table supports a maximum of 2000 rows. To add or import new rows, you must first remove some older entries.

Step 3 Click Add to track a single client, and then enter the following parameters:

- Client MAC address
- Expiration—Choose Never or enter a date.

Step 4 If you have a long list of clients, click Import to track multiple clients. This allows you to import a client list from a CSV file. Enter the MAC address and username.

A sample CSV file can be downloaded that provides data format:

Example:

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format, Note
00:40:96:b6:02:cc, 10/07/2010, Sample Test Client
00:02:8a:a2:2e:60, Never, NA
```

A maximum of 2000 clients can be tracked. If you have reached the limit, you will have to remove some clients from the list before you can add more.

Related Topics

Set Up Notifications About Clients Connecting to the Network, on page 300
Launch the Network Client Troubleshooting Tool, on page 289

Set Up Notifications About Clients Connecting to the Network

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.
3. Select the tracked client(s) for which you want to specify notification settings.
4. Select a notification settings option from the following:
5. Enter the email address.
6. Click Save.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Click Track Clients. The Track Clients dialog box appears listing the currently tracked clients.

Step 3 Select the tracked client(s) for which you want to specify notification settings.

Step 4 Select a notification settings option from the following:

- Purged Expired Entries—You can set the duration to keep tracked clients in database. Clients can be purged as follows:
  - after 1 week
  - after 2 weeks
  - after 1 month
  - after 2 months
  - after 6 months
  - kept indefinitely
- Notification Frequency—You can specify when s ends a notification of a tracked client:
  - on first detection
  - on every detection
- Notification Method—You can specify that the tracked client event generates an alarm or sends an email message.

Step 5 Enter the email address.

Step 6 Click Save.

Related Topics

Find Out When Network Clients Connect, on page 299
Identify Unknown Network Users, on page 301

Identify Unknown Network Users

Not all users or devices are authenticated via 802.1x (for example, printers). In such a case, a network administer can assign a username to a device.

If a client device is authenticated to the network through web auth, might not have username information for the client (applicable only for wired clients).

Clients are marked as Unknown when the NMSP connection to the wired switch is lost. A client status (applicable only for wired client) is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost.

To add users to the list of Unknown users manually, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Click Identify Unknown Users.
3. Click Add to add a user.
4. Enter the MAC address and username and click Add.
5. Repeat Step 3 to Step 4 to enter a MAC Address and its corresponding username for each client.
6. Click Save.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Click Identify Unknown Users.

Step 3 Click Add to add a user.

Step 4 Enter the MAC address and username and click Add.

Once a username and MAC address have been added, uses this data for client lookup by matching the MAC address.

Step 5 Repeat Step 3 to Step 4 to enter a MAC Address and its corresponding username for each client.

Step 6 Click Save.

Note
- The username is updated only when the next association of the client occurs.
- This table supports a maximum of 10,000 rows. To add or import new rows, you must first remove some older entries.

Import List Of Unknown Network Users

To import a list of Unknown users, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Click Identify Unknown Users.
3. Click Choose File to open the file import wizard.
4. Navigate to the required .csv file and click Choose.
5. Click Import to import the list.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Choose Monitor > Monitoring Tools > Clients and Users.	
Step 2	Click Identify Unknown Users.	
Step 3	Click Choose File to open the file import wizard.	
Step 4	Navigate to the required .csv file and click Choose.	You can dowload a sample csv file for the data format: Example: # MacAddress, Username 00:11:22:33:44:55, username
Step 5	Click Import to import the list.	

Export List Of Unknown Network Users

To export a list of Unknown users, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Click Identify Unknown Users and then click Export.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Choose Monitor > Monitoring Tools > Clients and Users.	
Step 2	Click Identify Unknown Users and then click Export.	This exports a .csv file to your system.

Related Topics

Customize the Controller Client and Users Page , on page 303
Find Out When Network Clients Connect, on page 299

Customize the Controller Client and Users Page

You can add, remove, or reorder columns in the Clients table.

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Click the settings icon, then click Columns.
3. Select the columns to show.
4. Click Reset to restore the default view.
5. Click Close to confirm the changes.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Click the settings icon, then click Columns.

Step 3 Select the columns to show.

Step 4 Click Reset to restore the default view.

Step 5 Click Close to confirm the changes.

Related Topics

Find Out When Network Clients Connect, on page 299
Set Up Automatic Controller Client Troubleshooting on a Diagnostic Channel, on page 304

Set Up Automatic Controller Client Troubleshooting on a Diagnostic Channel

In the Settings > Client page, you can enable automatic client troubleshooting on a diagnostic channel. This feature is available only for Cisco-compatible Extension clients Version 5.

To enable automatic client troubleshooting, follow these steps:

Step 1 Choose Administration > Settings > System Settings.

Step 2 From the left sidebar menu, choose Client.

Step 3 Check the Automatically troubleshoot client on diagnostic channel check box.

When the check box is selected, processes the diagnostic association trap. When it is not selected, raises the trap, but automated troubleshooting is not initiated.

Step 4 Click Save.

Related Topics

Obtain Radio Measurements for Wireless Network Clients, on page 304
Customize the Controller Client and Users Page , on page 303

Obtain Radio Measurements for Wireless Network Clients

In the client page, you can obtain radio measurements only if the client is Cisco-compatible Extensions v2 (or higher) and in the associated state (with a valid IP address). If the client is busy when asked to do the measurement, it determines whether to honor the measurement or not. If it declines to make the measurement, it shows no data from the client.

This feature is available to CCX Version 6 clients only if the Foundation service version is 1 or later.

To receive radio measurements, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Click the circle next to a client.

You can also perform a search for a specific client using Search feature.

Step 3 From the Test drop-down list, choose Radio Measurement.

The Radio Measurement option only appears if the client is Cisco-compatible Extensions v2 (or higher) and is in the associated state (with a valid IP address).

Step 4 Check the check box to indicate if you want to specify beacon measurement, frame measurement, channel load, or noise histogram.

Click Initiate. The different measurements produce differing results. See “View Results of Network Client Radio Measurements” in Related Topics.

The measurements take about 5 milliseconds to perform. A message from indicates the progress. If the client chooses not to perform the measurement, that is communicated.

Related Topics

View Results of Network Client Radio Measurements, on page 305

View Results of Network Client Radio Measurements

Depending on the measurement type requested, the following information might appear:

- Beacon Response
- Frame Measurement
- Channel Load
- Noise Histogram

For more details on the measurement parameters, see the Field Reference for Monitor pages.

Related Topics

Obtain Radio Measurements for Wireless Network Clients, on page 304

Run a Test to Display Network Client V5 Statistics

To access the Statistics request page, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Select a client.
3. From the Test drop-down list, choose CCX statistics.
4. Click Go.
5. Select the desired type of stats (Dot11 Measurement or Security Measurement).
6. Click Initiate to initiate the measurements.
7. Depending on the V5 Statistics request type, the following counters are displayed in the results page:

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Select a client.

Step 3 From the Test drop-down list, choose CCX statistics.

This menu is shown only for CCX v5 and later clients.

Step 4 Click Go.

Step 5 Select the desired type of stats (Dot11 Measurement or Security Measurement).

Step 6 Click Initiate to initiate the measurements.

The duration of measurement is five seconds.

Step 7 Depending on the V5 Statistics request type, the following counters are displayed in the results page:

- Dot11 Measurement
  - Transmitted Fragment Count
  - Multicast Transmitted Frame Count
  - Failed Count
  - Retry Count
  - Multiple Retry Count
  - Frame Duplicate Count
  - Rts Success Count
  - Rts Failure Count
  - Ack Failure Count
  - Received Fragment Count
  - Multicast Received Frame Count
  - FCS Error Count—This counter increments when an FCS error is detected in a received MPDU.
  - Transmitted Frame Count
- Security
  - Pairwise Cipher
  - Tkip ICV Errors
  - Tkip Local Mic Failures
  - Tkip Replays
  - Ccmp Replays
  - Ccmp Decryp Errors
  - Mgmt Stats Tkip ICV Errors
  - Mgmt Stats Tkip Local Mic Failures
  - Mgmt Stats Tkip Replays
  - Mgmt Stats Ccmp Replays
  - Mgmt Stats Ccmp Decrypt Errors
  - Mgmt Stats Tkip MHDR Errors
  - Mgmt Stats Ccmp MHDR Errors
  - Mgmt Stats Broadcast Disassociate Count
  - Mgmt Stats Broadcast Deauthenticate Count
  - Mgmt Stats Broadcast Action Frame Count

Related Topics

Run a Test to Display Network Client Operational Parameters, on page 306

Run a Test to Display Network Client Operational Parameters

To view specific client operational parameters, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.

2. Select a client.
3. From the Test drop-down list, choose Operational Parameters.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Select a client.

Step 3 From the Test drop-down list, choose Operational Parameters.

The following information is displayed:

Operational Parameters:

- Device Name—User-defined name for device.
- Client Type—Client type can be any of the following:
  - laptop(0)
  - pc(1)
  - pda(2)
  - dot11mobilephone(3)
  - dualmodephone(4)
  - wgb(5)
  - scanner(6)
  - tabletpc(7)
  - printer(8)
  - projector(9)
  - videoconfsystem(10)
  - camera(11)
  - gamingsystem(12)
  - dot11deskphone(13)
  - cashregister(14)
  - radiotag(15)
  - rfidsensor(16)
  - server(17)
- SSID—SSID being used by the client.
- IP Address Mode—The IP address mode such as static configuration or DHCP.
- IPv4 Address—IPv4 address assigned to the client.
- IPv4 Subnet Address—IPv4 subnet address assigned to the client.
- IPv6 Address—IPv6 address assigned to the client.
- IPv6 Subnet Address—IPv6 address assigned to the client.
- Default Gateway—The default gateway chosen for the client.
- Operating System—Identifies the operating system that is using the wireless network adapter.
- Operating System Version—Identifies the version of the operating system that is using the wireless network adapter.
- WNA Firmware Version—Version of the firmware currently installed on the client.
- Driver Version
- Enterprise Phone Number—Enterprise phone number for the client.
- Cell Phone Number—Cell phone number for the client.

- Power Save Mode—Displays any of the following power save modes: awake, normal, or maxPower.
- System Name
- Localization

Radio Information:

- Radio Type—The following radio types are available:
  - unused(0)
  - fhss(1)
  - dsss(2)
  - irbaseband(3)
  - ofdm(4)
  - hrdss(5)
  - erp(6)
- Radio Channel—Radio channel in use.

DNS/WNS Information:

- DNS Servers—IP address for DNS server.
- WNS Servers—IP address for WNS server.

Security Information:

- Credential Type—Indicates how the credentials are configured for the client.
- Authentication Method—Method of authentication used by the client.
- EAP Method—Method of Extensible Authentication Protocol (EAP) used by the client.
- Encryption Method—Encryption method used by the client.
- Key Management Method—Key management method used by the client.

Related Topics

Run a Test to Display Network Client V5 Statistics, on page 305
View Network Client Details, on page 308

View Network Client Details

To view specific client profile information, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Select a client.
3. From the More drop-down list, choose Profiles.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Select a client.

Step 3 From the More drop-down list, choose Profiles.

The following information is displayed:

- Profile Name—List of profile names as hyperlinks. Click a hyperlink to display the profile details.
- SSID—SSID of the WLAN to which the client is associated.

Related Topics

Disable Network Clients, on page 309

Disable Network Clients

To disable a current client, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Select a client.
3. Click Disable. The Disable Client page appears.
4. Enter a description in the Description text box.
5. Click OK.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Select a client.

Step 3 Click Disable. The Disable Client page appears.

Step 4 Enter a description in the Description text box.

Step 5 Click OK.

Once a client is disabled, it cannot join any network/ssid on controller(s). To enable the client again, choose Configuration > Network > Network Devices > Wireless Controller > Device Name > Security > Manually Disabled Clients, and remove the client entry.

Related Topics

View Network Client Details, on page 308
Remove Network Clients From Prime Infrastructure, on page 309

Remove Network Clients From Prime Infrastructure

To remove a current client, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Select a client.
3. Choose Remove.
4. Click Remove to confirm the deletion.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Select a client.

Step 3 Choose Remove.

Step 4 Click Remove to confirm the deletion.

Locate Network Clients on a Wireless Map

To display a high-resolution map of the client location, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Choose a client from the Client Username column.
3. From the More drop-down list:
4. Click Go.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Choose a client from the Client Username column.

Step 3 From the More drop-down list:

- Choose Recent Map,to view the recent location of the client.
- Choose Present Map, to view a high-resolution map of the client current location.
- Choose Client Sessions Report, to view the most recent client session report results for a client.

Note Prime Infrastructure 3.3 onwards, recent and current client locations are not displayed in Site Maps.

Step 4 Click Go.

Related Topics

View Network Client Roaming Using Reports, on page 311

View Network Client Roaming Using Reports

To view the most recent roam report for this client, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Select a client.
3. From the More drop-down list, choose Roam Reason.
4. Click Go.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Select a client.

Step 3 From the More drop-down list, choose Roam Reason.

Step 4 Click Go.

This page displays the most recent roam report for the client. Each roam report has the following information:

- New AP MAC address
- Old (previous) AP MAC address
- Previous AP SSID
- Previous AP channel
- Transition time—Time that it took the client to associate to a new access point.
- Roam reason—Reason for the client roam.

Related Topics

Identify Access Points That Can Hear a Network Client, on page 311

Identify Access Points That Can Hear a Network Client

To display details of access points that can hear the client including the signal strength/SNR, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Select a client.
3. From the More drop-down list, choose Detecting APs.
4. Click Go.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Select a client.
Step 3 From the More drop-down list, choose Detecting APs.
Step 4 Click Go.

Related Topics

View the Location History for a Network Client, on page 312

View the Location History for a Network Client

To display the history of the client location based on RF fingerprinting, follow these steps:

SUMMARY STEPS

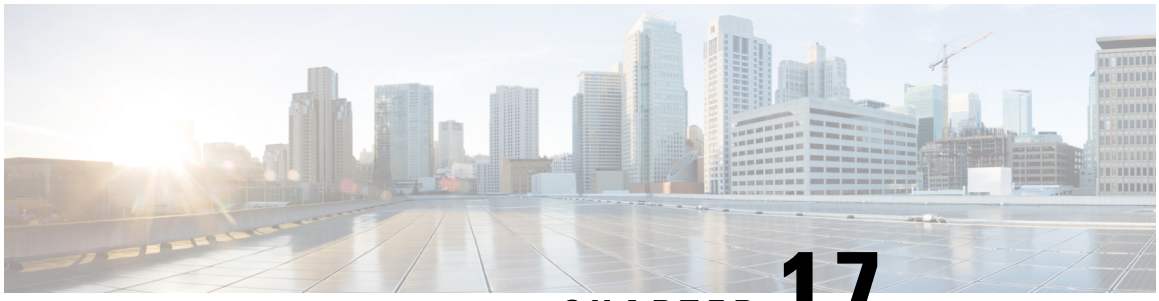
1. Choose Monitor > Monitoring Tools > Clients and Users.
2. Select a client.
3. From the More drop-down list, choose Location History.
4. Click Go.

DETAILED STEPS

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.
Step 2 Select a client.
Step 3 From the More drop-down list, choose Location History.
Step 4 Click Go.

Related Topics

How To Use the Network Client Troubleshooting Tool, on page 293



CHAPTER 17

Monitor Network Performance Using PfRv3 Monitoring

What is PfRv3?

Performance Routing Version 3 (PfRv3) represents the third generation of enhancement to the intelligent path control capabilities offered by Cisco. PfR monitors network performance and selects the best path for each application based upon advanced criteria such as reachability, delay, jitter and packet loss. PfR can evenly distribute traffic to maintain equivalent link utilization levels using an advanced load balancing technique.

PfRv3 is an intelligent path control of the IWAN initiative and provides a business-class WAN over Internet transports. PfR allows customers to protect critical applications from fluctuating WAN performance while intelligently load balancing traffic over all WAN paths.

PfR comprises two major Cisco IOS components:

- Primary Controller—The primary controller is a policy decision point at which policies are defined and applied to various traffic classes that traverse the border router systems. The primary controller can be configured to learn and control traffic classes on the network.
- Border Routers (BR)—The border routers are in the data forwarding path. The border router collects data from the Performance Monitor cache and from the smart probe results. The border router influences the packet forwarding path as directed by the primary controller to manage user traffic.

Related Topics

Use the PfR Monitoring Page, on page 314

View Details About Site to Site Events Using PfRv3, on page 317

Compare WAN Interfaces Usage Using PfRv3, on page 319

Get Access to PfR Monitoring for a User Group

PfR monitoring is enabled for the Prime Infrastructure root user group by default.

To access the PfR monitoring landing page by other user groups, do the following:

Step 1 Choose Administration > User, Roles & AAA > User.

Step 2 Click Users in the left pane, and choose Select a command > Add User, then click Go.

Step 3 Enter the username and password, and then confirm the password, for the new user.

Step 4 Assign user group to the new user by selecting the check box next to each user group which has PfR Monitoring Access entry in its task list.

Step 5 Click Save.

Step 6 Log in to Prime Infrastructure using the new Username and Password.

Step 7 Choose Services > Application Visibility & Control > PfR Monitoring.

Step 8 If you do not see PfR Monitoring, go to Administration > User, Roles & AAA > User Groups.

Step 9 Click Task List corresponding to the assigned user group and check whether PfR Monitoring is available.

Step 10 If PfR Monitoring is not available in the task list, click the Task Permissions tab and check the PfR Monitoring Access check box under the Network Monitoring list.

Step 11 Click Submit.

Use the PfR Monitoring Page

You can launch the PfR monitoring page by choosing Services > Application Visibility & Control > PfR Monitoring. The PfR monitoring page has PfR Eventstab including Site to Site PfR Events table, a filter panel, Metrics panel (Service Provider view and Differentiated Services Code Point (DSCP) View charts), time slider, and Compare WAN Links tab and SP Health Trend tab.

Site to Site PfR Events Table

The Site to Site PfR events table displays sites (Hub, Branch and Transit sites) and the following events:

- Threshold Crossing Alert (TCA) and Route change (RC) events—Represent the degraded network performance that are identified and corrected by PfR, and are indicated by blue dots.
- Immitigable event (IME)— Represents the metric violations that could not be corrected by the PfR, and are indicated as red dots.

Note The PfR events that occurred over last 72 hours are displayed, by default.

The site combinations are sorted in the following ways:

- The site combination with maximum number of IMEs, is present at top row of the table.

- If two site combinations have equal number of IMEs, then the one with maximum number of events (including IME, TCA, and RC) is placed on the top of the table and indicated in red color.

PfR Filter Panel

The PfR Filter Panel allows you to filter the events based on various filters. The Metrics panel and the Site to Site PfR Events table display the details based on the selected filter options. You can view the selected filter options in the top of the filter panel. See the Cisco Prime Infrastructure Reference Guide for the descriptions of the filter options.

SP Health Trend Tab

The SP Health Trend tab displays the dashlets such as SP Carrying Uncorrected traffic, SP Unreachability Trend and SP Overall Health trend, plotted against time.You can toggle between chart view and table view.

You can export the dashlets in pdf or CSV format by clicking export icon. Click Summary in the dashlet to view the overall average of impaired traffic, link downtime or link health for all the Service Providers, in table format.

We recommend that you do not select a time range beyond 60 days, when you are filtering the dashlets using the time filter, because it will slow down the performance of the SP Heath Trend tab. Additionally, you can filter the data based on service providers by selecting a desired service provider in the Service Provider Filter field and then clicking the Submit button.

You can perform the following tasks in the PfR monitoring page:

Table 40: PfR Monitoring Page Tasks

Tasks	Description
Refresh the page	Click the Refresh icon at the top right corner of the PfR monitoring page, to manually refresh the PfR landing page.
Changing Settings	Click the settings icon at the top right corner of the PfR monitoring page. The PfR Settings pop-up window will appear. Select your preferences for the following: • Global —Choose the VRF and other common settings. Hover your mouse over info icon to see tool tip about each option. • SP Health Trend Tab—Choose your preference for the number of charts to be displayed per row in the SP Health Trend tab. • PfR Events Tab—Choose your preference for Auto Refresh, Events Table, Live Topolgy popup, Service Provider chart and DSCP chart. • Site to Site Tab—Choose required value for Top N settings for Charts. • Compare WAN Links Tab—Choose required value for Top N settings for Charts. • FAQ Section—Provides you detailed information on troubleshooting. Click Save and Close to save your settings.

Tasks	Description
View in-line help	Click the info icon at the top right corner of the PfR monitoring page, to view the in-line help for the respective page.
View live topology	Click the topology icon next to any site pair to view the live topology popup that shows traffic corresponding to different DSCPs. Click Site to Site details to go to site to site tab, for more information see View Details About Site to Site Events Using PfRv3, on page 317. Choose the VRF for which you want to see the topology, from the VRF drop-down list. The VRFs listed corresponds to the site pair you have chosen. Click on required time option to view the live topology plotted for that time. • Select Auto refresh check-box to refresh the topology for every 5 minutes. • You can also choose Custom time. Make sure to select the time range such that time different is not less than 5 minutes. Auto refresh will be disabled for this option. • Click Live to view the topology corresponding to the last one minute. When you select the Live option, the Site to Site details button will be disabled and the topology will be refreshed automatically every 30 seconds when Auto Refresh is selected.
View border router or link metrics	Click a link, primary controller icon or border router icon in the Live topology to view a list of options. Click on each option to view the respective details. See View Details About Site to Site Events Using PfRv3, on page 317 for more information.
Trace the application traffic path	Select the required application from the Trace Application Path drop-down list, to trace the application traffic path. These applications are auto-populated from the border router Egress NetFlow in the selected time interval.
View Site to Site topology	Click Site to Site Details in the Live topology to go to Site to Site details tab. See View Details About Site to Site Events Using PfRv3, on page 317 for more information.

Related Topics

View PfRv3 Service Provider and DSCP Charts, on page 316
Get Access to PfR Monitoring for a User Group, on page 314
View Details About Site to Site Events Using PfRv3, on page 317
Compare WAN Interfaces Usage Using PfRv3, on page 319

View PfRv3 Service Provider and DSCP Charts

The Metrics panel displays Service provider View and DSCP View charts.

Service Provider View Chart—Displays the metrics gathered using the TCA. Each service provider is represented by a unique color in the chart. The charts available in this view are:

- Unreachability event count over time
- Maximum Delay over time
- Maximum Jitter over time
- Maximum Packet Loss% over time

DSCP View Chart—Displays six different metric charts with respect to different DSCPs. A maximum of five DSCPs can be viewed in the maximized view of the chart. You can also choose the required DSCP using the DSCP filter. The charts available in this view are:

- Service Provider (SP) Bandwidth (B/W) usage per DSCP
- DSCP vs TCAs
- DSCP vs Unreachable TCAs
- Maximum Delay Over time
- Maximum Jitter Over time
- Maximum Packet Loss% Over time

You can perform the following tasks in the Metrics Panel:

- Viewing different charts—Click the arrow icons in the metrics panel.
- Adding Charts—Click the add icon Add components. In the dialog box, choose the required components and clickSave.

Time Slider

A time slider present at the bottom of the page, represents the time range selected using the filter. You can drag the slider and set a particular time range. The Metrics Panels and the Site to Site PfR events table change corresponding to the set time range.

Related Topics

Use the PfR Monitoring Page, on page 314
View Details About Site to Site Events Using PfRv3, on page 317
Compare WAN Interfaces Usage Using PfRv3, on page 319

View Details About Site to Site Events Using PfRv3

From the Services > Application Visibility & Control > PfR Monitoring you can view various Site-to Site details as described in the following table.

Table 41: Site to Site Topology Tasks

Tasks	Description
View detailed information about Site to Site events	Click a dot in the Site to Site events table. You can see a Site to Site pop-up window. The pop-up window displays the type of events occurred in the selected time range, along with the event details in a table format. You can expand this window to the required size. The violated metrics (Byte Lost%, Delay, Jitter, Packet Loss%) that cause IME are indicated within Square Brackets [].

Tasks	Description
View Site to Site topology	Click Site to Site details in the pop-up window to view the schematic Site to Site topology representation and All Events table including the details of all events. The topology includes legends representing border router, primary controller, service provider, and Internal and External links. The topology is plotted based on the data for a minimum of 72 hours, even if you select a time frame of less than 72 hours using the time filter. The Border router and the corresponding links are dimmed and you cannot click them for the following reasons: • If the inventory collection has failed for the border router. • If the border router is not managed. • If a user is not authorized to access the border router (as per Role Based Access Control). Choose the VRF for which you want to see the topology, from theVRF drop-down list.
View Device Utilization Metrics Using PfRv3	Click the Primary Controller icon and select one of the following options: • Device Metrics—Opens a device metrics pop-up window comprising CPU and Memory utilization. • PfR Policy—Opens a Policy window including policies configured in the Primary controller, for different VRFs. Click each VRF to view the respctive policy. Click Sync with Device to view the latest policy information. Click any of the Border Router icons and select one of the following options: • Device Metrics—A device metrics pop-up window comprising CPU and Memory utilization opens. • Launch Device Dashboard—Opens the Device dashlets in the Performance dashboard. • Compare WAN Links—Opens the Compare WAN Links tab. See Compare WAN Interfaces Usage Using PfRv3, on page 319. for more information. • Analayze—Opens a device context tab. You can view the following: • Border router Metrics—Displays three charts in which the utilization of service provider Bandwidth, memory and CPU are plotted for the selected time range, and a chart in which Service Provider Usage is plotted against Traffic. Click the zoom icon to see the enlarged view of the chart. You can further enlarge the chart to view the data pattern in a specific time interval by moving the slider. • WAN Link Usage and Performance—Displays a table that shows WAN link usage and performance with respect to DSCP markings, for the WAN interfaces of the selected border router. The data includes Egress Bandwidth (B/W) usage, number of TCAs, RCs and IMEs occurred and the number of applications associated to DSCP markings.The number of applications is visible only if AVC NetFlow is received by for this WAN link. • Click the Expand arrow adjacent to the DSCP to drill-down to further details.

Tasks	Description

View Link Utilization Metrics Using PfRv3	Click an egress or ingress link in the topology and select one of the options:
	• Link Metrics—Opens a Link Metrics pop-up window
	• Launch Interface Dashboard—Opens the the Interface dashlets in the Performance dashboard.
	• Add to Compare—Opens the Compare WAN Links tab. See Compare WAN Interfaces Usage Using PfRv3, on page 319. for more information.
	• Analayze—Opens a device context tab. You can view the following:
	  • WAN Link Metrics—Displays SP Usage Trend, Top 10 Application Traffic (In and Out), Top 10 Application Usage (Out), Top QOS Class Map Statistics Trend, SP Usage - Traffic between Source Site and All Sites, and Interface Availability Trend charts.
	  • WAN Link Usage and Performance—Displays a table that shows WAN Link Usage and Performance with respect to DSCP markings, for the WAN interface.
	  • Click the Expand arrow adjacent to the DSCP to drill-down to further details.

Troubleshooting the Topology Diagram

If the topology is not loaded, check the following:

- Availability of any one of the border router, primary controller or service provider.
- Availability of PfR Bandwidth and Egress between the sites for the selected time Interval.
- There is no inventory failure in the protocol endpoint.
- The Interfaces are managed by .
- Availability of WAN links.
- Whether you have logged in as root user and have access to the required devices.

Related Topics

Use the PfR Monitoring Page, on page 314
Compare WAN Interfaces Usage Using PfRv3, on page 319

Compare WAN Interfaces Usage Using PfRv3

The Compare WAN Links tab shows a guided workflow for comparing the WAN link usage and performance of the selected WAN links.

Step 1 Choose Services > Application Visibility & Control > PfR Monitoring.

You can also click Compare WAN Links in the device metrics pop-up window in the or click Add To Compare in the Link Metrics pop-up window to view the Compare WAN Links tab. The border router and WAN Interface details get automatically populated based on the device or link you clicked.

Step 2 Click Compare WAN Links tab.

Step 3 Click the filter icon to view the Time Filter, if required.

Step 4 Choose the required options from PfR Controlled Site, Border Router and WAN Interface/SP drop-down lists, in each WAN link you want to compare.

Step 5 Click Compare to compare the selected WAN links.

Step 6 If you want to add third WAN link for comparison click + icon and select the required options and click Update.

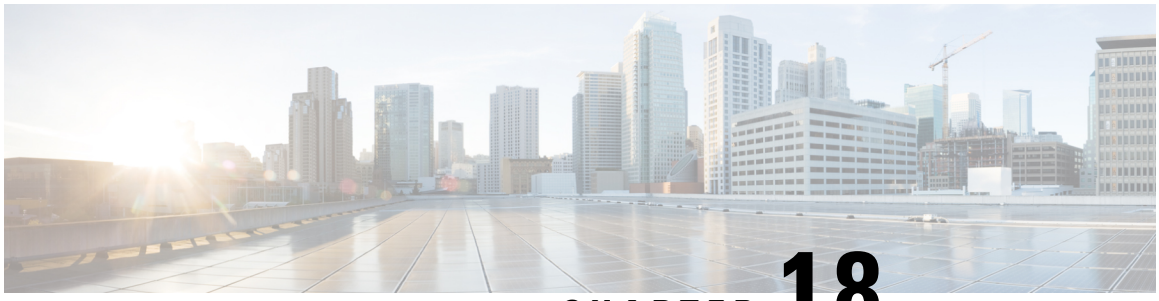
Step 7 Click the edit icon to change the previous selections.

You can view charts representing WAN link Utilization, Top N application, Top QOS Trend and Interface Availability of the select WAN links, and a table that compares the Egress Bandwidth (B/W) usage, number of TCAs, RCs and IMEs occurred and number of applications routed, for the selected WAN links.

Step 8 Click the required WAN link metrics to view the respective charts.

Related Topics

Use the PfR Monitoring Page, on page 314
View Details About Site to Site Events Using PfRv3, on page 317



CHAPTER 18

Monitor Wireless Networks

What is Radio Resource Management (RRM)

The operating system security solution uses the Radio Resource Management (RRM) function to continuously monitor all nearby access points to automatically discover rogue access points.

RRM, built into the Cisco Unified Wireless Network, monitors and dynamically corrects performance issues found in the RF environment.

would receive traps whenever a change in the transmit power of the access point or channel occurred. These trap events or similar events such as RF regrouping were logged into Prime Infrastructure events as informational and were maintained by the event dispatcher. The reason behind the transmit power or channel changes (such as signals from neighboring access points, interference, noise, load, and the like) were not evident. You could not view these events and statistics to then perform troubleshooting practices.

RRM statistics help to identify trouble spots and provide possible reasons for channel or power-level changes. The dashboard provides network-wide RRM performance statistics and predicts reasons for channel changes based on event groupings. The event groupings may include the following:

- Worst performing access points
- Configuration mismatch between controllers in the same RF group
- Coverage holes that were detected by access points based on threshold
- Precoverage holes that were detected by controllers
- Ratios of access points operating at maximum power

Note RRM dashboard information is available only for lightweight access points.

RRM Notifications Sent to Prime Infrastructure

Notifications are sent to the Prime Infrastructure RRM dashboard when a channel change occurs. Channel changes depend on the Dynamic Channel Assignment (DCA) configuration where the mode can be set to auto or on demand. When the mode is auto, channel assignment is periodically updated for all lightweight access points that permit this operation. When the mode is set to on demand, channel assignments are updated based on request. If the DCA is static, no dynamic channel assignments occur, and values are set to their global defaults.

When a channel change trap is received after an earlier channel change, the event is marked as Channel Revised; otherwise, it is marked as Channel Changed. A channel change event can have multiple causes. The reason code is factored and equated to 1, irrespective of the number of reasons that are possible. For example, suppose a channel change might be caused by signal, interference, or noise. The reason code in the notification is refactored across the reasons. If the event had three causes, the reason code is refactored to 1/3 or 0.33 per reason. If ten channel change events have the same reason code, all three reasons are equally factored to determine the cause of the channel change.

Notifications are sent to the Prime Infrastructure RRM dashboard when transmission power changes occur. Each event for transmit power changes is caused by multiple reasons. The reason code is factored and equated to one, irrespective of the number of reasons for the event to occur.

When RRM is run on the controller, dynamic grouping is done and a new group leader is chosen. Dynamic grouping has three modes: Automatic, Off, and Leader. When grouping is Off, no dynamic grouping occurs, and each switch optimizes only its own lightweight access point parameters. When grouping is Automatic, switches form groups and elect leaders to perform better dynamic parameter optimization. With automatic grouping, configured intervals (in seconds) represent the period with which the grouping algorithm is run. (Grouping algorithms also run when the group contents change and automatic grouping is enabled.)

Use the RRM Dashboard to Monitor APs

The RRM dashboard is available at Monitor > Wireless Technologies > Radio Resource Management.

The dashboard is made up of the following parts:

- The RRM RF Group Summary shows the number of different RF groups. To get the latest number of RF Groups, run the configuration synchronization background task.
- The RRM Statistics portion shows network-wide statistics.
- The Channel Change Reason portion shows why channels changed for all 802.11a/b/g/n radios.
    - Signal—The channel changed because it improved the channel quality for some other neighbor radio(s). Improving the channel quality for some other neighbor radio(s) improved the channel plan of the system as evaluated by the algorithm.
    - WiFi Interference
    - Load

- Radar
- Noise
- Persistent Non-WiFi Interference
- Major Air Quality Event
- Other

- The Channel Change shows all events complete with causes and reasons.
- The Configuration Mismatch portion shows comparisons between leaders and members.
- The Coverage Hole portion rates how severe the coverage holes are and gives their location.
- The Percent Time at Maximum Power shows what percent of time the access points were at maximum power and gives the location of those access points.

The following statistics are displayed:

- Total Channel Changes—The sum total of channel changes across 802.11a/b/g/n radios, irrespective of whether the channel was updated or revised. The count is split over a 24-hour and 7-day period. If you click the percentages link or the link under the 24-hour column, a page with details for that access point only appears.
- Total Configuration Mismatches—The total number of configuration mismatches detected over a 24-hour period.
- Total Coverage Hole Events—The total number of coverage hole events over a 24-hour and 7-day period.
- Number of RF Groups—The total number of RF groups (derived from all of the controllers which are currently managed by Prime Infrastructure).
- Configuration Mismatch—The configuration mismatch over a 24-hour period by RF group with details on the group leader.
- APs at MAX Power—The percentage of access points with 802.11a/n radios as a total percentage across all access points which are at maximum power. The maximum power levels are preset and are derived with reference to the preset value.

  Maximum power is shown in three areas of the RRM dashboard. This maximum power portion shows the current value and is poll driven.
- Channel Change Causes—A graphical bar chart for 802.11a/n radios. The chart is factored based on the reason for channel change. The chart is divided into two parts, each depicting the percentage of weighted reasons causing the event to occur over a 24-hour and 7-day period. Each event for channel change can be caused by multiple reasons, and the weight is equally divided across these reasons. The net reason code is factored and equated to one irrespective of the number of reasons for the event to occur.
- Channel Change - APs with channel changes—Each event for channel change includes the MAC address of the lightweight access point. For each reason code, you are given the most channel changes that occurred for the 802.11a/n access point based on the weighted reason for channel events. This count is split over a 24-hour and 7-day period.
- Coverage Hole - APs reporting coverage holes—The top five access points filtered by IF Type 11 a/n which triggered a coverage hole event (threshold based) are displayed.

- Aggregated Percent Max Power APs—A graphical progressive chart of the total percentage of 802.11a/n lightweight access points which are operating at maximum power to accommodate coverage holes events. The count is split over a 24-hour and 7-day period.

  This maximum power portion shows the values from the last 24 hours and is poll driven. This occurs every 15 minutes or as configured for radio performance.

- Percent Time at Maximum Power—A list of the top five 802.11a/n lightweight access points which have been operating at maximum power. This maximum power portion shows the value from the last 24 hours and is event driven.

View AP Interferers

In the Monitor > Wireless Technologies > Interferers page, you can monitor interference devices detected by CleanAir-enabled access points. By default, the Monitoring AP Detected Interferers page is displayed.

Table 42: Menu Paths to Monitor Interferers

To See...	Go To...
AP-detected interferers	Monitor > Wireless Technologies > Interferers **Note** This page does not display Interferers if using CMX.
AP-detected interferer details	Monitor > Wireless Technologies > Interferers > Interferer ID
AP-detected interferer details location history	Monitor > Wireless Technologies > Interferers > Interferer ID, then choose SLocation History, and click Go.

Edit the AP Detected Interferers Page

The Edit View page allows you to add, remove, or reorder columns in the AP Detected Interferers Summary page. To edit the columns in the AP Detected Interferers page, follow these steps:

SUMMARY STEPS

1. Choose Monitor > Wireless Technologies > Interferers. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.
2. Click the Edit View link.
3. To add an additional column to the access points table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the table.
4. To remove a column from the access points table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table.
5. Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.

6. Click Reset to restore the default view.
7. Click Submit to confirm the changes.

DETAILED STEPS

Step 1 Choose Monitor > Wireless Technologies > Interferers. The AP Detected Interferers page appears showing details of the interferers detected by the CleanAir-enabled access points.

Step 2 Click the Edit View link.

Step 3 To add an additional column to the access points table, click to highlight the column heading in the left column. Click Show to move the heading to the right column. All items in the right column are displayed in the table.

Step 4 To remove a column from the access points table, click to highlight the column heading in the right column. Click Hide to move the heading to the left column. All items in the left column are not displayed in the table.

Step 5 Use the Up/Down buttons to specify the order in which the information appears in the table. Highlight the desired column heading and click Up or Down to move it higher or lower in the current list.

Step 6 Click Reset to restore the default view.

Step 7 Click Submit to confirm the changes.

View RFID Tagged APs

The Monitor > Wireless Technologies > RFID Tags page allows you to monitor tag status and location on maps as well as review tag details.

This page is only available in the Location version of Prime Infrastructure.

This section provides information on the tags detected by the location appliance.

The Tag Summary page is available at Monitor > Wireless Technologies > RFID Tags.

Search for RFID Tags

Use the Prime Infrastructure Advanced Search feature to find specific tags or all tags.

To search for tags:

SUMMARY STEPS

1. Click Advanced Search.
2. From the Search Category drop-down list, choose Tags.
3. Enter the required information. Note that search fields sometimes change, depending on the category chosen.
4. Click Go.

DETAILED STEPS

Step 1 Click Advanced Search.

Step 2 From the Search Category drop-down list, choose Tags.

Step 3 Enter the required information. Note that search fields sometimes change, depending on the category chosen.

Step 4 Click Go.

Check RFID Tag Search Results

To check the search results, click the MAC address of a tag location on a search results page.

Note the following:

- The Tag Vendor option does not appear when Asset Name, Asset Category, Asset Group, or MAC Address is the search criterion.
- Only vendor tags that support telemetry appear.
- The Telemetry data option appears only when MSE (select for location servers), Floor Area, or Outdoor Area is selected as the “Search for tags by” option.
- Telemetry data displayed is vendor-specific; however, some commonly reported details are GPS location, battery extended information, pressure, temperature, humidity, motion, status, and emergency code.
- Asset Information, Statistics, Location, and Location Notification details are displayed.
- Only CCX v1 compliant tags are displayed for emergency data.

View Tag List

Click the Total Tags number link to view the Tags List for the applicable device name. The Tag List contains the MAC address, asset details, vendor name, mobility services engine, controller, battery status, and map location.

Monitor Wireless Media Streams

To monitor the media streams configurations, follow these steps:

Step 1 Choose Monitor > Wireless Technologies > Media Streams. The Media Streams page appears showing the list of media streams configured across controllers.

Step 2 To view the media stream details, click a media stream name in the Stream column. The Media Streams page appears.

Troubleshoot Unjoined APs

When a lightweight access point initially starts up, it attempts to discover and join a wireless LAN controller. After joining the wireless controller, the access point updates its software image if needed and receives all the configuration details for the device and network. After successfully joining the wireless controller, the access point can be discovered and managed by . Until the access point successfully joins a wireless controller

the access point cannot be managed by and does not contain the proper configuration settings to allow client access.

provides you with a tool that diagnoses why an access point cannot join a controller and lists corrective actions.

The Unjoined AP page displays a list of access points that have not joined any wireless controllers. All gathered information about the unjoined access point is included in the page. This includes name, MAC address, IP address, controller name and IP address, switch and port that the access point is attached to, and any join failure reason if known.

To troubleshoot unjoined access points, do the following:

Step 1 Choose Monitor > Wireless Technologies > Unjoined Access Points. The Unjoined APs page appears containing a list of access points that have not been able to join a wireless controller.

Step 2 Select the access point that you wish to diagnose, then click Troubleshoot. An analysis is run on the access point to determine the reason why the access point was not able to join a wireless controller. After performing the analysis, the Unjoined APs page displays the results.

Step 3 If the access point has tried to join multiple wireless controllers and has been unsuccessful, the controllers are listed in the left pane. Select a controller.

Step 4 In the middle pane, you can view what the problem is. It will also list error messages and controller log information.

Step 5 In the right pane, recommendations for solving the problems are listed. Perform the recommended action.

Step 6 If you need to further diagnose a problem, you can run RTTS through the Unjoined AP page. This allows you to see the debug messages from all the wireless controllers that the access point tried to join at one time.

Identify Low-Frequency Transmitting AP Devices (Chokepoints)

Chokepoints are low-frequency transmitting devices. When a tag passes within range of a placed chokepoint, the low-frequency field awakens the tag, which, in turn, sends a message over the Cisco Unified Wireless Network that includes the chokepoint device ID. The transmitted message includes sensor information (such as temperature and pressure). A chokepoint location system provides room-level accuracy (ranging from few inches to 2 feet, depending on the vendor).

Chokepoints are installed and configured as recommended by the chokepoint vendor. After the chokepoint is installed and operational, it can be entered into the location database and plotted on a Prime Infrastructure map.

Add AP Chokepoints to Prime Infrastructure

To add a chokepoint to the database:

Step 1 Choose Monitor > Wireless Technologies > Chokepoints.

Step 2 From the Select a command drop-down list, choose Add Chokepoint

Step 3 Click Go.

Step 4 Enter the MAC address and name for the chokepoint.

Step 5 Specify either an entry or exit chokepoint.

Step 6 Enter the coverage range for the chokepoint.

Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 7 Click Save.

After the chokepoint is added to the database, it can be placed on the appropriate floor map.

Note Prime Infrastructure does not support Embedded Wireless Controller on an Access Point (EWC). It is only supported by Cisco DNA Centre.

Remove AP Chokepoints from Prime Infrastructure

To remove a chokepoint from the database:

Step 1 Choose Monitor > Wireless Technologies > Chokepoints.
Step 2 Select the check box of the chokepoint that you want to delete.
Step 3 From the Select a command drop-down list, choose Remove.
Step 4 Click Go.
Step 5 Click OK to confirm the deletion.

Remove Chokepoints from Prime Infrastructure Maps

To remove a chokepoint from a Prime Infrastructure map:

SUMMARY STEPS

1. Choose Maps > Wireless Maps > Site Maps.
2. In the Maps page, click the link that corresponds to the floor location of the chokepoint.
3. From the Select a command drop-down list, choose Remove Chokepoints.
4. Click Go.
5. Click OK to confirm the deletion.

DETAILED STEPS

Step 1 Choose Maps > Wireless Maps > Site Maps.
Step 2 In the Maps page, click the link that corresponds to the floor location of the chokepoint.
Step 3 From the Select a command drop-down list, choose Remove Chokepoints.
Step 4 Click Go.
Step 5 Click OK to confirm the deletion.

Edit AP Chokepoints

To edit a chokepoint in the Prime Infrastructure database and the appropriate map:

Step 1 Choose Monitor > Wireless Technologies > Chokepoints.

Step 2 In the MAC Address column, click the chokepoint that you want to edit.

Step 3 Edit the parameters that you want to change.

The chokepoint range is product-specific and is supplied by the chokepoint vendor.

Step 4 Click Save.

Enhance Tag Location Reporting with WiFi TDOA Receivers

TDOA receivers use the method of Time Difference of Arrival (TDOA) to calculate tag location. This method uses data from a minimum of three TDOA receivers to generate a tagged asset location.

Note If a TDOA receiver is not in use and the partner engine software is resident on the mobility service engine, then the location calculations for tags are generated using RSSI readings from access points.

Note The Cisco Tag engine can calculate the tag location using the RSSI readings from access points.

Before using a TDOA receiver within the Cisco Unified Wireless Network, you must perform the following steps:

1. Have a mobility services engine active in the network. See Add MSEs to , on page 774.
2. Add the TDOA receiver to Prime Infrastructure database and map. See Add WiFi TDOA Receivers to and Maps, on page 330.
3. Activate or start the partner engine service on the MSE using Prime Infrastructure.
4. Synchronize Prime Infrastructure and mobility services engines. See Data That is Synchronized With MSE, on page 780.
5. Set up the TDOA receiver using the AeroScout System Manager. See the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User's Guide for configuration details at the following URL: http://support.aeroscout.com

Add a WiFi TDOA Receiver to MSE

After the Wi-Fi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on an Prime Infrastructure map.

After adding TDOA receivers to the Prime Infrastructure maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than the Prime Infrastructure.

For more details on configuration options, see the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide at the following URL:XREF http://support.aeroscout.com.

To add a TDOA receiver to the Prime Infrastructure database and appropriate map, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > WiFi TDOA Receivers to open the All WiFi TDOA Receivers summary page.

To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

Step 2 From the Select a command drop-down list, choose Add WiFi TDOA Receivers, then click Go.

Step 3 Enter the MAC address, name and static IP address of the TDOA receiver.

Step 4 Click OK to save the TDOA receiver entry to the database.

After you add the TDOA receiver to the database, you can place the TDOA receiver on the appropriate Prime Infrastructure floor map.

A WiFi TDOA Receiver must be configured separately using the receiver vendor software.

Add WiFi TDOA Receivers to and Maps

After the WiFi TDOA receiver is installed and configured by the AeroScout System Manager and the partner software is downloaded on the mobility services engine, you are ready to add the TDOA receiver to the mobility services engine database and position it on a map.

After adding TDOA receivers to maps, you continue to make configuration changes to the TDOA receivers using the AeroScout System Manager application rather than .

For more details on configuration options, see the AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine User Guide at the following URL: http://support.aeroscout.com.

To add a TDOA receiver to the database and the appropriate map:

Step 1 Choose Monitor > Wireless Technologies > WiFi TDOA Receivers to open the All WiFi TDOA Receivers summary page.

To view or edit current WiFi TDOA receiver details, click the MAC Address link to open the details page.

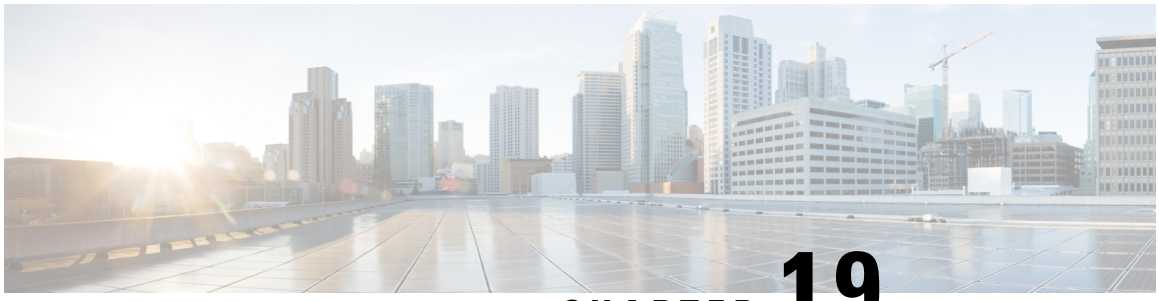
Step 2 From the Select a command drop-down list, choose Add WiFi TDOA Receivers.

Step 3 Click Go.

Step 4 Enter the MAC address, name, and static IP address of the TDOA receiver.

Step 5 Click Save to save the TDOA receiver entry to the database.

Note A WiFi TDOA Receiver must be configured separately using the receiver vendor software.



CHAPTER 19

Use Monitoring Tools

Perform a Wireless Controller Voice Audit

provides a voice auditing mechanism to check controller configuration and to ensure that any deviation from the deployment guidelines is highlighted as an Audit Violation. You can run a voice audit on a maximum of 50 controllers in a single operation.

To run the voice audit:

Step 1 Choose Monitor > Tools > Wireless Voice Audit.

Step 2 Click the Controllers tab, and complete the fields as described in the Voice Audit Field Descriptions section in the following link http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html.

Step 3 Click the Rules tab.

Step 4 In the VoWLAN SSID text box, type the applicable VoWLAN SSID.

Note The red circle indicates an invalid rule (due to insufficient data). The green circle indicates a valid rule.

Step 5 Do either of the following:

- To save the configuration without running a report, click Save.
- To save the configuration and run a report, click Save and Run.

Step 6 Click the Report tab to view the report results.

Check AP Performance Using the Voice Diagnostic Tool

The Voice Diagnostic tool is an interactive tool that diagnoses voice calls in real time. This tool reports call control errors, clients' roaming history, and the total number of active calls accepted and rejected by an associated AP.

The Voice Diagnostic test is provisioned for multiple controllers; that is, if the AP is associated with more than one controller during roaming, the Voice Diagnostic tool tests all associated controllers. supports testing on controllers whose APs are placed on up to three floors. For example, a map might have floors 1 to 4, with all APs associated to controllers (WLC1, WLC2, WLC3, and WLC4) and placed on the map. If a client on any AP is associated with WLC1 on the first floor and a Voice Diagnostic test is started for that client, a test is also provisioned on WLC2 and WLC3.

The Voice Diagnostic page lists prior test runs, if any. For information about the fields on this page, see the Voice Diagnostic Field Descriptions section in the (http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html).

From the Select a command drop-down list, you can start a new test, check the results of an existing test, or delete a test.

Note To support roaming, the tool figures out controllers in the same building as of client's associated AP building and adds to all controller's watchlist. The tool looks for controllers in +/-5 floors from client's current association A's location to configure on controllers. Configuration on controller's watchlist is done for 10 minutes. After 10 minutes controller will remove the entry from the watchlist.

To run a Voice Diagnostic test:

Step 1 Choose Monitor > Tools > Wireless Voice Audit.

Step 2 From the Select a command drop-down list, choose the New test and click Go.

Note You can configure a maximum of two clients for voice call diagnosis. Both clients can be on the same call or can be on a different call.

Step 3 Enter a test name and the length of time to monitor the voice call.

Step 4 Enter the MAC address of the device for which you want to run the voice diagnostic test.

Step 5 Select a device type; if you select a custom phone, enter an RSSI range.

Step 6 Click Start Test.

Wireless Configuration Audit

Choose Monitor > Tools > Wireless Configuration Audit to launch the Configuration Audit Summary page.

This page provides a summary of the following:

- Total Enforced Config Groups—Templates that are configured for Background Audit and are enforcement enabled.

- Total Mismatched Controllers—Configuration differences found between and the controller during the last audit.
- Total Config Audit Alarms—Alarms generated when audit discrepancies are enforced on configuration groups. If enforcement fails, a critical alarm is generated on the configuration group. If enforcement succeeds, a minor alarm is generated on the configuration group. Alarms contain links to the audit report, where you can view a list of discrepancies for each controller.
- Most recent 5 config audit alarms—Includes object name, event type, date, and time of the audit alarm.

Click View All to view the applicable Alarm page that includes all configuration audit alarms.

Determine Which Autonomous APs Can Be Migrated to Lightweight APs

Choose Monitor > Tools > Autonomous AP Migration Analysis to launch the Migration Analysis Summary page. Autonomous access points are eligible for migration only if all criteria have a pass status. A red X designates ineligibility, and a green check mark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version—Conversion is supported only from Cisco IOS 12.3(7)JA releases excluding Cisco IOS 12.3(11)JA, Cisco IOS 12.3(11)JA1, Cisco IOS 12.3(11)JA2, and Cisco IOS 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only
- Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.

Ensure AP Location Accuracy with the Location Accuracy Tool

You can analyze the location accuracy of non-rogue and rogue clients, interferers, and asset tags by using the Location Accuracy tool.

By verifying for location accuracy, you are ensuring that the existing access point deployment can estimate the true location of an element within 10 meters at least 90% of the time.

The Location Accuracy tool enables you to run either of the following tests:

- Scheduled Accuracy Testing—Employed when clients, tags, and interferers are already deployed and associated to the wireless LAN infrastructure. Scheduled tests can be configured and saved when clients, tags, and interferers are already prepositioned so that the test can be run on a regularly scheduled basis.
- On-Demand Accuracy Testing—Employed when elements are associated but not pre-positioned. On-demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy for a small number of clients, tags, and interferers.

Both are configured and executed through a single page.

Related Topics

Set Up the AP Location Accuracy Tool, on page 334
Schedule a Location Accuracy Test, on page 334
Run an On-Demand Location Accuracy Test, on page 336

Set Up the AP Location Accuracy Tool

You must enable the Advanced Debug option in to use the Scheduled and On-demand location accuracy tool testing features. The Location Accuracy tool does not appear as an option on the Monitor > Tools menu when the Advanced Debug option is not enabled.

To enable the advanced debug option in :

Step 1 In , chooseMaps > Wireless Maps > Site Maps.

Step 2 Choose Properties from the Select a command drop-down list, and click Go.

Step 3 Check theEnabled check box to enable the Advanced Debug Mode. Click OK.

Note If Advanced Debug is already enabled, you do not need to do anything further. Click Cancel.

Use the Select a command drop-down list in the Location Accuracy page, to create a new scheduled or on-demand accuracy test, to download logs for last run, to download all logs, or to delete a current accuracy test.

Note You can download logs for accuracy tests from the Accuracy Tests summary page. To do so, select an accuracy test and from the Select a command drop-down list, choose either Download Logs or Download Logs for Last Run. Click Go.

- The Download Logs option downloads the logs for all accuracy tests for the selected test(s).
- The Download Logs for Last Run option downloads logs for only the most recent test run for the selected test(s).

Related Topics

Ensure AP Location Accuracy with the Location Accuracy Tool, on page 333
Schedule a Location Accuracy Test, on page 334
Run an On-Demand Location Accuracy Test, on page 336

Schedule a Location Accuracy Test

Use the scheduled accuracy testing to verify the accuracy of the current location of non-rogue and rogue clients, interferers, and asset tags. You can get a PDF of the test results at Accuracy Tests > Results. The Scheduled Location Accuracy report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram.
- A cumulative error distribution graph.
- An error distance over time graph.

- A summary by each MAC address whose location accuracy was tested noting its actual location, error distance and a map showing its spatial accuracy (actual vs. calculated location), and error distance over time for each MAC.

To schedule a Location Accuracy test:

SUMMARY STEPS

1. ChooseMonitor > Tools > Location Accuracy.
2. Choose New Scheduled Accuracy Test from the Select a command drop-down list.
3. Enter a test name.
4. Choose an area type, a building, and a floor from the corresponding drop-down lists.
5. Choose a beginning and ending time for the test by entering the days, hours, and minutes. Hours are entered using a 24-hour clock.
6. Choose a destination point for the test results. (If you choose the e-mail option, you must first define an SMTP Mail Server for the target email address. Choose Administration > Settings > System Settings > Mail Server Configuration to enter the appropriate information.)
7. Click Position Test Points.
8. On the floor map, select the check box next to each client, tag, and interferer for which you want to check location accuracy.
9. (Optional) To enter a MAC address for a client, tag, or interferer that is not listed, select the Add New MAC check box, enter the MAC address, and click Go.
10. When all elements are positioned, click Save.
11. Click OK to close the confirmation dialog box.
12. To check the test results, click the test name, click the Results tab in the page that appears, and click Download under Saved Report.

DETAILED STEPS

Step 1 ChooseMonitor > Tools > Location Accuracy.

Step 2 Choose New Scheduled Accuracy Test from the Select a command drop-down list.

Step 3 Enter a test name.

Step 4 Choose an area type, a building, and a floor from the corresponding drop-down lists.

Note Campus is configured as Root Area, by default. There is no need to change this setting.

Step 5 Choose a beginning and ending time for the test by entering the days, hours, and minutes. Hours are entered using a 24-hour clock.

Note When entering the test start time, be sure to allow enough time prior to the test start to position testpoints on the map.

Step 6 Choose a destination point for the test results. (If you choose the e-mail option, you must first define an SMTP Mail Server for the target email address. Choose Administration > Settings > System Settings > Mail Server Configuration to enter the appropriate information.)

Step 7 Click Position Test Points.

Step 8 On the floor map, select the check box next to each client, tag, and interferer for which you want to check location accuracy.

When you select a MAC address check box, two icons appear on the map. One represents the actual location and the other represents the reported location. If the actual location for an element is not the same as the reported location, drag the actual location icon for that element to the correct position on the map. (You cannot drag the reported location.)

Step 9 (Optional) To enter a MAC address for a client, tag, or interferer that is not listed, select the Add New MAC check box, enter the MAC address, and click Go.

An icon for the newly added element appears on the map. If the element is on the location server but on a different floor, the icon appears in the left-most corner (in the 0,0 position).

Step 10 When all elements are positioned, click Save.

Step 11 Click OK to close the confirmation dialog box.

You are returned to the Accuracy Tests summary page.

Step 12 To check the test results, click the test name, click the Results tab in the page that appears, and click Download under Saved Report.

Related Topics

Ensure AP Location Accuracy with the Location Accuracy Tool, on page 333
Set Up the AP Location Accuracy Tool, on page 334
Run an On-Demand Location Accuracy Test, on page 336

Run an On-Demand Location Accuracy Test

You can run an On-Demand Accuracy Test when elements are associated but not prepositioned. On-Demand testing allows you to test the location accuracy of clients, tags, and interferers at a number of different locations. It is generally used to test the location accuracy of a small number of clients, tags, and interferers. You can get a PDF of the test results at Accuracy Tests Results. The On-Demand Accuracy Report includes the following information:

- A summary location accuracy report that details the percentage of elements that fell within various error ranges.
- An error distance histogram.
- A cumulative error distribution graph.

To run an On-Demand Accuracy Test:

Step 1 Choose Monitor > Tools > Location Accuracy.

Step 2 From the Select a command drop-down list, choose New On demand Accuracy Test.

Step 3 Enter a test name.

Step 4 Choose an area type, a building, and a floor from the corresponding drop-down lists.

Note Campus is configured as Root Area, by default. There is no need to change this setting.

Step 5 Choose a destination point for the test results. (If you choose the e-mail option, you must first define an SMTP Mail Server for the target email address. Choose Administration > Settings > System Settings > Mail ServerConfiguration to enter the appropriate information.)

Step 6 Click Position Test Points.

Step 7 To test the location accuracy and RSSI of a particular location, select client, tag, or interferer from the drop-down list on the left. A list of all MAC addresses for the selected option (client, tag, or interferer) is displayed in a drop-down list to the right.

Step 8 Choose a MAC address from the drop-down list, move the red cross hair to a map location, and click the mouse to place it.

Step 9 From the Zoom percentage drop-down list, choose the zoom percentage for the map.

The X and Y text boxes are populated with the coordinates based on the position of the red cross hair in the map.

Step 10 Click Start to begin collection of accuracy data, and click Stop to finish collection. You must allow the test to run for at least two minutes before stopping the test.

Step 11 Repeat Step 7 to Step 10 for each testpoint that you want to plot on the map.

Step 12 Click Analyze Results when you are finished mapping the testpoints, and then click the Results tab in the page that appears to view the report.

Related Topics

Ensure AP Location Accuracy with the Location Accuracy Tool, on page 333
Set Up the AP Location Accuracy Tool, on page 334
Schedule a Location Accuracy Test, on page 334

Monitoring IPSLA

Perform the following steps to implement the IPSLA real time monitoring:

Before you begin

The IPSLA Real Time Monitoring page helps users to analyse and monitor the devices to extract detailed information on parameters such as, response time, packet loss, performance of application, and so on.

Step 1 Navigate to Monitor > Tools > IPSLA Real Time Monitoring.

Step 2 Click the Next button in the Begin page.

Step 3 Select the source and destination devices. You can filter the devices based on the device name.

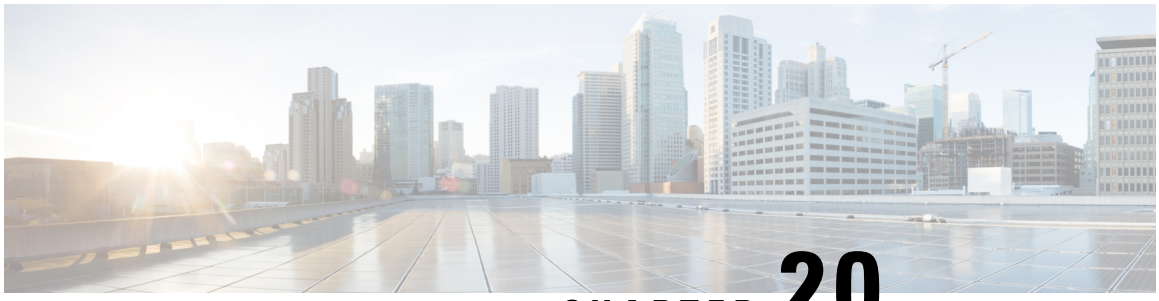
The source and destination devices cannot be the same.

Step 4 Select the Operation Type. You must enter a port number if you select the operation type as UDP Echo or UDP Jitter. The value must be between 1 and 65535. Enter a valid URL, if you select the operation type as HTTP/TCP.

Step 5 Click the Clear Selections button to discard the selections.

Step 6 Click the Next button to view the monitoring charts. The charts get regenerated every minute. Once the number of captures reaches 10, the earlier data disappears from the chart and the latest capture information is displayed.

Note Click the refresh icon if you wish to move to the Begin page without saving the data.



CHAPTER 20

Monitor Wireless and Data Center Performance Using Performance Graphs

To compare the Key Performance Indicators (KPIs) for devices and interfaces, choose Monitor > Monitoring Tools > Performance Graphs. You can chose the device or interface metrics you want to view over a specified time, and the resulting performance graphs allows you to quickly monitor performance.

Create Performance Graphs

Step 1 Choose Monitor > Monitoring Tools > Performance Graphs.

The first time you access this page, an overlay help window appears with helpful tips.

Step 2 Select one of the tabs at the top of the left frame:

- Devices—Allows you to select a device for which to create a performance graph.
- Interfaces—Allows you to select an interface for which to create a performance graph.

Depending on what you select, the Metrics panel displays the available metrics for the device or interface type.

Step 3 Hover your cursor over a metric for which you want to measure performance, then click and drag the metric on to the Graphs portion of the window.

An overlay help window appears explaining the icons, date range, and other information.

Related Topics

View Multiple Metrics on a Single Performance Graph, on page 340

Performance Graphs Options, on page 340

View Multiple Metrics on a Single Performance Graph

You might want to view more than one metric on a single performance graph. For example, if you see a spike in CPU utilization, you might to add the memory utilization metric to the performance graph to see if the memory was impacted by change in CPU utilization.

You can add a maximum of 10 metrics on a single performance graph.

Note Prime Infrastructure does not monitor the interface of the UCS devices with fabric interconnect. Hence, the Tx and Rx utilization details will not be displayed in the Performance Graphs screen.

Step 1 Choose Monitor > Monitoring Tools > Performance Graphs.

Step 2 Select one of the tabs at the top of the left frame:

- Devices—Allows you to select a device for which to create a performance graph.
- Interfaces—Allows you to select an interface for which to create a performance graph.

Depending on what you select, the Metrics panel displays the available metrics for the device or interface type.

Step 3 Hover your cursor over a metric for which you want to measure performance, then click and drag the metric on to the Graphs portion of the window.

Step 4 To add a second metric to the same graph, hover your cursor over the metric you want to add, then click and drag the metric on to the same graph that has the metric you added in the previous step.

If you don't want multiple metrics in a single graph, you can create a new graph on the same page by dragging the metric on to the lower portion of the Graphs window where Drop item here is displayed.

Step 5 To launch the Device 360° View, click on the IP address hyperlink at the top of the graph.

Related Topics

Create Performance Graphs, on page 339
Performance Graphs Options, on page 340

Performance Graphs Options

The Show menu at the top of the performance chart allows you to change the following graph display options:

- Legend Options—Specify whether to show or hide the legend.
- Show Legends—Specify if the legends are at the right or the top of the performance chart.
- Show Alarms—Specify whether to display alarms. A colored flag appears in the performance graph to indicate that an alarm occurred at that time. To view details about the alarm, click on the colored flag.
- Show Config Changes—Specify whether to display configuration changes. A black flag appears in the performance graph to indicate that a configuration on the device was modified at that time. To view details about the configuration change, click on the flag.

You can also Export and Print performance graphs by clicking the arrow at the top of the graph.

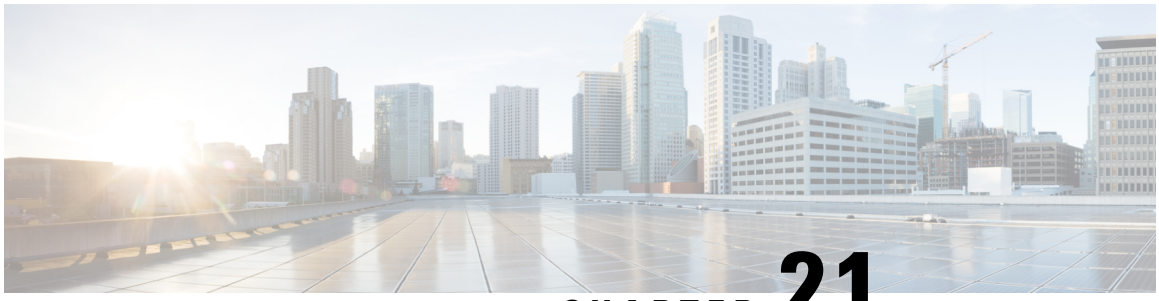
Click Detach at the top right of the performance graph page to open the performance graph in a new browser window. This allows you to continue monitoring the performance graph in a separate window while you perform actions in another window.

You can draw up to 10 charts on each tab and up to 7 series in each chart. Any additional charts or series over these limits are not displayed and a warning message appears. To add additional charts, add a new tab and add additional charts you want to plot to the new tab.

If you plot a parent group with more than 7 items, the items are drawn in one chart to allow you to view the data for the entire group.

Related Topics

Create Performance Graphs, on page 339
View Multiple Metrics on a Single Performance Graph, on page 340



CHAPTER 21

Troubleshooting

provides the following for sophisticated monitoring and troubleshooting of end-user network access.

The following sections describe some typical troubleshooting tasks:

Get Help from the Cisco Support Community and Technical Assistance Center (TAC)

Open a Cisco Support Case

When you open a support case from the web GUI, automatically populates the case form with information it can retrieve from a device. This includes technical details about the device, configuration changes on the device, and all device events that occurred in the last 24 hours. You can also attach your own files to the case.

Before you begin

You can open a support case from the web GUI if:

- Your administrator has configured to allow you to do so. .
- The server has a direct connection to the internet, or a connection by way of a proxy server.
- You have a Cisco.com username and password.

Step 1 Choose one of the following:

- From Monitor > Monitoring Tools > Alarms and Events. Click a single alarm, then choose Troubleshoot > Support Case. If you do not see the Troubleshoot button, widen your browser window.
- From the Device 360 view. Hover your mouse over a device IP address, then click the information icon. Choose Support Request from the Actions drop-down menu.

Step 2 Enter your Cisco.com username and password.

Step 3 Click Create. populates the form with data it retrieves from the device.

Step 4 (Optional) Enter a Tracking Number that corresponds to your own organization's trouble ticket system.

Step 5 Click Next and enter a description of the problem.

populates the form with data it retrieves from the device and automatically generates the necessary supporting documents.

If desired, upload files from your local machine.

Step 6 Click Create Service Request.

Join the Cisco Support Community

You can access and participate in discussion forums in the online Cisco Support Community. You will need a Cisco.com username and password.

Step 1 Choose one of the following:

- From Monitor > Monitoring Tools > Alarms and Events. Click a single alarm, then choose Troubleshoot > Support Forum. If you do not see the Troubleshoot button, widen your browser window.
- From the Device 360 view. Hover your mouse over a device IP address, then click the information icon. Choose Support Community from the Actions drop-down menu.

Step 2 In the Cisco Support Community Forum page, enter your search parameters to find what you need.

Troubleshoot User Problems

You can use the User 360° View to troubleshoot problems reported by users.

Step 1 In the Search field on any page, enter the end user's name.

Step 2 In the Search Results window, hover your mouse cursor over the end user's name in the User Name column, then click the User 360° view icon. See Get User Details from the User 360° View, on page 875.

Step 3 With the User 360° view displayed, identify where the problem is occurring using the information described in the following table.

To Gather This Data	Click Here in User 360° View	Additional Information
Information about the device to which the user is attached, such as the endpoint, location, connections, and session information	Click a device icon at the top of the User 360° View.	Click available links to display additional information. For example, you can click the Authorization Profile link to launch ISE. If the end user is not associated with the appropriate policy category, you can hand off the problem (for example, to an ISE admin or help tech) or perform actions outside Prime Infrastructure to investigate why the user was placed in the current policy category (Authorization Profile). Check to see whether there are any indications of authentication errors (authentication failure could be due to various things, including an expired password). The visual indication of authentication errors allows you to see more data related to the authentication errors. At that point, you might need to hand off the problem (for example, to an ISE admin or help tech).
Alarms associated with the device to which the user is attached	Click a device icon at the top of the User 360° View, then click the Alarms tab.	Click the Troubleshoot Client icon  to go to client troubleshooting.

To Gather This Data	Click Here in User 360° View	Additional Information
Applications running on the device to which the user is attached and Site Bandwidth Utilization	Click a device icon at the top of the User 360° View, then click the Applications tab.	Click an application to view the end-user data filtered for the user you specified. To get more information about an application, choose Dashboard > Performance > Application. To get more information about an application, including the bandwidth utilization of the application consumed by the end user (the bandwidth consumed for the conversation), choose Dashboard > Performance > Application. **Note** This feature requires: • Integration with an ISE server (to access endpoint information). • For wired sessions, that AAA accounting information is being sent to ISE. • That session information (netflow/NAM data, Assurance licenses) is available.

To Gather This Data	Click Here in User 360° View	Additional Information
Information about Site Network Devices	Click a device icon at the top of the User 360° View, then click the Alarms tab.	You can choose to view: • Active alarms list for the site • List of all site devices (with alarm indications) • Topo map of site (with alarm indications) If a problem with a site has been detected, an alarm icon will appear next to the site location. Click the icon to view all of the alarms associated with that site. If a problem has been detected, it might not be appropriate to continue troubleshooting the problem; it is probably sufficient to note that fact and hand off the task to second tier support. If you want to continue detailed client troubleshooting, exit the User 360° View and launch the full client and user troubleshooting page (choose Monitor > Monitoring Tools > Clients and Users).
Information about network Attachment Devices	Click a device icon at the top of the User 360° View, then click the Alarms tab.	Click the Go to Client Details icon.

Monitor Applications and Their Performance

Use the following procedure to determine if there are any problem indications associated with any of the specific applications being run across the network by the end user.

Before You Begin

This feature requires:

- Integration with an ISE server (to access endpoint information).
- That session information (NetFlow/NAM data, Assurance licenses) is available.

Step 1 To view the applications accessed by the end user and the response time for the applications for the user's devices, open the User 360° View for that user and click the Applications tab.

Step 2 This tab displays the following information:

a. Endpoint

b. Mac address

c. Application

d. Last one hour volume (in MB)

To get more information about an application, choose Dashboard > Performance > Application.

Troubleshoot Wireless Device Performance Problems

If an end user reports a problem with their wireless device, you can use the Site dashboard to help you determine the AP that is experiencing problems.

Before You Begin

This feature requires that session information (netflow/NAM data, Assurance licenses) is available.

Step 1 Choose Dashboard > Performance > Site and view the site to which the client experiencing trouble belongs.

Step 2 To see the AP that is experiencing trouble at this site, click the Settingsicon, then click Add next to Busiest Access Points.

Step 3 Scroll down to the Busiest Access Points dashlet. You can

a. Hover your mouse over a device to view device information. See Get Device Details from Device 360° View, on page 871.

b. Click on an AP name to go to the AP dashboard from where you can use the AP filter option to view AP details such as Client Count, Channel Utilization, and, if you have an Assurance license, Top N Clients and Top N Applications.

- Utilization based on SNMP polling for the APs.
- Volume information based on Assurance NetFlow data, if you have an Assurance license. For example, you can see the traffic volume per AP.

Root Cause and Impact Analysis of Physical and Virtual Data Center Components

The physical servers shows the list of UCS B-Series and C-series servers that are managed by . It also shows the Host/Hypervisor running on these servers, only if the corresponding Vcenter is added.

The Cisco UCS Server Schematic shows the complete architecture of the UCS device. The Schematic tab shows a graph that can be expanded to show different elements of UCS device such as chassis and blades. You can view quick summary of the element by hovering your mouse over the operational status icon next to the chassis or blade. In addition, clicking on the operational status icon, which symbolizes each unique element (chassis or blade), would show the subsequent connection. You can view the connection to host and its VM if managed by by clicking the operational status icon. The schematic view also shows the operational status of the data center components and the associated alarms using which you can trace the root cause of an application delivery failure to a UCS hardware problem of Cisco UCS device.

Troubleshoot UCS Device Hardware Problems

Use the following procedure to trace the root cause of an application delivery failure to a UCS hardware problem of Cisco UCS B-series and C-series servers. You can identify whether the problem is in fabric interconnect port, chassis or blades.

To identify the issue in UCS chassis, blade server, fabric interconnect port:

Step 1 Choose Inventory > Device Management > Compute Devices.

Step 2 Choose Cisco UCS Servers in the Compute Devices pane.

Step 3 Click the faulty UCS device in the Cisco UCS Servers pane to view the Schematic tab that shows the inter-connections of the UCS chassis and blades, and the up/down status of chassis and blade servers. Hover your mouse over the faulty chassis or blade server name to view the Quick Summary of the element.

If you want to view the detailed information about the faulty chassis or blade server, click View 360.

Step 4 Click the Chassis tab and hover your mouse cursor over the faulty chassis name, then click the information icon to launch the chassis 360° view that shows up/down status of power supply unit and fan modules.

Step 5 Click the Servers tab and hover your mouse cursor over the faulty blade server name, then click the information icon to launch the server 360° view.

The server 360° view provides detailed blade server information including the number of processors, memory capacity, up/down status of adapters, Network Interface Cards (NICs), and Host Bus Adapters (HBAs) and Service Profile.

Step 6 Click the Network tab to view the entire network interface details of fabric interconnect such as port channel, Ethernet interface, vEthernet, and vFabric Channel.

Step 7 Click the IO Modules tab to view the operational status of backplane ports and fabric ports.

Step 8 Click the Service Profile tab to view the hardware faults that impacts the services.

Step 9 In the Service Profile pane on the left, click the expand icon to view the service profiles.

Step 10 Click the information icon corresponding to the service profile to view the alarm severity levels of that service profile.

Step 11 Click the faulty service profile in the Service Profile pane on the left to view the Service Profile table that displays the Profile Name, Service Profile Template, Server, Overall Status, Associated status and Associated Alarms.

Step 12 Click the information icon corresponding to the profile name in the Service Profile table to launch the Service Profile 360° view that shows the basic summary information of the service profile.

Identify the bandwidth issue in fabric interconnect port

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Click the faulty UCS device from the All Devices pane.

Step 3 Click the expand icon corresponding to fabric interconnect switch.

Step 4 Click Fixed ModulesFixed Modules to view the operational status of fabric interconnect ports.

Step 5 Click Interfaces to view the operational status for fabric interconnect port and interfaces. This is same as the operational stays of fabric interconnect port and interfaces viewed from Network tab in Compute Devices page.

Troubleshoot UCS Device Bandwidth Problems

You can view the details of a fabric interconnect port or a fabric interconnect port group using the Top-N Interface Utilization dashlet from the Overview and Performance dashboards. Use the following procedure to identify whether the overuse of bandwidth on the ports connecting the fabric interconnect to the UCS chassis is causing application performance issues such as slowness on Cisco UCS.

We recommend you to create a fabric interconnect port group and select the port group in the dashlet to view the bandwidth utilization details.

To identify the overuse of bandwidth on the fabric interconnect ports:

Step 1 Choose Dashboard > Performance > Interface then choose the UCS device interface from the Interface drop-down list.

or

Choose Dashboard > Overview > Network Interface.

Step 2 Click the Settings icon as shown in and choose Add Dashlets.

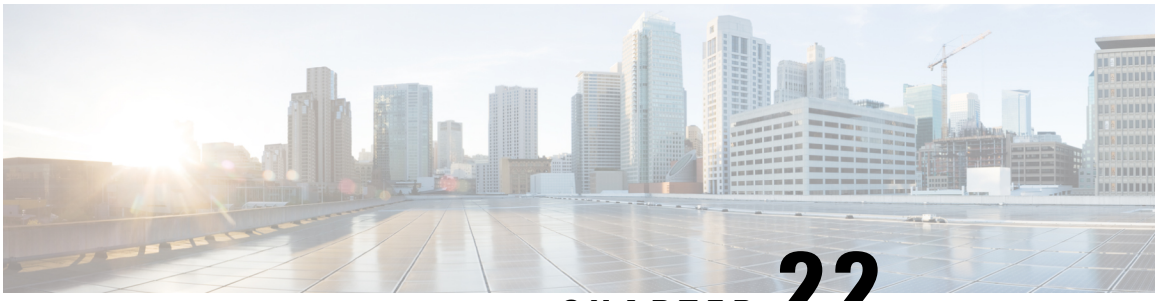
Step 3 Choose Top N Interface Utilization dashlet and click Add.

Step 4 Do the following if you have already created a fabric interconnect port group:

a) Click the Dashlet Options icon in the Top N Interface Utilization dashlet.

b) Select the fabric interconnect port group in the Port Group and click Save And Close.

The Top N Interface Utilization dashlet displays the list of interfaces with maximum utilization percentage. This dashlet also shows the average and maximum data transmission and reception details of the fabric interconnect ports.



CHAPTER 22

Use Operations Center to Monitor Multiple Prime Infrastructure Instances

How to Monitor Multiple Instances

There are three situations in which you will want to use multiple server instances to manage your network:

- You want to categorize the devices in your network into logical groups, with a different instance managing each of those groups. For example, you could have one instance managing all of your network's wired devices and another managing all of its wireless devices.
- The one instance you have running is sufficient to manage your network, but the addition of one or more instances would improve performance by spreading the CPU and memory load among multiple instances.
- Your network has sites located throughout the world, and you want a different instance to manage each of those sites in order to keep their data separate.

If multiple instances are running in your network, you can monitor those instances from the Operations Center. In this chapter, we will cover a typical workflow you might employ when using the Operations Center. This workflow consists of the following tasks:

- Use the Operations Center Config Dashboard to Manage Multiple Servers
- Run Reports on Deployments with Multiple Servers Using Operations Center

See Related Topics for more details:

Related Topics

Run Reports on Deployments with Multiple Servers Using Operations Center, on page 366
Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 352
FAQs: Operations Center and Prime Infrastructure, on page 905

Use the Operations Center Config Dashboard to Manage Multiple Servers

After viewing the various dashboards available in the Operations Center, you can then take a closer look at what is going on in your network. Specifically, you can monitor:

- The devices that belong to your network.
- The servers that manage those devices.
- The alarms, events and other incidents that have taken place in your network.
- The clients and users configured to use your network.

The following related topics cover these items in more detail.

Related Topics

View Devices Managed by All Servers Using Operations Center, on page 359
Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 360
Manage Servers using Operations Center, on page 363
View the Status of Multiple Servers using Operations Center, on page 364
View Software Updates on Multiple Prime Infrastructure Servers Using Operations Center
View Alarms on Devices Managed by Multiple Servers Using Operations Center, on page 365
View Clients and Users Managed by Multiple Servers Using Operations Center, on page 366

Supported Reports in Operations Center

The list of supported reports in operation center are:

- Autonomous AP
  - Autonomous AP Summary
  - Autonomous AP Uptime
- CleanAir
  - Air Quality vs Time
  - Security Risk Interferers
  - Worst Air Quality APs
  - Worst Interferers
- Client
  - Busiest Clients
  - CCX Client Statistics
  - Client Count
  - Client Sessions

- Client Summary
- Client Traffic
- Client Traffic Stream Metrics
- Mobility Client Summary
- Throughput
- Unique Clients
- Unique Clients and Users Summary

- Compliance
  - Change Audit
  - Network Discrepancy
  - PCI DSS Detailed
  - Wireless Configuration Audit

- Device
  - AP Ethernet Port Utilization
  - AP Profile Status
  - AP Radio Downtime Summary
  - AP Summary
  - AP Utilization
  - Busiest APs
  - CPU Utilization
  - Detailed Hardware
  - Detailed Software
  - Device Credential Verification
  - Device Health
  - Interface Availability
  - Interface Detail
  - Interface Utilization
  - Interface Utilization Trend
  - Inventory
  - Memory Utilization
  - Non-Primary Controller APs

- Port Capacity
- Port Reclaim Report
- Top AP by Client Count
- Unified AP Ping Availability
- Vlan
- Wired Device Availability
- Wired Module Detail
- Wired Port Attribute
- Wireless Up Time
- Wireless Utilization

- Guest
  - Guest Accounts Status
  - Guest Association
  - Guest Count
  - Guest Operations
  - Guest User Sessions
- Mesh
  - Link Stats
- Network Summary
  - 802.11n Summary
  - Wireless Network Executive Summary
- Performance
  - 802.11 Counters
  - AP RF Quality
  - AP RF Quality History
  - Application Summary
  - Conversations
  - Coverage Hole
  - Environmental Temperature
  - Interface Errors and Discards
  - Interface Summary

- Threshold Violation
- VoIP Calls Graph
- VoIP Calls Table
- Voice Statistics
- Wireless Network Utilization
- Wireless Traffic Stream Metrics
- Wireless Tx Power and Channel
- Worst RF APs

- Raw NetFlow
  - Netflow V5

- Security
  - Adaptive wIPS Alarm
  - Adaptive wIPS Top 10 AP
  - Adhoc Rogues
  - New Rogue AP Count Summary
  - New Rogue APs
  - Rogue AP Count Summary
  - Rogue AP Events
  - Rogue APs(Updated)
  - Security Alarm Trending Summary
  - Wired Rogue APs via SPT(New)

- System Monitoring
  - CPU Threshold Breach Reports

Supported Dashlet in Operations Center

The list of supported dashlets in the operation center are:

- Network Summary
  - Overview
    - Interface Availability Summary
    - Interface Utilization Summary
    - Top N CPU Utilization
    - Top N Environmental Temperature

- Top N Interface Utilization
- Top N Memory Utilization
- Top N WAN Interfaces by Utilization

- Incidents
  - Alarms
  - Device Reachability Status
  - Syslog Summary
  - Syslog Watch
  - Top N Syslog Sender
  - Top N Alarms Types
  - Top N Event Types

- Client Summary
  - Client Count By Association/Authentication
  - Client Count By Wireless/Wired
  - Client Distribution
  - Client Posture Status
  - Client Traffic
  - Coverage Area
  - Top 5 SSIDs by Client Count
  - Top 5 Switches by Client Count

- Site Summary
  - Top N Applications
  - Top N Clients
  - Top N Devices With Most Alarms
  - Top N Servers

- Network Health

- Overview
  - Incidents
    - Top N Sites with Most Alarms
    - Top N Alarm Types

- Alarm Summary
- Device Reachability Status

- Client
  - Client Count By Association/Authentication
  - Client Count By Wireless/Wired
  - Client Distribution
  - Client Posture Status
  - User Auth Failure Count
  - Guest Users Count
  - Most Recent Client Alarms

- Network Devices
  - Coverage Area
  - Recent Alarms
  - Top N CPU Utilization
  - Top N Memory Utilization
  - Device Availability Summary
  - Interface Availability Summary

- Network Interface

- Wireless
  - Security
    - AP Threats/Attacks
    - Attacks Detected
    - Cisco Wired IPS Events
    - CleanAir Security
    - MFP Attacks
    - Security Index

  - Mesh
    - Mesh Top Over Subscribed AP

  - Clean Air
    - 802.11a/n/ac/ax Interferer Count

- 802.11b/g/n/ax Interferer Count
- Recent Security-risk Interferers
- Worst 802.11a/n/ac/ax Interferers
- Worst 802.11b/g/n/ax Interferers

- Context Aware
  - Rouge Element Detected by CAS

- Performance
  - Device
    - Device Memory Utilization Trend
    - Device Port Summary
    - Device CPU Utilization Trend
    - Device Health Information

Add Devices Using Operations Center

Operations Center allows you to add the devices to one or more of managed instances from the Operations Center user interface. In addition to manually adding devices, you can also choose to import devices using the Bulk Import option.

Step 1 Choose Monitor > Managed Elements > Network Devices.

Step 2 To add devices manually, do the following:

a) Click the + icon above the Network Devices table, then choose Add Device.
b) In the Add Device dialog box, choose the server to which you want to add the devices.
c) Complete the required fields. Click the "?" next to a field for a description of that field.

Note Telnet/SSH information is mandatory for devices such as most Cisco NCS devices.

d) (Optional) Click Verify Credentials to validate the credentials before adding the device.

supports HTTP credentials-verification for NAM devices only.

e) Click Add to add the device with the settings you specified.

Note User Defined Field (UDF) parameters will be available for the new device only if you first choose Administration > Settings > System Settings > Inventory > User Defined Fields and then add these UDF parameters. Do not use the special characters : ; and # for UDF field parameters.

Step 3 To import devices from another source using CSV file, do the following:

a) Click the + icon above the Network Devices table, then choose Bulk Import.
b) In the Bulk Device Import dialog box, choose the server to which you want to import the devices.

c) Click Choose File and select the CSV file containing the device details for bulk import.

For details on creating a CSV file, see Create Device Import CSV Files, on page 34

d) Click Import.

Move Device from One Prime Infrastructure Instance to Another Prime Infrastructure Instance

You can move the device that is managed in one instance to another instance for load balancing among different managed instances.

Step 1 Choose Monitor > Managed Elements > Network Devices.

Step 2 In the Network Devices table, choose the device and click Move Device.

Step 3 In the Moving Devices Dialog box, choose the server to which you want the device to be moved.

Step 4 Check the Remove device from source server check box and click OK.

If you uncheck the Remove device from source server check box, the device will be managed by more than one instance which is not a recommended practice.

View Devices Managed by All Servers Using Operations Center

Select Monitor > Managed Elements > Network Devices to open the Network Devices page in Operations Center. From here, you can view information for every device that belongs to your network that a instance is managing. This information includes the device's hostname/IP address, its current reachability status, and the last time inventory data was successfully collected from that device. You can also launch the Device 360° view and perfom Telnet, Ping, and Traceroute actions.

When you first open the Network Devices page, every network device is displayed. To refine the devices displayed, do one of the following:

- From the Device Group pane, select the desired device type, location, or user-defined group.

Note Cisco Prime Infrastructure Operations Center now supports the Meraki group of devices which includes Meraki Access Point, Meraki Dashboard, Meraki Security Appliances, and Meraki Switches. Click on any one of the Meraki device groups to view the list of devices associated with that particular group.

- Apply a custom filter or select one of the predefined filters from the Show drop-down list. Operations Center provides a custom filter that allows you to view duplicate devices across your managed instances. For details on how to use filters, see the related topic "Quick Filter".
- Search for a particular device. For details, see the related topic "Search Methods".
- If you want to hide the empty device groups, do the following:

- Choose Administration > System Settings > Inventory > Grouping.
- Uncheck the Display groups with no members check box.
- Click Save.

If you delete a device from the Operations Center Network Devices page, the device is also deleted from all the managed instances monitoring that device.

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 352
Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 360
Quick Filters, on page 867
Search Methods, on page 877

Synchronize Devices Using Operations Center

To synchronize the Prime Infrastructure Operation Center database with the configuration running on Prime Infrastructure devices, you can force an inventory collection.

To synchronize devices, follow these steps:

Step 1 Choose Monitor > Managed Elements > Network Devices.

Step 2 Select the device(s) whose configuration you want synchronized with the configuration stored in the Prime Infrastructure Operation Center database.

Step 3 Click Sync.

Note If the synchronized device is a default/Admin VDC, then all the configuration of all the child VDCs are synchronized automatically and the configuration is updated in the Prime Infrastructure Operation Center database. Admin VDC sync will also add the newly added VDC in hardware to the user interface or delete the deleted VDC in hardware from the user interface.

Use Virtual Domains on Deployments with Multiple Servers Using Operations Center

As explained in Control User Access, this feature provides an Operations Center administrator the ability to define a virtual domain on managed instances. The Virtual Domains page will be modified to give Operations Center administrators visibility to each virtual domain defined under a managed instance. The list of domains will be consolidated and displayed in the Operations Center.

From the Operations Center, you can view all the virtual domains available in all of the instances that Operations Center is managing.

You can also create or edit virtual domains from Operations Center itself. If the same virtual domain is active in multiple instances, Operations Center displays the virtual domain once, with data aggregated from all the active virtual domains with the same name on all the managed instances.

You can create virtual domain only if an instance is present or it is in reachable state. The Number of network elements in Virtual Domains is limited when compared to that of , since the Virtual Domain shows only

managed network elements. You can assign device groups to virtual domain and also choose the instances to which you want to distribute the virtual domain using Operations Center.

Creating, editing, importing, and exporting virtual domains from within Operations Center works the same way as creating, editing, importing, and exporting virtual domains in a single instance of . For more details, see Using Virtual Domains to Control Access

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 352
View Devices Managed by All Servers Using Operations Center, on page 359
Manage Servers using Operations Center, on page 363
Distribute Virtual Domains to Servers, on page 361

Distribute Virtual Domains to Servers

In Operations Center, if you want to distribute the existing virtual domain to instances, follow these steps:

Step 1 Choose Administration > Users > Virtual Domains.

Step 2 From the Virtual Domains sidebar menu, click an existing virtual domain which you want to create in new instance.

Step 3 Click Managed Servers tab.

Step 4 Click Add and choose the manage instances for which you want to distribute the virtual domain.

Step 5 Click OK.

Step 6 Click Submit.

For more information see the chapter User Permissions and Device Access in Cisco Prime Infrastructure Administrator Guide.

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 352

Enable Operations Center RBAC Support

The Role Based Access Control (RBAC) support in Operations Center allows a collection of devices from multiple managed instances to be associated with a user via virtual domains. This feature enables to assign privileges such as accessing Monitor and Manage server page, adding, modifying or deleting managed instances, and populate certain dashlets, to a specific user.

Follow these steps to enable RBAC in the Operations Center:

Step 1 Log in to as an administrator.

Step 2 Choose Administration > Users > Users, Roles & AAA > User Groups.

Step 3 Click a group name to which RBAC is to be provided.

Step 4 Click Task Permissions tab.

Step 5 Check the following check boxes under Operations Center Tasks:

- Monitor and Manage Servers Page Access.
- Administrative Privileges under Manage and Monitor Server Pages.

These options are enabled by default for admin and super users.

Step 6 Click Save.

For more information refer the chapter User Access and Device Permisssions in Cisco Prime Infrastructure Administrator Guide.

Related Topics

Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 360

Share Device Configuration Templates Across Prime Infrastructure Servers Using Operations Center

Although it does not directly manage or configure any device in your network, Operations Center gives you access to the configuration templates stored on the server instances it manages. You can use Operations Center to:

- View the configuration templates on any of the servers.
- Distribute templates that exist on one server to any of the other servers Operations Center manages. Template distribution like this is required if (for example) you want to deploy a template across your entire network.

The steps for doing these tasks are identical to the ones you follow when you perform the same tasks on standalone servers. You simply need to log into the Operations Center instance first, and then select the server instance whose templates you want to work on.

View Configuration Templates Using Operations Center

You can view configuration templates on any managed instance by selecting the Configuration menu option in Operations Center and expanding the listing until you find the templates you want.

Step 1 Log in to Operations Center and choose Configuration > Templates > Features & Technologies.

Step 2 Expand the template category you want to view (for example, My Templates). Operations Center display a list of the managed instances with templates in that category.

Step 3 Expand the managed instance whose templates you want to view. Expand the template sub-categories as needed.

Deploy Configuration Templates Using Operations Center

Step 1 After you create a configuration template, click Deploy.
The Deployment wizard appears.

Step 2 Select the devices on which you want to deploy the template, then click Next to choose the input values.

Step 3 In the Input Values tab, you can toggle between Form and CLI view.

Step 4 After entering the necessary configuration values, click CLI to confirm the device and template configuration values.

Step 5 Click Next to view the job deployment summary.

Step 6 On the Deployment Summary tab, you can see the CLI view for each of the devices.

Step 7 Click Finish to deploy the template.

Distribute Configuration Templates Across Managed Servers

You can distribute any user-defined configuration template from one managed instance to another managed instance.

Distributing a template to another server instance occurs automatically when you deploy a template to a device on another such instance without first copying (distributing) that template to the other instance.

Step 1 Log in to Operations Center and choose Configuration > Templates > Features & Technologies.

Step 2 Expand the template category you want to view (for example, My Templates). Operations Center displays a list of the managed instances with templates in that category.

Step 3 Expand the managed instance whose templates you want to view. Expand the template sub-categories as needed.

Step 4 (optional) If you want to edit the template before distribution, do the following:

a) Click Add Variable and choose the template variable.
b) Click the edit icon and make the necessary changes.
c) Click Save.

Step 5 When you see the template you want to distribute, click on it to select it. Operations Center displays details for the selected template.

Step 6 Click Distribute. Operations Center displays a list of all the server instances that it manages and that are currently reachable.

Step 7 Select the checkbox next to each server instance to which you want to distribute the template.

Step 8 Check the Overwrite template with the same name check box and then click OK.

If you uncheck the Overwrite template with the same name check box and if the template already exists on the other server, Operations Center will not distribute the template and will alert you to check the Overwrite template with the same name check box.

Manage Servers using Operations Center

Select Monitor > Monitoring Tools > Manage and Monitor Servers to open the Manage and Monitor Servers page. From here, you can:

- Add new servers (up to the license limit).
- Edit, delete, activate, and deactivate current servers.
- View each servers reachability, CPU utilization, memory utilization, software update status and secondary server details (if it is configured), summary of purchased licenses and utilized licenses, and alarms generated for the instances.
- Determine whether any servers are down.
- View alarms and events.
- Cross-launch into individual instances.
- See if any backup servers are running. Administrators can use the High Availability (HA) framework to configure a backup server to automatically come online and take over operations for the associated primary server when it goes down. For more information on HA framework, see “Configure High

Availability" in Related Topics. Administrators should be sure to follow the restrictions on use of HA with Operations Center given in "Before You Begin Setting Up High Availability".

Aside from a server's reachability status, there are three server metrics you should focus on:

- CPU utilization
- Memory utilization.

If a server has a network latency figure that exceeds one second, or it has a CPU or memory utilization percentage greater than 80%, the chances are good that an issue exists with that server.

If a server's status is listed as "unreachable", a "?" icon will appear next to the reachability status message. Hover your mouse cursor over the icon to see a popup message giving possible causes for the server's status (for example, server cannot be pinged, API response (latency) is too slow and SSO is not setup properly).

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 352
Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 360
View the Status of Multiple Servers using Operations Center, on page 364

View the Status of Multiple Servers using Operations Center

Use the Server Status Summary to view the current status of your servers without leaving the dashboard or page you have open. To open it, place your cursor over any portion of the Server Status area at the top of the Operations Center's main page. From here, you can quickly determine if any of your servers are currently down. You can also launch a separate instance for the selected server.

You can also quickly view the reachability history for any server managed by Operations Center.

Step 1 Select Monitor > Monitoring Tools > Manage and Monitor Servers. Operations Center displays the list of servers it manages.

Step 2 Select one of the managed servers. The page displays summary status for that server.

Step 3 Click the Reachability History tab at the bottom of the page. Operations Center displays a list of recent changes in reachability for the selected server.

Step 4 If want to clear the reachability history, click Clear History and click Yes in the pop-up window.

Related Topics

Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 352

Activate Operation Center using Smart Licensing

Smart Licensing is a cloud-based, software license management solution that enables you to automate time-consuming, manual licensing tasks. The solution allows you to easily track the status of your license and software usage trends.

Smart Licensing helps simplify three core functions:

- Purchasing: The software that you have installed in your network can automatically self-register themselves, without Product Activation Keys (PAKs).

- Management: You can automatically track activations against your license entitlements. Additionally, there is no need to install the license file on every node.
- Reporting: Through the portal, Smart Licensing offers an integrated view of the licenses you have purchased and what has been actually deployed in your network. You can use this data to make better purchase decisions, based on your consumption.

To select smart software licenses, see Choose Smart Software Licenses section in Cisco Prime Infrastructure Administrator Guide.

Distribute Software Updates to Prime Infrastructure Instances Managed by Operations Center

Operation Center allows you to distribute software updates to multiple Prime Infrastructure instances.

To distribute a software update:

Step 1 Go to Administration > Licenses and Software Updates > Software Update.

Step 2 Click Prime Infrastructure tab and click upload link. In the Upload Update dialog, click the Upload from local computer or Copy from server's local disk radio button as required.

Step 3 Click Browse to choose the dowloaded patch file from the save location and click Ok.

Step 4 Click Distribute to distribute the patch file to Prime Infrastructure servers.

Note You may now choose to distribute the patch file from Prime Infrastructure Operations Center to Prime Infrastructure's Secondary Server. Please note that installing patches on paired High Availability servers is not allowed. For more information, refer How to Patch Paired HA Servers section in the Cisco Prime Infrastructure Administrator Guide.

Step 5 Choose the required Prime Infrastructure servers from the list of servers and click Ok. Update success popup message appears.

Step 6 Select the Prime infrastructure tab and click the Install button to install the updates in Prime Infrastructure instances.

Step 7 You can view the status of the updates in Status of Updates section.

Note You can distribute the software update to any number of available Prime Infrastructure servers using Distribute button in Prime Infrastructure tab. To know more on Software Updates, see Licensens and Software Updates chapter in Cisco Prime Infrastructure Administrator Guide.

View Alarms on Devices Managed by Multiple Servers Using Operations Center

Select Monitor > Monitoring Tools > Alarms and Events to open the Alarms and Events page. From here, you can view a comprehensive listing of your network's alarms, events, and syslog messages. With one or multiple alarms selected, you can also determine whether those alarms have been acknowledged, add a note that describes them in more detail, or delete them from the page.

The Alarm Summary displays an aggregated count of critical, major, and minor alarms from the managed instances.

To refine the alarms, events, and syslog messages displayed here, do one of the following:

- From the Device Group pane, select the desired device type, location, or user-defined group.
- Apply a custom filter or select one of the predefined filters from the Show drop-down list. For details on how to use filters, see the related topic “Quick Filters”.
- Search for a particular alarm or event. For details, see the related topic “Search Methods”.
- Hover your cursor on the Alarm Browser screen to display the aggregated count of alarms for the managed instances. You can also acknowledge, annotate, and delete alarms; that action is duplicated on the respective instance.

Related Topics

Quick Filters, on page 867
Search Methods, on page 877
Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 352
View Clients and Users Managed by Multiple Servers Using Operations Center, on page 366

View Clients and Users Managed by Multiple Servers Using Operations Center

Select Monitor > Monitoring Tools > Clients and Users to open the Clients and Users page, which contains the aggregated clients of all managed instances. From here, you can view information for the clients configured on your network, such as a client’s MAC address, the user associated with the client, and the name of the device that hosts the client. You can choose a client or user and view the client association history and the statistical information. You can also launch the 360° Degree View to get more information about the device and the associated clients.

To refine the list of clients displayed here, do one of the following:

- Apply a custom filter or select one of the predefined filters from the Show drop-down list. For details on how to use filters, see the related topic “Quick Filters”.
- Search for a particular client. For details, see the related topic “Search Methods”.

Related Topics

Quick Filters, on page 867
Search Methods, on page 877
Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 352

Run Reports on Deployments with Multiple Servers Using Operations Center

In addition to the Operations Center dashboards and monitor pages, Operations Center provides a subset of reports that combine network management and performance data across all the managed instances of . If you are using Operations Center to segment and rationalize your management of a global network, these specialized versions of the standard reports can help get a closer look at your network as a whole, help you monitor health across the globe, and troubleshoot emergent issues.

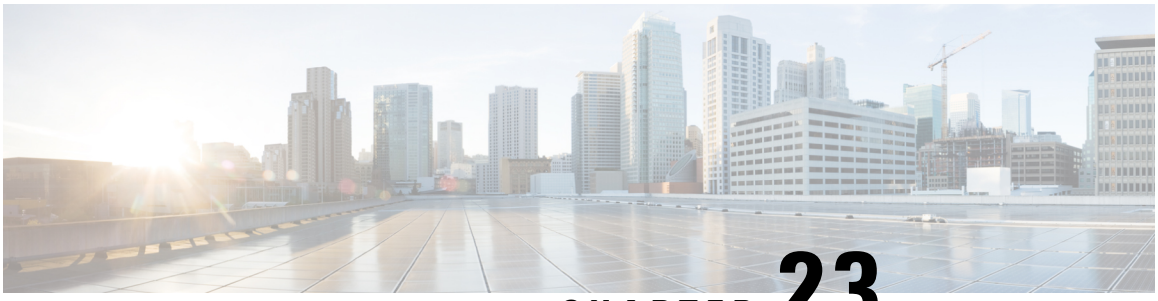
The Operations Center reports contain aggregated data from all of the managed instances. If you want to restrict this aggregation to a subset of the managed instances, the best ways to do this are to:

- Temporarily deactivate those managed instances whose data you do not want included in the aggregated Operations Center report data. You can do this by selecting Monitor > Monitoring Tools > Manage and Monitor Servers and choosing to deactivate the servers you want to ignore.
- Use virtual domains to restrict the data the instances in which you are interested. For details, see “Use Virtual Domains on Deployments with Multiple Prime Infrastructure Servers Using Operations Center” in Related Topics.

Except for aggregating data across managed instances, Operations Center reports generation works the same way as in . For more information about reports and how to generate them, see "Create, Schedule, and Run a New Report" in Related Topics.

Related Topics

Create, Schedule, and Run a New Report
Use the Operations Center Config Dashboard to Manage Multiple Servers, on page 352
Use Virtual Domains on Deployments with Multiple Servers Using Operations Center, on page 360
View Alarms on Devices Managed by Multiple Servers Using Operations Center, on page 365
View Clients and Users Managed by Multiple Servers Using Operations Center, on page 366
FAQs: Operations Center and Prime Infrastructure, on page 905



CHAPTER 23

Advanced Monitoring

What are the Data Sources Used by Site Dashlets

Cisco Prime Infrastructure consumes a lot of information from various different sources, including NAM, NetFlow, NBAR, Cisco Medianet, PerfMon, and Performance Agent. The following table depicts the sources of the data for the site dashlets used by Prime Infrastructure:

Table 43: Site Dashlet Data Sources

Dashlet Name	NAM	Cisco Medianet	NetFlow	PA	NBAR2
Application Usage Summary	y	y	y	y	y
Top N Application Groups	y	y	y	y	y
Top N Applications	y	y	y	y	y
Top N Applications with Most Alarms	y	y	y	y	y
Top N Clients (In and Out)	y	y	y	y	y
Top N VLANs	y	_	y	y	_
Worst N RTP Streams by Packet Loss	y	y	_	_	_
Worst N Clients by Transaction Time	y	_	_	y	_

The following table shows how Prime Infrastructure populates the application-specific dashlets:

Table 44: Application-Specific Dashlet Data Sources

Dashlet Name	NAM	Cisco Medianet	NetFlow	PA	NBAR2
Application Configuration	y	y	y	y	y

Dashlet Name	NAM	Cisco Medianet	NetFlow	PA	NBAR2
Application ART Analysis	y	_	_	y	_
App Server Performance	y	_	_	y	_
Application Traffic Analysis	y	y	_	y	y
Top N Clients (In and Out)	y	_	_	y	_
Worst N Clients by Transaction Time	y	_	_	y	_
Worst N Sites by Transaction Time	y	_	_	y	_
KPI Metric Comparison	y	y	_	y	_
DSCP Classification	y	_	y	_	_
Number of Clients Over Time	y	_	y	_	_
Top Application Traffic Over Time	y	_	y	_	_
Top N Applications	y	_	y	y	_
Top N Clients (In and Out)	y	_	y	y	_
Average Packet Loss	y	y	_	_	_
Client Conversations	y	_	y	_	_
Client Traffic	y	_	y	_	_
IP Traffic Classification	y	_	y	_	_
Top N Applications	y	_	y	_	_
DSCP Classification	y	_	y	_	_
RTP Conversations Details	y	y	_	_	_
Top N RTP Streams	y	y	_	_	_
Voice Call Statistics	Y	_	_	_	_
Worst N RTP Streams by Jitters	y	y	_	_	_
Worst N RTP Streams by MOS	y	_	_	_	_
Worst N Sites by MOS	y	_	_	_	_
Worst N Site to Site Connections by KPI	y	y	_	y	_

Related Topics

- Enabling Medianet NetFlow
- Enabling NetFlow and Flexible NetFlow

Enable WAN Optimization

Cisco Wide Area Application Services (WAAS) devices and software help you to ensure high-quality WAN end-user experiences across applications at multiple sites. For various scenarios for deploying WAAS in your network, see Using Cisco NAM Hardware in a WAAS Deployment .

After you have deployed your WAAS changes at candidate sites, you can navigate to Dashboards > Performance > WAN Optimization to validate the return on your optimization investment. From this dashboard, you can click View Multi-Segment Analysis to monitor WAAS-optimized WAN traffic. From the Multi-Segment Analysis display, you can select the:

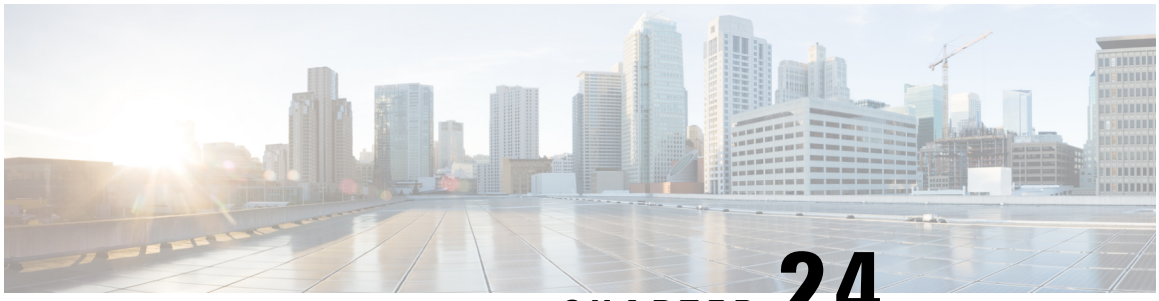
- Conversations tab to see individual client/server sessions.
- Site to Site tab to see aggregated site traffic.

The following table describes the key WAAS monitoring dashlets.

Table 45: Key WAAS Monitoring Dashlets

Dashlet	Description
Average Concurrent Connections (Optimized versus Pass-through)	Graphs the average number of concurrent client and pass-through connections over a specified time period.
Multi-segment Analysis	Displays WAAS traffic across multiple segments in a conversation or between sites.
Multi-segment Network Time (Client LAN-WAN - Server LAN)	Graphs the network time between the multiple segments.
Transaction Time (Client Experience)	Graphs average client transaction times (in milliseconds) for the past 24 hours, with separate lines for optimized traffic and pass-through traffic (in which optimization is disabled). With optimization enabled, you should see a drop in the optimized traffic time when compared to the pass-through time.
Traffic Volume and Compression Ratio	Graphs the bandwidth reduction ratio between the number of bytes before compression and the number of bytes after compression.

Note that you cannot access Multi-Segment Analysis unless you have purchased and applied Prime Infrastructure Assurance licenses. The WAAS monitoring dashlets will display no data unless you have implemented WAAS at candidate sites.



CHAPTER 24

Manage Reports

This chapter contains the following topics:

Reports Overview

reports provide information about system and network health as well as fault information. You can customize and schedule reports to run on a regular basis. Reports can present data in a tabular, or graphical format (or a mixture of these formats). You can also save reports in CSV or PDF format. The CSV or PDF files can be saved on the server for later download, or sent to an e-mail address.

provide the following type of data:

- Current—Provides a snapshot of data that is not time-dependent.
- Historical—Periodically retrieves data from the device and stores it in the database.
- Trend—Generates a report using aggregated data, which is collected and summarized as minimums, maximums, and averages.

With , you can filter these reports based on a specific criteria. You can also export reports, sort reports into logical groups, and archive reports for long-term storage.

Create, Schedule, and Run a New Report

The Report Launch Pad provides access to all reports from a single page. From this page, you can perform all report operations: Create, save, view, schedule, and customize.

To see more report details, hover the cursor over the tooltip next to the report type.

To create, schedule, and run a new report:

Step 1 From the left sidebar, choose Reports > Report Launch Pad.

Step 2 Locate the report you want to launch, then click New.

A new text box, Last, is added as part of the Reporting Period field which allows users to generate reports for the last 24 hours.

Note You must enter a value between 1 to 24, i.e. for the last 24 hours.

Step 3 In the Report Details page, enter the report title.

You can edit the Report Title field.

Step 4 Choose the appropriate Report By category from the drop down list.

Step 5 The Report Criteria field allows you to sort your results depending on the previous Report By selection made.

Note If you select the virtual domain checkbox at the top, edit button is enabled when one or more values present in the report criteria filter.

Step 6 Click Edit to open the device selection wizard and select the required device. Click on Preview tab to confirm the selected devices and click Ok. You can also remove the selected devices.

The parameters shown in the Report Details page depend on the report type you chose. With some reports, you are required to customize the report results. For more information about how to customize a report result, see Customize Report Results, on page 378.

Note In Client reports, SSIDs are listed only if their Wireless LAN Controllers are mapped to a Virtual Domain.

Step 7 If you plan to run this report later or as a recurring report, enter the required Schedule parameters.

Step 8 To run the report, choose one of the following options:

- Run—Runs the report without saving the report setup.
- Save—Saves this report setup without immediately running the report. If you have entered Schedule parameters, the report runs automatically at the scheduled date and time.
- Run and Save—Saves this report setup and runs the report immediately.
- Save and Export—Saves the report, runs it, and exports the results to a file. You will be prompted to:
  - Select the exported report's file format (CSV or PDF). Exported CSV file is a single .csv file which has capability to hold one million records. If the number of records exceeds one million, then another CSV file will be generated accomodating the remaining records. Finally, both the CSV files will be provided in zip format.

    Note Above mentioned condition is applicable only for the reports listed under Reports Launchpad which is called as simple reports, while the custom reports will not have this conditional check.

  - Choose whether to send an email when the report has been generated. If you choose this option, you must enter the destination email address and the email subject line content, and choose whether you want the exported file included as an attachment to the email.

  When you are finished, click OK.

- Save and Email—Saves the report, runs it, exports the results as a file, and emails the file. You will be prompted to:
  - Select the exported report file format.

- Enter the destination email address and the email subject line content.

  Note In Prime Infrastructure 3.8, selecting the Export Format as CSV and clicking the Save and Email option will send the CSV file in the zip format, if the file holds more than 15k records. A file with less than 15k records will be sent as a plain CSV file.

When you are finished, click OK.

- Cancel—Returns to the previous page without running or saving this report.

Combine Reports in

Two or more reports can be combined and information can be filtered based on requirements. Users can select multiple reports and combine them instead of creating special reports for different scenarios. Composite reports can be created from a pre-defined list of supported reports.

To create a new composite report:

Step 1 Choose Reports > Reports Launch Pad. You can create a new report in one of the following ways:

a) From the left sidebar menu, choose Composite > Compostie Report and then click New.

b) On the Report Launch Pad page, scroll down to view the Composite section, then click New.

Step 2 In the New Custom Composite Report page, enter the report title.

A new text box, Last, is added as part of the Reporting Period field which allows users to generate reports for the last 24 hours.

Note You must enter the value in hours.

Step 3 From the Report Category drop-down list, choose a category.

Step 4 Select the required reports from the available list and add them to the Selected Reports text box. You can also remove the selected reports.

Step 5 Choose the appropriate Report By category from the drop-down list. The categories differ for each report.

Step 6 The Report Criteria field allows you to sort your results depending on the previous Report By selection made. Click Edit to open the Filter Criteria page and select the required filter criteria.

Step 7 If you plan to run this report later or as a recurring report, enter the Schedule parameters given in the Schedule section.

Step 8 To run the report, choose one of the following options:

- Run—Click to run the report without saving the report setup.
- Save—Click to save the report setup without immediately running the report. If you have entered the Schedule parameters, the report runs at the scheduled date and time.
- Run and Save—Click to save the report setup and run the report immediately.
- Save and Export—Click to save the report, run it, and export the results to a file or as an email attachment. For this you need to:
  - Choose the exported report file format (CSV or PDF).
  - Check the first check box if you want to send an email when the report has been generated. You must enter the destination email address and email subject line content.

- Check the second check box if you want the exported file to be included as an attachment in the email.

Click OK.

- Save and Email—Click to save the report, run it, export the results as a file, and email the file. You will be prompted to:
  - Choose the exported report file format.

    Note File size limitation for sending mail will always dependent on users SMTP server.

  - Enter the destination email address and email subject line content.

  Note In Prime Infrastructure 3.8, selecting the Export Format as CSV and clicking the Save and Email option will send the CSV file in the zip format, if the file holds more than 15k records. A file with less than 15k records will be sent as a plain CSV file.

Click OK.

- Cancel—Click to return to the previous page without running or saving the report.

You can access the saved composite reports from the Saved Reports Template.

Create Custom Reports

Custom Reports feature is not supported in Operations-Center environment.

Step 1 Choose Reports > Custom Reports

Step 2 Enter Report title in the custom reports page.

Step 3 Drag and Drop the required reports from the Available Options pane to the Selected Options pane.

Step 4 Choose the reporting period from Reporting Period drop down list or from Select date range.

A new text box, Last, is added as part of the Reporting Period field which allows users to generate reports for the last 24 hours.

Note You must enter the value in hours.

Step 5 Choose the Summary View or Detailed View as required.

- Summary view
  - When you run the report - Displays the top 10 records per tabular subreports.
  - When you export the report as CSV/PDF - Displays the top 20 records per tabular subreports.
- Detailed view
  - When you run the report - Displays up to top 1000 records per tabular subreports, where each table is paginated on the screen.
  - When you export the report as PDF - Displays up to 1000 records per tabular subreports.

- When you export the report as CSV - Displays all records per tabular subreports.

Note The above stated views effects only the tabular data.

Step 6 Enter the Report Criteria. This field allows you to enter the details based on the selected reports.

Step 7 Click Edit to open the Filter Criteria page and select the required filter criteria.

Step 8 Click Edit Sub Reports and select the sub reports. Each sub reports will be loaded with different values based on the report criteria to customize the report.

Step 9 You can Enable or Disable the Sub reports for the combination of reports known as composite reports.

Step 10 Once you enable the sub report, select the sub report values. User can customize each subreport by selecting the attribute to be diplayed on the tabular report and the fields based on which the tabular subreports need to be sorted as either ascending or descending order. To re-order the attributes by dragging and dropping them to a specific location.

Step 11 Click Apply and Run report. The selected field values are displayed in the table once you generate the report summary.

Step 12 If you disable the sub report, the remaining sub reports for other report criteria were displayed in the table with the default field values in the report summary.

Step 13 If you plan to run this report later or as a recurring report, click the Schedule Report tab and set the following parameters.

- Drag the slider to turn on Scheduling.
- Select the Export Format as CSV or PDF.
- Select the Destination as File or Email. Enter the email id, if you choose Email as destination.
- Choose the Start/Date time.
- Select the appropriate Recurrence Option.

Step 14 To run the report, choose one of the following options.

- Run—Runs the report without saving the report setup.
- Save—Saves this report setup without immediately running the report. If you have entered Schedule parameters, the report runs automatically at the scheduled date and time.
- Run and Save— Click to save this report setup and run the report immediately.
- Save and Export—Click to save the report, runs it, and exports the results to a file. You will be prompted to:
  - Select the file format (CSV or PDF) of the exported report.
  - Choose whether to send an email when the report is generated. If you choose this option, you must enter the destination email address and the email subject line content, and choose whether you want the exported file included as an attachment to the email.
  - Click OK. If the CSV file fails to open correctly, make sure you specify a comma as the List Separator in one of the following locations:
    - Control Panel > Region/Language/Region and Language >Formats > Additional Settings
    - In Excel: File > Options > Advanced > Use System Separators.
- Save and Email—Click to save the report, run it, export the results as a file, and email the file. You will be prompted to:
  - Select the exported report file format.

Note File size limitation for sending mail will always dependent on users SMTP server.

- Enter the destination email address and the email subject line content.

  Note In Prime Infrastructure 3.8, selecting the Export Format as CSV and clicking the Save and Email option will send the CSV file in the zip format, if the file holds more than 15k records. A file with less than 15k records will be sent as a plain CSV file.

- Click OK.

- Cancel—Click to return to the previous page without running or saving this report.

Step 15 Custom Chart Options - Once the report is generated, the View Report tab is enabled automatically and report output is displayed. The subreports generated as charts which has the small chart icon in the top left of each charts. Click on the smart chart icon, which allows you to plot different customized visualizations of charts such as Pie chart, Bar chart, Line Chart etc, on the data.

Note These custom charts are applicable only for on screen mode (on the live interactive mode) and not on save reports and export reports actions.

Step 16 Choose Administration > Dashboards > Job Dashboard > User Jobs.

Step 17 Click Report Status to view the status of the job.

Step 18 Click the report name to view the last five job instances. However, you will not be able to perform any actions available under Edit and Job Series drop-down lists.

If a report has been saved for a specific report type, you can access the current reports from the Report Launch Pad. You cannot change or update generated reports for all sub domains at the same time. You can open and change the reports individually through their respective sub domains. To update all reports, delete the reports created on sub domains and regenerate virtual domain reports with the changes. If you upgrade the Prime Infrastructure server to a higher version, you must delete and recreate the reports that were already modified and saved in the older version.

Customize Report Results

Many reports allow you to customize their results, letting you include or exclude different types of information. Reports that support this feature display a Customize button. Click this button to access the Create Custom Report page and customize the report results.

To customize a report result:

Step 1 Choose the report you want to customize:

a) Create a new report. Click Reports > Report Launch Pad.
b) Customize a recurring report. Click Reports > Saved Report Templates and, then click the report name hyperlink.

Step 2 In the Report Details page, click Customize.

Step 3 On the Create Custom Report page, complete the required information, then click Apply to confirm the changes.

Step 4 Click Save in the Report Details page.

Scheduled Reports in

The scheduled report tasks are not visible outside the Virtual Domain they run in. The results of the scheduled report tasks are visible in the Reports Run Results page of the respective domains.

The list of scheduled runs can be orted by report category, report type, time frame, and report generation method.

For information about the fields on this page, see the Scheduled Run Results page in Field Reference for Cisco Prime Infrastructure Reports.

Saved Report Templates

Saved report templates are available at Reports > Saved Report Templates. From the Saved Report Templates page, you can create report templates and manage saved report templates. You can also enable, disable, delete, copy or run saved reports, and you can filter and sort report templates by category, type, and status. . For information about the fields on the Saved Report Templates page and filtering saved report templates, see Field Reference for Cisco Prime Infrastructure Reports.

The Saved Report Templates page displays the following information:

- Report Title—Identifies the user-assigned report name.

Click the report title to view the details for this report.

- Report Type—Identifies the specific report type.
- Scheduled—Indicates whether this report is enabled or disabled.
- Virtual Domain—Identifies the name of the virtual domain under which this report is scheduled.
- Run Now—Click the run icon to immediately run the current report.

Note Post the Prime Infrastructure version upgrade to 3.8, if you wish to run any of the saved reports that has column level updates, you must save the report details once and then click the Run button. This is recommended to avoid missing the progressions done by the owner/proprietor to the report.

When you execute any domain based report for a sub virtual domain, the report displays all of the device attributes that are mapped to the virtual domain where you are currently logged-in.

Select a report from the Saved Report Templates and click the Copy button to create a replica of that particular report.

Note You can only create a replication of simple reports and not the custom, composite, and expired reports.

Prime Infrastructure Report Data Retention Periods

The report shows hourly, daily or weekly data depending on the data retention period configured by choosing Administration > Settings > System Settings > Data Retention. The data is retrieved from the database based on the following conditions.

If the period is:

1. Up to last 1 day, the data is fetched from raw table.
2. From last 2 days to 4 weeks, the data is fetched from a hourly aggregated table.
3. From previous month calendar to last 12 week, the data is fetched from daily aggregated table.
4. From last 6 months to last 1 year, the data is fetched from a weekly aggregated table.

The valid range for performance data retention period is:

1. Short term Data Retain Period:1 to 31 days.
2. Long term Data Retain Period: 2 to 756 days.
3. Medium term Data Retain Period: 7 to365 days.
4. Hourly Data Retain Period: Valid Range: is 1 to 31 hours.
5. Daily Data Retain Period: 7 to 365 hours.
6. Weekly Data Retain Period: 2 to 108 hours.

Click Advanced Settings option to edit age and max records for each table. While saving, both age and max records values will be saved in the database. During the next data clean up job execution, pruning will happen based on either by age or max records whichever limit is reached first.

For detailed information about Prime Infrastructure reports, see Field Reference for Cisco Prime Infrastructure Reports.

PART V

Configure Devices

CHAPTER 25

Create Templates to Automate Device Configuration Changes

This chapter contains the following topics:

Why Create New Configuration Templates?

provides a number of out-of-the-box configuration templates that you can use to make changes on your network devices. Those are described in .

If you have sufficient privileges, you can also create new templates that meet the exact needs of your environment, and then make those templates available for others to use. You can make the templates as simple or as complex as needed, including grouping multiple templates together into a composite template. Finally, you can associate templates with particular devices by creating configuration groups.

provides out-of-the-box CLI commands that you can use in your templates. It also provides a blank CLI template you can use to create new CLI commands. You can use them singly or with other commands in a composite template.

How you use configuration templates can depend on factors such as how large your network is, the number of designers in your organization, and how much variation there is among devices configuration. For example:

- For a small network with only one or two designers and a limited number of device configurations, start by copying the CLI configurations you know are “good” into a set of templates. You could then combine them into composite templates and make them available to your operators.
- For a large network with many different device configurations, try to identify the configurations you can standardize. This lets you control the amount of exceptions to these standards, and lets you turn features on and off as needed.

Ways to Create Configuration Templates Using Prime Infrastructure

Cisco Prime Infrastructure provides the following types of feature-level configuration templates:

- Features and technologies templates—Configurations that are specific to a feature or technology in a device configuration.
- CLI templates—User-defined templates that are created based on your own parameters. CLI templates allow you to choose the elements in the configurations. Prime Infrastructure provides variables that you replace with actual values and logic statements. You can also import templates from the Cisco Prime LAN Management System.
- Composite templates—Two or more feature or CLI templates grouped together into one template. You specify the order in which the templates contained in the composite template are deployed to devices

Related Topics

Create a New CLI Configuration Template Using a Blank Template, on page 386
Create a New Composite Template, on page 391
Create a New Features and Technologies Template Using an Existing Template, on page 385

Create a New Features and Technologies Template Using an Existing Template

Features and Technologies templates are templates that are based on device configuration and that focus on specific features or technologies in a device's configuration.

When you add a device to , gathers the device configuration for the model you added. does not support every configurable option for all device types. If does not have a Features and Technologies template for the specific feature or parameter that you want to configure, create a CLI template.

Features and Technologies templates simplify the deployment of configuration changes. For example, you can create an SNMP Features and Technologies template and then quickly apply it to devices you specify. You can also add this SNMP template to a composite template. Then later, when you update the SNMP template, the composite template in which the SNMP template is contained automatically has your latest changes.

To create Features and Templates, follow these steps:

Step 1 Choose Configuration > Templates > Features and Technologies.

Step 2 In the Features and Technologies menu on the left, choose a template type to create.

Step 3 Complete the fields for that template.

If you are creating a feature template that applies only to a particular device type, the Device Type field lists only the applicable device type, and you cannot change the selection. Specifying a device type helps you to prevent a mismatch; that is, you cannot create a configuration and apply the configuration to a wrong device.

Step 4 Click Save as New Template. After you save the template, apply it to your devices.

Step 5 To verify the status of a template deployment, choose Administration > Dashboard > Jobs Dashboard.

To modify the deployment parameters for any subsequent configuration template deployments, select a configuration job, then click Edit Schedule.

Related Topics

Deployment Flow for Configuration Group Using the Wizard, on page 393

Prerequisites for Creating CLI Templates

Before you create a CLI template, you must:

- Have expert knowledge and understanding of the CLI and be able to write the CLI in Apache VTL.
- Understand to what devices the CLI you create can be applied.
- Understand the data types supported by .
- Understand and be able to manually label configurations in the template.

Create a New CLI Configuration Template Using a Blank Template

Use templates to define a set of reusable device configuration commands. A description of CLI templates and how you can use them is displayed in the web GUI when you choose Configuration > Templates > Features & Technologies, then choose CLI Templates.

If you want to edit a template that is provided with , make a copy of the template, give it a new name, and then edit it. See Create a New CLI Configuration Template Using An Existing Template, on page 386.

Templates that you create are stored under My Templates.

Step 1 Choose Configuration > Templates > Features & Technologies.

Step 2 Expand CLI Templates, then choose CLI.

Step 3 Complete the required fields in Templates Basic area.

Step 4 Click the Ports radio button, if you want to apply the template to a set of selected interfaces across selected devices The template will be tagged as port based template.

Step 5 In the Template Detail area, configure the following:

- Click the Add Variable tab. This allows you to specify a variable for which you will define a value when you apply the template. Click Add Row and enter the parameters for the new variable, then click Save.

  or

  Search for the global variable in the Add Global Variable search box by entering the first few characters of the global variable name and choose the desired global variable you want to apply

- Enter the CLI information. In the CLI tab, you must enter code using Apache VTL. See Apache Velocity Language Template Guide.
- Click Form View (a read-only view) to view the variables.

Step 6 Save your template. Click Save as New Template, specify the folder (in My Templates) in which you want to save the template, then click Save.

Related Topics

Deployment Flow for CLI Templates using the Wizard, on page 394
Data Types, on page 388
Manage Database Variables in CLI Templates, on page 389

Create a New CLI Configuration Template Using An Existing Template

The easiest way to create a new configuration template is to find a similar existing template, copy it, and edit it. You can also use this procedure to edit templates that you created. (You can only edit templates that you create.)

Step 1 Choose Configuration > Templates > Features & Technologies.

Step 2 Expand CLI Templates, then choose System Templates - CLI.

Step 3 In the Template navigation panel on the left , locate the template you want to copy, hover your mouse cursor over the i icon that is displayed next to the template name, then click Duplicate in the popup window.

Step 4 In the Duplicate Template Creation dialog, specify a name and the folder (under My Templates) where you want the new template to be saved, and click OK.

For example, if you copy a template that resides under CLI Templates > System Templates - CLI, by default the template is saved under My Templates > CLI Templates > System Templates - CLI (User Defined) .

Step 5 Add the validation criteria and CLI content as described in .

Example: Updating Passwords Using a CLI Template

The devices in these regions must have an assigned location attribute.

Step 1 If the four groups, North Region, South Region, East Region, and West Region, have not been created:

a) Choose Inventory > Device Management > Network Devices(gear icon) then hover your mouse cursor over User Defined and click Add SubGroup.

b) In the Create Sub-Group area, enter:

- Group Name: North Region
- Group Description: List of devices in the north region
- Filter: Location > Contains > SJC-N

  To determine the location of a device, choose Inventory > Device Management > Network Devices(gear icon) > Columns > Location.

The devices for the new group appear under Device Work Center > User Defined > North.

c) Do the same for south, east, and west regions.

Step 2 To deploy the password template:

a) Choose Configuration > Templates > Features and Technologies > CLI Templates > System Templates-CLI.

b) Select the Enable Password-IOS template and click Deploy.

c) In the Device Selection area, open the User Defined groups and select the North Region and South Region groups.

d) In the Value Selection area, enter and confirm the new enable password, then click Apply.

e) In the Schedule area, enter a name for the job, the date and time to apply the new template (or click Now), then click OK.

Step 3 After the job has run, choose Administration > Dashboards > Job Dashboard to view the status of the job.

Entering Variables in a Template

These topics provide information that will help you when entering variables into a template:

Data Types

Table 1 lists data types that you can configure in the Manage Variables page.

Data Type	Description
String	Enables you to create a text box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
Integer	Enables you to create a text box that accepts only numeric value. If you want to specify a range for the integer, expand the row and configure the Range From and To fields. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
DB	Enables you to specify a database type. See the Manage Database Variables in CLI Templates, on page 389.
IPv4 Address	Enables you to create a text box that accepts only IPv4 addresses for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
Drop-down	Enables you to create a list for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field (with a comma-separated value for multiple lists which appears in the UI).
Check box	Enables you to create a check box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field.
Radio Button	Enables you to create a radio button for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field.
Text Area	Enables you to create a text area which allows multiline values for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.

Manage Database Variables in CLI Templates

You can use database (DB) variables for the following reasons:

- DB variables are one of the data types in CLI templates. You can use the DB variables to generate device-specific commands.
- DB variables are predefined variables. To view the list of predefined DB variables, see the CLITemplateDbVariablesQuery.properties file at the following location: folder/opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate.
- For example, SysObjectID, IPAddress, ProductSeries, ImageVersion are DB variables.When a device is added to , the complete details of the device is collected in the DB variables. That is, the OID of the devices is collected in SysObjectID, product series in ProductSeries, image versions of the device in ImageVersion, and so on.
- Using the data collected by the DB variables, accurate commands can be generated to the device.
- You can select the DB variable in the Type field (using the Managed Variables page). Expand the name field and fill in the default value field with any of the DB variables which you want to use.
- When a device is discovered and added to , you can use the database values that were gathered during the inventory collection to create CLI templates.

Note While it is possible to create a customized query using Enterprise JavaBeans Query Language (EJB QL), only advanced developers should attempt this. We recommend you use the variables defined in the CLITemplateDbVariablesQuery.properties file only.

Use Validation Expressions

The values that you define in the Validation Expression are validated with the associated component value. For example, if you enter a default value and a validation expression value in the design flow, this will be validated during the design flow. That is, if the default value does not match with the entered value in the validation expression, you will encounter a get error at the design flow.

Note The validation expression value works only for the string data type field.

For example, choose Configuration > Templates > Features and Technologies, then choose CLI Templates > CLI. In the Template Detail area, click the Add Variable tab to view the list of Variables. Click the Add plus sign (+) in the Add Variables tab to add a row to the CLI template. Choose String in the Type field, enter the remaining values, and click Save. From the list of variables, expand the details of this new variable and configure the regular expression, which will not allow a space in that text box. Enter the following expression in the Validation Expression field.

```
^[\S]+$
```

Default value (optional)—ncs

The value should match with regular expression in the validation expression field.

Save the template, and then select a device. Try to enter a space in the text field. You will encounter a regular expression error.

Add Multi-line Commands

To enter multi-line commands in the CLI Content area, use the following syntax:

```
<MLTCMD>First Line of Multiline Command
Second Line of Multiline Command
......
......
Last Line of Multiline Command</MLTCMD>
```

where:

- <MLTCMD> and </MLTCMD> tags are case-sensitive and must be entered as uppercase.
- The multi-line commands must be inserted between the <MLTCMD> and </MLTCMD> tags.
- The tag cannot be started with a space.
- The <MLTCMD> and </MLTCMD> tags cannot be used in a single line.

Example 1:

```
<MLTCMD>banner_motd Welcome to
Cisco. You are using
Multi-line commands.
</MLTCMD>
```

Example 2:

```
<MLTCMD>banner motd ~ ${message}
</MLTCMD>
```

where {message} is a multi-line input variable.

Restrictions for Using Multi-Line Banner Commands

does not support multi-line banner commands. You can use banner file xyz format as shown in the following example.

```
#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
(config)#parameter-map type webauth global
(config-params-parameter-map)# type webauth
(config-params-parameter-map)#banner file tftp://209.165.202.10/banner.txt
(config-params-parameter-map)#^Z
#more tftp://192.168.0.0/banner.txt
Disclaimer:
Usage of this wireless network is restricted to authorized users only.
Unauthorized access is strictly forbidden.
All accesses are logged and can be monitored.
#
```

Add Enable Mode Commands

Use this syntax to add enable mode commands to your CLI templates:

```
#MODE_ENABLE<<commands >>#MODE_END_ENABLE
```

Import and Export a CLI Configuration Template

These topics explain how to export and import configuration templates. Templates can be exported templates have an .xml file name; multiple templates are exported as a zip file.

- If you export multiple configuration templates, the .xml files are placed in a zip file with the prefix name Exported Templates.
- Single files are exported and imported as .xml files
- You can import multiple .xml files by selecting individual files or by importing a zip file.
- When you import CLI templates, the user-defined global variables that are part of the file are not imported automatically. You need to add these variables to the CLI template manually.

Step 1 Choose Configuration > Templates > Features & Technologies. > Templates > Features & Technologies.

Step 2 To export a configuration template:

a) Save the files at the desired location.

Step 3 To import a configuration template:

a) Under the CLI Templates folder, hover your mouse cursor over the "i" next to CLI.
b) Click Show All Templates, then click Import.
c) In the Import Templates dialog box, choose the My Templates folder where you want to import the templates, then click Select Templates and navigate to the file you want to import.
d) Confirm your choices, then click OK.

Create a New Composite Template

All out-of-the-box and user-created templates can be added to a single composite template, which aggregates all of the individual feature templates that you need. When you create a composite template, you can also specify the order in which member templates should be executed. You can use composite templates to make changes to single or groups of devices.

Step 1 Choose Configuration > Templates > Features & Technologies.

Step 2 Expand the Composite Templates folder and choose Composite Templates.

Step 3 In the Template Basic area, enter a name for the template.

Step 4 In the Template Detail area, choose the templates to include in the composite template. Using the arrows, place the templates in the in the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the interface template.

Step 5 Click Save as New Template. After you save the template, and apply it to your devices (see).

Create a Shortcut to Your Templates Using Tags

When you apply a tag to a template, the template is listed under the My Tags folder. Tagging a configuration template helps you:

- Search a template using the tag name in the search field
- Use the tagged template as a reference to configure more devices

To tag an existing template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies.

Step 2 Expand the My Templates folder and choose the template that you want to tag.

Step 3 Enter a tag name in the Tag as text box, then click Save.

Deploy Templates to Devices

These topics describe the ways you can deploy (run) groups of commands on devices using configuration templates:

- Create Configuration Groups for Deploying Templates to Groups of Devices
- Deployment Flow for Configuration Group Using the Wizard
- Deployment Flow for CLI Templates using the Wizard
- Deployment Flow for Composite Templates Using the Wizard
- Deploy Templates to Devices Without Using Configuration Groups

Create Configuration Groups for Deploying Templates to Groups of Devices

If you have devices that require the same configuration, you can create a configuration group that contains devices and templates that can be applied to those devices. Creating a configuration group allows you to quickly apply new templates without remembering to which devices the new templates should be deployed.

Composite templates allow you to group smaller templates together, but configuration groups specify the relationship between the templates and the groups of devices, and the order in which commands are executed.

Step 1 Choose Configuration > Templates > Configuration Groups.

Step 2 In the Configuration Group Basic area, enter a name.

Step 3 To display devices from which you can make selections, in the Template Selection area, add one or more templates by clicking Add and selecting the templates. This also populates the Device Type field.

Step 4 Add additional templates by clicking Add in the Template Selection area. You cannot choose templates that are mutually-exclusive; for example, you cannot choose Add-Host-Name-IOS and Add-Host-Name-IOS-XR.

Step 5 Select the devices on which you want to deploy the template, then click Next to choose the input option.

Step 6 In the Device Selection area, select the devices you want to add to the configuration group.

Step 7 If you have multiple templates, the order in which templates will be listed by selecting one and clicking the up or down arrow.

Step 8 Click Save as New Configuration Group.

Deployment Flow for Configuration Group Using the Wizard

Note This deployment flow is not applicable for Controller based templates.

Step 1 After you create a configuration group, click Deploy. The Template Deployment -Prepare and Schedule wizard page opens.

Step 2 In the Templates area, view the templates that are added in the configuration group.

Step 3 In the Deployed on Devices area and during creation of Configuration Group, view the devices that you have chosen during creation of configuration group.

Step 4 In the Value Assignment area, from the Select Template drop-down list, choose a CLI template and an appropriate device. You can view the device details on which the template is going to be deployed, CLI Preview details, and so on. Click Apply.

Step 5 (Optional) Schedule the deployment job in the Schedule area:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

  Failure Policy:

  - Ignore failure and continue—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  - Stop on failure—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
  - Copy Running Config to Startup—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
  - Archive Config after deploy—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 6 In the Summary area, view the summary of the deployment.

Step 7 Click OK to deploy the template.

Step 8 Click Job Status in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Deployment Flow for CLI Templates using the Wizard

Step 1 After creating the CLI template, click Deploy. The Deployment wizard page opens.

Step 2 Select the devices on which you want to deploy the template from the Add devices table. The selected devices appear in the Devices to deploy table.

Step 3 Select the mode in which you want to deploy the template. The options are Work Flow and Export/Import CSV.

Step 4 Click the Work Flow option and click Next. See Step 6 .

Step 5 Alternately, click Export/Import CSV option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.

a) Uncheck the Do you want Optional Parameters check box, if you want to skip the optional fields while filling the configuration values in the CSV file.
b) Click Export CSV to download the CSV template to your local system.
c) Enter the configuration values for each specific device in the downloaded CSV template.
d) Click Import CSV to upload the updated CSV file.The input values automatically gets updated.
e) Click Next to input values.

Step 6 In the Input Values tab, you can toggle between Form and CLI view. Configure the following in the Input Values tab:

a) Enter all the mandatory fields for each template, then click Apply.

If the validation is successful, then the border of the circle around the selected template changes to green.

Note The successful validation message means that the change has been applied only to the selected devices in the workflow. To complete the configuration, perform the remaining steps in the procedure.

Step 7 After entering the necessary configuration values, click Next or CLI to confirm the device and template configuration values.

Step 8 Schedule the deployment job using Schedule Deployment tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

  Failure Policy:

  - Ignore failure and continue—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  - Stop on failure—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.

- Copy Running Config to Startup—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
- Archive Config after deploy—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 9 Click Next to view the job deployment summary.

Step 10 On the Deployment Summary tab, you will see the CLI view for each of the device.

Step 11 Click Finish to deploy the template.

Step 12 Click Job Status in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Note The SG220 device does not support any of the configuration template deployments whereas the SG300 and SG500 devices support CLI template deployment. However, both the SG300 and SG500 devices support only the following system CLI templates.

- APIC Bootstrap
- Banner Configuration-IOS
- Best_Practice_Access_3k
- Best_Practice_Access_4k
- Best_Practice_Global
- Certificate Authority-IOS
- Configure SNMPv3
- Configure VLAN
- Configure_Access_Port
- Crypto Map Configuration
- DNS Configuration
- EEM Environmental Variables
- Enable Password-IOS
- EtherChannel
- HTTP SWIM Image Upgrade Template
- HTTP-HTTPS Server and WSMA Configuration-IOS
- Local Management User
- Plug And Play Bootstrap
- RADIUS_AUTH
- Radius Acct. Servers
- Radius Configuration-IOS
- Reload Configuration-IOS
- TACACS Server
- TACACS-POST-PNP
- Trap Receiver
- stp

Add Interactive Commands

An interactive command contains the input that must be entered following the execution of a command.

To enter an interactive command in the CLI Content area, use the following syntax:

```
CLI Command<IQ>interactive question 1<R>command response 1 <IQ>interactive question
2<R>command response 2
```

where <IQ> and <R> tag are case-sensitive and must be entered as uppercase.

For example:

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

Note You must replace the <IQ> tag with the <IQNONEWLINE> tag for any interactive questions in which the default <return> or newline character is not required in the command for any of the controller devices. For example,

```
#INTERACTIVE
transfer download start <IQNONEWLINE>y/N<R>y<IQNONEWLINE>y/N<R>y
#ENDS_INTERACTIVE
```

Note The <IQ> tag utilizes regular expressions for interactive questions. You must use the valid regular expressions for matching patterns.

Format

```
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
```

Example for invalid content used in interactive question

```
#INTERACTIVE
save config<IQ>Are you sure you want to save? (y/n)<R>y
#ENDS_INTERACTIVE
```

Using the Question Mark "?" in between is invalid and does not match the pattern.

Example for valid content used in interactive question

```
#INTERACTIVE
save config<IQ>(y/n)<R>y
#ENDS_INTERACTIVE
```

Combining Interactive Enable Mode Commands

Use this syntax to combine interactive Enable Mode commands:

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R>response
```

```
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

For example:

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>XXX
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

Adding Interactive Multi-line Commands

This is an example of an interactive command that contains multiple lines:

```
#INTERACTIVE
macro name EgressQoS<IQ>Enter macro<R><MLTCMD>mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
wrr-queue random-detect min-threshold 4 70 80 90 100
wrr-queue random-detect max-threshold 4 80 90 100 100
wrr-queue random-detect min-threshold 5 70 80 90 100
wrr-queue random-detect max-threshold 5 80 90 100 100
wrr-queue random-detect min-threshold 6 70 80 90 100
wrr-queue random-detect max-threshold 6 80 90 100 100
wrr-queue random-detect min-threshold 7 60 70 80 90
wrr-queue random-detect max-threshold 7 70 80 90 100
@</MLTCMD>
#ENDS_INTERACTIVE
```

Deployment Flow for Composite Templates Using the Wizard

Step 1 Choose Configuration > Templates > Features & Technologies > Composite Templates > Composite Templates.

Step 2 Enter the required information in the Template Basic section.

Step 3 In the Template Detail section, choose the templates to include in the composite template, and click Save as New Template.

Step 4 After creating the composite template, click Deploy. The Deployment wizard page opens.

Step 5 Select the devices on which you want to deploy the template.

Step 6 Select the mode in which you want to deploy the template. The options are Work Flow and Export/Import CSV.

Step 7 Click the Work Flow option and click Next. See Step 6.

Step 8 Alternately, click Export/Import CSV option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.

a) Uncheck the Do you want Optional Parameters check box, if you want to skip the optional fields while filling the configuration values in the CSV file.
b) Click Export CSV to download the CSV template to your local system.
c) Enter the configuration values for each specific device in the downloaded CSV template.
d) Click Import CSV to upload the updated CSV file.The input values automatically gets updated.
e) Click Next to input values.

Step 9 In the Input Values tab, you can toggle between Form and CLI view. Configure the following in the Input Values tab:

a) Select templates for a device from the navigation widget. To select templates, click the circle (T1, T2, T3, T4, T5 ...) in the upper right corner. If there are more than five templates, click three dots. The drop-down list will pop-up with all the available templates.
b) Enter all the mandatory fields for each template, then click Apply.

   If the validation is successful, then the border of the circle around the selected template changes to green and green tick mark appears adjacent to the selected templates for the available templates in the popup.

Step 10 After entering the necessary configuration values, click Next or CLI to confirm the device and template configuration values.

Step 11 Schedule the deployment job using Schedule Deployment tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

  Failure Policy:

  - Ignore failure and continue—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  - Stop on failure—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
  - Copy Running Config to Startup—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
  - Archive Config after deploy—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 12 Click Next to view the job deployment summary.

Step 13 On the Deployment Summary tab, you will see the CLI view for each of the device.

Step 14 Click Finish to deploy the template.

Step 15 Click Job Status in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Deploy Templates to Devices Without Using Configuration Groups

Once a template is saved, it can be deployed (run on) devices. You can deploy a template from the Configuration > Templates > Features & Technologies navigation area, or by using Configuration Groups, which is launched from Configuration > Templates > Configuration Groups (see Create Configuration Groups for Deploying Templates to Groups of Devices , on page 392).

To deploy a customized or system template from the Features & Technologies navigation area:

Step 1 Choose Configuration > Templates > Features & Technologies

Step 2 Expand the drawer that contains the template(s) you want to deploy.

Step 3 Choose the templates you want to deploy, and click Deploy.

Step 4 In the Template Deployment window, check the settings and schedule and click OK.

Configure Controllers Using Configuration Templates

This section describes how to add and apply wireless templates. Templates allow you to set fields that you can then apply to multiple devices without having to reenter the common information.

The controller templates provides access to all templates from a single page. You can add and apply controller templates, view templates, or make modifications to the existing templates. This section also includes steps for applying and deleting controller templates and creating or changing access point templates.

To access the controller templates, choose Configuration > Templates > Features & Technologies > Features and Technologies > Controller.

See Controller Templates and Field Descriptions.

Related Topics

Create Controller Templates, on page 400
Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402
Configure Controller WLAN Client Profiles, on page 403
Configure Controllers to Use Mobile Concierge (802.11u), on page 404
Use AP Groups to Manage WLAN Configuration and Deployment, on page 404
Create WLAN AP Groups Templates, on page 405
Configure Lightweight APs Using Configuration Templates, on page 446
Configure Location Information for Switches Using Templates, on page 433
Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates, on page 434

Create Controller Templates

To create Features and Templates, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Controller Template.

Step 2 Hover your mouse cursor over the tool tip next to the template type and click New to create the template.

Step 3 Complete the required fields.

If you are creating a feature template that applies only to a particular device type, the Device Type field lists only the applicable device type, and you cannot change the selection. Specifying a device type helps you to prevent a mismatch; that is, you cannot create a configuration and apply the configuration to a wrong device.

Step 4 Click Save as New Template. After you save the template, apply it to your devices.

Step 5 To verify the status of a template deployment, choose Administration > Dashboard > Jobs Dashboard.

To modify the deployment parameters for any subsequent configuration template deployments, select a configuration job, then click Edit Schedule.

Add Controller Templates

To add a new controller template:

Step 1 Choose Configuration > Features & Technologies > Controller.

Step 2 Select the template you want to add.

Step 3 Enter the template name.

Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 Provide a description of the template.

Step 5 Click Save.

Related Topics

Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Delete Controller Templates

To delete a controller template:

Step 1 Choose Configuration > Features & Technologies > My Templates.

Step 2 Select the template(s) you want to delete, then click Delete.

Step 3 Click OK to confirm the deletion. If this template is applied to controllers, the Remove Template Confirmation page opens and lists all controllers to which this template is currently applied.

Step 4 Select the check box of each controller from which you want to remove the template.

Step 5 Click OK to confirm the deletion or Cancel to close this page without deleting the template.

Related Topics

Add Controller Templates, on page 401
Apply Controller Templates, on page 402

Apply Controller Templates

You can apply a controller template directly to a controller or to controllers in a selected configuration group.

To apply a controller template, follow these steps:

Step 1 Choose Configuration > Features & Technologies > Controller.

Step 2 From the left sidebar menu, choose the category of templates to apply.

Step 3 Click the template name for the template that you want to apply to the controller.

Step 4 Click Apply to Controllers to open the Apply to Controllers page.

Step 5 Select the check box for each controller to which you want to apply the template.

To select all controllers, select the check box that appears at the left most corner of the controllers table.

Select the Ignore errors on Apply template to Controllers check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

Step 6 Choose between applying the template directly to a controller or to all controllers in a selected configuration group.

To apply the template directly to a controller (or controllers), follow these steps:

a) Select the Apply to controllers selected directly radio button. The Apply to Controllers page lists the IP address for each available controller along with the controller name and the configuration group name (if applicable).
b) Select the check box for each controller to which you want to apply the template.

   Select the Ignore errors on Apply template to Controllers check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

To apply the template to all controllers in a selected configuration group, follow these steps:

a) Select the Apply to controllers in the selected Config Groups radio button. The Apply to Controllers page lists the name of each configuration group along with the mobility group name and the number of controllers included
b) Select the check box for each configuration group to which you want to apply the template.

   Configuration groups which have no controllers cannot be selected to apply the templates.

Step 7 You can perform the following additional operations:

- If you select the Save Config to Flash after apply check box, the save config to Flash command is executed after the template is applied successfully.
- If you select the Reboot Controller after apply check box, the controller reboots after the template is successfully applied.

This configuration results can be viewed in the Template Results page by enabling the View Save Config / Reboot Results option.

Step 8 Click Save.

You can apply some templates directly from the Template List page. Select the check box(es) of the template(s) that you want to apply, choose Apply Templates from the Select a command drop-down list, and click Go to open the Apply to Controllers page. Select the check box(es) of the controllers to which you want to apply this template, and click OK.

Related Topics

Add Controller Templates, on page 401

Configure Controller WLAN Client Profiles

When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form.

Follow these guidelines when configuring client profiling:

By default, client profiling will be disabled on all WLANs.

- Client profiling is supported on access points that are in Local mode and FlexConnect mode.
- Profiling is not supported for clients in the following scenarios:
  - Clients associating with FlexConnect mode APs in Standalone mode.
  - Clients associating with FlexConnect mode APs when local authentication is done with local switching is enabled.
- Both DHCP Proxy and DHCP Bridging mode on the controller are supported.
- Accounting Server configuration on the WLAN must be pointing at an ISE running 1.1 MnR or later releases. Cisco ACS does not support client profiling.
- The type of DHCP server used does not affect client profiling.
- If the DHCP_REQUEST packet contains a string that is found in the Profiled Devices list of the ISE, then the client will be profiled automatically.
- The client is identified based on the MAC address sent in the Accounting request packet.
- Only MAC address should be sent as calling station ID in accounting packets when profiling is enabled.
- With profiling enabled for local switching FlexConnect mode APs, only VLAN override is supported as an AAA override attribute.

To configure client profiling, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > WLANs > WLAN Configuration.

Step 2 Click the Advanced tab.

Step 3 Select the DHCP Profiling check box to enable DHCP profiling.

Step 4 Select the HTTP Profiling check box to enable HTTP profiling.

HTTP client profiling is supported since controller Version 7.3.1.31.

Step 5 Click Save.

See the section Controller >WLANs > WLAN Configuration > Advanced in Cisco Prime Infrastructure Reference Guide

Configure Controllers to Use Mobile Concierge (802.11u)

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:

- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

To configure Mobile Concierge (802.11u) groups:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > WLANs > WLAN Configuration.

Step 2 Click the Hot Spot tab.

Step 3 Complete the required fields on the following tabs:

- 802.11u Configuration
- Others
- Realm
- Service Advertisements
- Hotspot 2.0

Step 4 Click Save as New Template.

See the section Controller > WLANs > WLAN Configuration in Cisco Prime Infrastructure Reference Guide

Use AP Groups to Manage WLAN Configuration and Deployment

- Remember the following points when managing WLAN configurations using AP groups
- AP Groups (for controllers Release 5.2 and later) are referred to as AP Group VLANs for controllers prior to 5.2.
- To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.
- Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.
- The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

Related Topics

Create WLAN AP Groups Templates, on page 405
Add WLAN AP Groups, on page 406
Delete WLAN AP Groups, on page 405

Create WLAN AP Groups Templates

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits include more effective management of load balancing and bandwidth allocation.

To configure WLAN AP Groups, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > WLANs > AP Groups.

The WLAN > AP Groups page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 2 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go. To modify an existing template, click the template name. The AP Groups template page appears.

This page displays a summary of the AP groups configured on your network. In this page, you can add, remove, edit, or view details of an AP group. Click in the Edit column to edit its access point(s). Select the check box in the WLAN Profile Name column, and click Remove to delete WLAN profiles.

Note
- The maximum characters that you can enter in the Description text box is 256.

Related Topics

Use AP Groups to Manage WLAN Configuration and Deployment, on page 404
Add WLAN AP Groups, on page 406
Delete WLAN AP Groups, on page 405

Delete WLAN AP Groups

To delete an access point group, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies.

Choose Controller > WLANs > AP Groups from the left sidebar menu.

Step 2 Click Remove.

Related Topics

Use AP Groups to Manage WLAN Configuration and Deployment, on page 404
Add WLAN AP Groups, on page 406
Create WLAN AP Groups Templates, on page 405

Add WLAN AP Groups

You can create or modify a template for dividing the WLAN profiles into AP groups.

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > WLANs > AP Groups.

Step 2 Choose Add Template from the Select a command drop-down list, and click Go.

Step 3 Enter a name and group description for the access point group. The group description is optional.

Step 4 If you want to add a WLAN profile, click the WLAN Profiles tab and configure the following fields:

a) Click Add.

b) Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.

c) Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.

To display all available interfaces, delete the current interface from the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

d) Select the NAC Override check box, if applicable. The NAC override feature is disabled by default.

e) Specify the policy configuration parameters by clicking the Add/Edit link.

- • Policy Name—Name of the policy.
  • Policy Priority—Configure policy priority between 1 and 16. No two policies can have same priority. Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.

f) When access points and WLAN profiles are added, click Save.

Step 5 If you want to add a RF profile, click the RF Profiles tab, and configure the following fields:

- 802.11a—Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
- 802.11b—Drop-down list from which you can choose an RF profile for APs with 802.11b radios.
- When RF profiles are added, click Save.

See the section Controller > 802.11 > RF Profiles in Cisco Prime Infrastructure Reference Guide

Create a Remote LAN (RLAN) Template

Step 1 Choose Configuration > Features and Technologies > Controller > WLANs > WLAN Configuration.

Step 2 In the Template Basic area, fill the requisite details..

Step 3 In the General tab in Template Detail area, check the Wired LAN checkbox to enable it.

Step 4 Select Remote LAN from the LAN Type dropdown menu.

Step 5 Enter the Profile Name.

Step 6 Select the Admin Status checkbox to enable it.

Note This is necessary if you want to map your RLAN with an AP Group and enable the ports.

Step 7 Save the settings.

Step 8 Deploy the template.

Note Applicable only to MEs with version 8.7 onwards.

Map Remote LAN (RLAN) to an AP Group

Step 1 Choose Configuration > Features and Technologies > Controller > WLANs > AP Groups.
Alternatively, to view the available AP groups, look for the same folder structure under My Templates.

Step 2 Enter the requisite details in the Template Basic area (if creating a new template).

Step 3 Click WLAN Profile and then click Add.

Step 4 Select the WLAN Profile and the Interface or Interface group from their respective dropdown menus.

Step 5 Click Save.

Step 6 Click Ports.

Step 7 Select the RLAN from the drop down menu adjacent Port number.

Step 8 Deploy the template.

Note Applicable only to MEs with version 8.7 onwards.

Configure FlexConnect Users in FlexConnect AP Groups

You can click the Users configured in the group link that appears when the FlexConnect Local Authentication check box is enabled to view the list of FlexConnect users. You can create FlexConnect users only after you save the FlexConnect AP Group.Maximum 100 FlexConnect users are supported in controller Release 5.2.x.x and later. If controller Release 5.2.0.0, and earlier supports only 20 FlexConnect users.

To delete a FlexConnect User, choose a user from the FlexConnect Users list, and then click Delete.

To configure a FlexConnect user, follow these steps:

Step 1 Choose Configuration > Features & Technologies > Controller > FlexConnect >FlexConnect AP Groups.

Step 2 Hover the mouse on FlexConnect AP Groups and select Show All Templates.

Step 3 Click the Local Authentication tab and select the FlexConnect Local Authentication check box to enable local authentication for this FlexConnect group.

Step 4 Click the Users configured in the group link. The FlexConnect Users page appears.

Step 5 If you want to add a new user, choose Add User from the Select a command drop-down list, and click Go. The Add User page appears.

Step 6 In the User Name text box, enter the FlexConnect username.

Step 7 In the Password text box, enter the password.

Step 8 Reenter the password in the Confirm Password text box.

Step 9 Click Save.

See the section Controller > FlexConnect > FlexConnect AP Groups in Cisco Prime Infrastructure Reference Guide.

Configure Device-Based and User-Based Controller Policies

The Policy Configuration Templates page enables you to configure the device-based policies on the controller. You can configure policies for a user or a device on the network. The maximum number of policies that you can configure is 64. Policies are not applied on WLANs and AP groups if AAA override is configured on the controller.

To configure Policy Configuration templates:

Step 1 Choose Configuration > Templates > Features &Technologies > Controller > WLANs > Policy Configuration.

Step 2 If you want to add a new template, choose Add Template from the Select a command drop-down list, and click Go.

Step 3 Configure the required fields.

Step 4 Click Save as New Template.

Configure AAA on Controllers Using Config Templates

To add a new template with general security information for a controller, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security.

Step 2 Choose AAA > General - AAA from the left sidebar menu.

Step 3 Click New beside the template you want to add.

Step 4 Configure the following fields:

- Template Name—Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.
- Maximum Local Database Entries (on next reboot)—Enter the maximum number of allowed database entries. This becomes effective on the next reboot.
- Mgmt User Re-auth Interval—Enter the termination interval for management users.

Step 5 Click Save.

Step 6 The template appears in the Template List page. In the Template List page, you can apply this template to controllers.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure RADIUS Authentication Servers to Control User Access to Controllers

You can add a RADIUS authentication template or make modifications to an existing template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

See the section Controller > Security > AAA > RADIUS Auth Servers in Cisco Prime Infrastructure Reference Guide.

Configure RADIUS and TACACS Server Fallback Settings on Controllers

To add and configure a RADIUS TACACS Fallback template or modify an existing template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > AAA > RADIUS TACACS+ Fallback.

Step 2 From the Radius Fallback group box, configure the following:

- From the Radius Fallback Mode drop-down list, you can choose one of the following:
  - Off—Disables fallback.
  - Passive—You must enter a time interval.
  - Active—You must enter a username and time interval.

Step 3 From the TACACS Fallback group box, configure the following:

- Choose either Enable or Disable from the Fallback Mode drop-down list.
- In the Time Interval text box, enter a value for TACACS Fallback test interval in seconds.

Step 4 Click Save as New Template.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure Local EAP Timeout Settings

This page allows you to specify a timeout value for local EAP. You can then add or make changes to an existing local EAP general template.

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

Related Topics

Configure Authentication Order When Using LDAP and a Local Database to Control User Access to Controllers, on page 410

Configure Authentication Order When Using LDAP and a Local Database to Control User Access to Controllers

You can specify the order that LDAP and local databases use to retrieve user credential information. This page allows you to add or make modifications to an existing network user credential retrieval priority template.

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > Local EAP > Network Users Priority.

Step 2 Use the left and right arrow keys to include or exclude network user credentials in the right page.

Step 3 Use the up and down keys to determine the order credentials are tried.

Step 4 Click Save.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure Credentials Used for Controller User authentication (Local Network Templates)

With this template, you can store the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP might use the local user database as its back end database to retrieve user credentials. This page allows you to add or make modifications to an existing local network user template. You must create a local net user and define a password when logging in as a web authentication client.

To configure a Local Network Users template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > AAA > Local Net Users.

Step 2 Click Import CSV to import from a file, then click Browse to navigate to the file. Then continue to Step 6. If you disable the import, continue to Step 3.

Only CSV file formats are supported.

reads data from the second row onwards. The first row in the file is treated as the header and the data is not read by . The header can either be blank or filled.

Step 3 Enter the following details:

- Username
- Password
- Profile
- Description.

The Profile column if left blank (or filled in with any profile) means a client on any profile can use this account.

Step 4 Use the drop-down list to choose the SSID which this local user is applied to or choose the any SSID option.

Step 5 Enter a user-defined description of this interface.

Step 6 Click Save.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Control How Many Concurrent Login Sessions a User Can Have

You can set the maximum number of concurrent logins that each single user can have.

To add a user login template or make modifications to an existing template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > User Login Policies.

Step 2 Enter the maximum number of concurrent logins each single user can have.

Step 3 Click Save as New Template.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure APs to Filter on MAC Addresses

To add a MAC filter template or make modifications to an existing template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > AAA > MAC Filtering or choose Security > MAC Filtering.

Step 2 Click Import CSV to import a file containing access point MAC addresses.

Step 3 Enter the desired file path or click Browse to import the file.

The import file must be a CSV file with MAC address, profile name, interface, and description (such as 00:11:22:33:44:55, Profile1, management, test filter). If you disable the Import from File check box, continue to step 4.

The client MAC address appears.

Step 4 Choose the profile name to which this MAC filter is applied or choose the Any Profile option.

Step 5 Use the drop-down list to choose from the available interface names.

Step 6 Enter a user-defined description of this interface.

Step 7 Click Save as New Template.

You cannot use MAC address in the broadcast range.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure AP or MSE Controller Authorization

These templates are devised for Cisco 11xx/12xx series access points converted from Cisco IOS to lightweight access points or for 1030 access points connecting in bridge mode. See the Cisco Mobility Services Engine Configuration Guide for further information.

To add a MSE authorization template or make modifications to an existing template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > AAA > AP or MSE Authorization.

Step 2 Click Import CSV to import a file containing access point MAC addresses.

You can only import a CSV file. The file format parallels the fields in the GUI and therefore includes access point base radio MAC, Type, Certificate Type (MIC or SSC), and key hash (such as 00:00:00:00:00:00, AP, SSC, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx). No other file formats are not supported.

Step 3 Enter the desired file path or click Browse to import the file.

Step 4 Click Save As New Template.

You cannot use MAC address in the broadcast range.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure Controllers to Manually Disable Clients By MAC Address

This page allows you to add a manually disable client template or make modifications to an existing disabled client template.

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > Manually Disable Clients.

Step 2 Enter the MAC address of the client you want to disable.

Step 3 Enter a description of the client you are setting to disabled.

Step 4 Click Save as New Template.

You cannot use a MAC address in the broadcast range.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure Controllers' Client Exclusion Policies

To add a client exclusion policies template or modify an existing client exclusion policies template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > Client Exclusion Policies.

Step 2 Complete the following fields:

- Template Name—Enter a name for the client exclusion policy.
- Excessive 802.11 Association Failures—Enable to exclude clients with excessive 802.11 association failures.
- Excessive 802.11 Authentication Failures—Enable to exclude clients with excessive 802.11 authentication failures.
- Excessive 802.1X Authentication Failures—Enable to exclude clients with excessive 802.1X authentication failures.
- Excessive 802.11 Web Authentication Failures—Enable to exclude clients with excessive 802.11 web authentication failures.
- IP Theft or Reuse—Enable to exclude clients exhibiting IP theft or reuse symptoms.

Step 3 Click Save as New Template

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure AP Authentication Using MFP

Management Frame Protection (MFP) provides for the authentication of 802.11 management frames by the wireless network infrastructure. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy. An access point must be a member of a WDS to transmit MFP frames.

When MFP detection is enabled, the access point validates every management frame that it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system.

To add or make modifications for the access point authentication and management frame protection (MFP) template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > AP Authentication and MFP.

Step 2 From the Protection Type drop-down list, choose one of the following authentication policies:

- None—No access point authentication policy.
- AP Authentication—Apply authentication policy.
- MFP—Apply management frame protection.

Alarm trigger threshold appears only when AP authentication is selected as a protection type. Set the number of hits from an alien access point to ignore before raising an alarm.

The valid range is from 1 to 255. The default value is 255.

Step 3 Click Save as New Template.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure the Web Auth Authentication Type for a Controller WLAN

With web authentication, guests are automatically redirected to a web authentication page when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts might be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. You can use this template to replace the Web authentication page provided on the controller.

To add or make modifications to an existing web authentication template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Security > AAA > Web Auth Configuration.

Step 2 Choose one of the following web authentication type from the drop-down list.

- default internal— You can still alter the page title, message, and redirect URL, as well as whether the logo appears. Continue to Step 5.
- customized web authentication—Click Save and apply this template to the controller. You are prompted to download the web authentication bundle.
- Before you can choose customized web authentication, you must first download the bundle by going to Config > Controller and choose Download Customized Web Authentication from the Select a command drop-down list, and click Go.
- external—you need to enter the URL you want to redirect to after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page

Step 3 Select the Logo Display check box if you want your company logo displayed.

Step 4 Enter the title you want displayed on the Web Authentication page.

Step 5 Enter the message you want displayed on the Web Authentication page.

Step 6 Provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user would be directed to the company home page.

Step 7 Click Save as New Template.

Related Topics

Download Customized Web Authentication Pages to Controllers, on page 415

Download Customized Web Authentication Pages to Controllers

Before You Begin, follow these steps:

You can download a customized Web Authentication page to the controller. With a customized web page, you can establish a username and password for user web access.

When downloading customized web authentication, you must follow these strict guidelines:

- Provide a username.
- Provide a password.
- Retain a redirect URL as a hidden input item after extracting from the original URL.
- Extract the action URL and set aside from the original URL.

Include scripts to decode the return status code.

Step 1 Download the sample login.html bundle file from the server. The following figure displays .html file. The login page is presented to web users the first time they access the WLAN if web authentication is turned on.

Figure 10: Login.html

Step 2 Edit the login.html file and save it as a .tar or .zip file.

You can change the text of the Submit button to read Accept terms and conditions and Submit.

Step 3 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add IP address of TFTP server).

- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as because the built-in TFTP server of and third-party TFTP server use the same communication port.

Step 4 Download the .tar or .zip file to the controller(s).

The controller allows you to download up to 1 MB of a .tar file containing the pages and image files required for the Web authentication display. The 1 MB limit includes the total size of uncompressed files in the bundle.

You can now continue with the download.

Step 5 Copy the file to the default directory on your TFTP server.

Step 6 Choose Configuration > Network > Network Devices > Wireless Controller.

Step 7 Click on a Device Name. If you select more than one device, the customized Web authentication page is downloaded to multiple controllers.

Step 8 From the left sidebar menu, choose System > Commands.

Step 9 From the Upload/Download Commands drop-down list, choose Download Customized Web Auth, and click Go.

Step 10 The IP address of the controller to receive the bundle and the current status are displayed.

Step 11 Choose local machine from the File is Located On field. If you know the filename and path relative to the root directory of the server, you can also select TFTP server.

For a local machine download, either .zip or .tar file options exists, but does the conversion of .zip to .tar automatically. If you chose a TFTP server download, only .tar files would be specified.

Step 12 Enter the maximum number of times the controller should attempt to download the file in the Maximum Retries field.

Step 13 Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout field.

Step 14 The files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click Browse to navigate to it.

Step 15 Click OK.

If the transfer times out, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of . Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of server, and the download web page now automatically populates the filename.

Step 16 Click the Click here to download a sample tar file link to get an option to open or save the login.tar file.

Step 17 After completing the download, you are directed to the new page and able to authenticate.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402
Configure the Web Auth Authentication Type for a Controller WLAN, on page 414

Configure External Web Authorization Servers for Controllers

To create or modify an External Web Auth Server template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > External Web Auth Server or choose Security > External Web Auth Server.

Step 2 Enter the server address of the external web auth server.

Step 3 Click Save as New Template.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure Password Policies for Controllers

To add or make modifications to an existing password policy template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > Password Policy.

Step 2 You can enable or disable the following settings:

- Password must contain characters from at least 3 different classes such as uppercase letters, lowercase letters, digits, and special characters.
- No character can be repeated more than 3 times consecutively.
- Password cannot be the default words like cisco or admin.
- Password cannot be “cisco”, “ocsic”, “admin”, “nimda’ or any variant obtained by changing the capitalization of letters, or by substituting ‘1” “|” or “!” for i, or substituting “0” for “o”, or substituting “$” for “s”.
- Password cannot contain username or reverse of username.

Step 3 Click Save.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Apply Controller Templates

You can apply a controller template directly to a controller or to controllers in a selected configuration group.

To apply a controller template, follow these steps:

Step 1 Choose Configuration > Features & Technologies > Controller.

Step 2 From the left sidebar menu, choose the category of templates to apply.

Step 3 Click the template name for the template that you want to apply to the controller.

Step 4 Click Apply to Controllers to open the Apply to Controllers page.

Step 5 Select the check box for each controller to which you want to apply the template.

To select all controllers, select the check box that appears at the left most corner of the controllers table.

Select the Ignore errors on Apply template to Controllers check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

Step 6 Choose between applying the template directly to a controller or to all controllers in a selected configuration group.

To apply the template directly to a controller (or controllers), follow these steps:

a) Select the Apply to controllers selected directly radio button. The Apply to Controllers page lists the IP address for each available controller along with the controller name and the configuration group name (if applicable).
b) Select the check box for each controller to which you want to apply the template.

   Select the Ignore errors on Apply template to Controllers check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

To apply the template to all controllers in a selected configuration group, follow these steps:

a) Select the Apply to controllers in the selected Config Groups radio button. The Apply to Controllers page lists the name of each configuration group along with the mobility group name and the number of controllers included
b) Select the check box for each configuration group to which you want to apply the template.

   Configuration groups which have no controllers cannot be selected to apply the templates.

Step 7 You can perform the following additional operations:

- If you select the Save Config to Flash after apply check box, the save config to Flash command is executed after the template is applied successfully.
- If you select the Reboot Controller after apply check box, the controller reboots after the template is successfully applied.

This configuration results can be viewed in the Template Results page by enabling the View Save Config / Reboot Results option.

Step 8 Click Save.

You can apply some templates directly from the Template List page. Select the check box(es) of the template(s) that you want to apply, choose Apply Templates from the Select a command drop-down list, and click Go to open the Apply to Controllers page. Select the check box(es) of the controllers to which you want to apply this template, and click OK.

Related Topics

Add Controller Templates, on page 401

Configure Controller Access Control List

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs can be applied to data traffic to and from wireless clients or to all traffic destined for the controller Central Processing Unit

(CPU) and can now support reusable grouped IP addresses and reusable protocols. After ACLs are configured in the template, they can be applied to the management interface, the AP-manager interface, or any of the dynamic interfaces for client data traffic; to the Network Processing Unit (NPU) interface for traffic to the controller CPU; or to a WAN.

You can create or modify an ACL template by protocol, direction, and the source or destination of the traffic.

You can now create new mappings from the defined IP address groups and protocol groups. You can also automatically generate rules from the rule mappings you created. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add up to 29 rules.

Existing ACL templates are duplicated into a new ACL template. This duplication clones all the ACL rules and mappings defined in the source ACL template.

This release of provides support to IPv6 ACLs.

To add or modify an existing ACL template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > Access Control Lists.

Step 2 Complete the following fields:

- Access Control List Name—User-defined name of the template.
- ACL Type—Choose either IPv4 or IPv6. IPv6 ACL is supported from controller Release 7.2.x.

Step 3 Choose IP Groups from the left sidebar menu to create reusable grouped IP addresses and protocols.

Step 4 Choose Add IP Group from the Select a command drop-down list and click Go to define a new IP address group.

One IP address group can have a maximum of 128 IP address and netmask combinations. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group page opens.For the IP address of any, an any group is predefined.

Step 5 Edit the following current IP group fields if required in the ACL IP Groups details page:

- IP Group Name
- IP Address
- Netmask OR CIDR Notation
- Enter the Netmask or CIDR Notation and then click Add. The list of IP addresses or Netmasks appears in the List of IP Address/Netmasks text box.
- CIDR or Classless InterDomain Routing a protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks. CIDR notation allows you to add a large number of clients that exist in a subnet range by configuring a single client object.
- Netmask allows you to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property.
- BroadCast/Network
- List of IP Addresses/Netmasks
- Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete any IP address or Netmask.

Step 6 Choose Access Control > Protocol Groups from the left sidebar menu to define an additional protocol that is not a standard predefined one.

The protocol groups with their source and destination port and DSCP are displayed.

Step 7 Choose Add Protocol Group from the Select a command drop-down list, and click Go to create a new protocol group. To view or modify an existing protocol group, click the URL of the group.

The Protocol Groups page appears.

Step 8 Enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the parameters of a rule, the action for this rule is exercised.

Step 9 Choose one of the following protocols from the drop-down list:

- Any—All protocols
- TCP—Transmission Control Protocol
- UDP—User Datagram Protocol
- ICMP—Internet Control Message Protocol
- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP—Internet Protocol
- Eth Over IP—Ethernet over Internet Protocol
- Other Port OSPF—Open Shortest Path First
- Other—Any other IANA protocol (http://www.iana.org/)

Some protocol choices (such as TCP or UDP) cause additional Source Port and Dest Port GUI elements to appear.

- Source Port—Specify the source of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.
- Dest Port—Specify the destination of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.

Step 10 Choose any or specific from the DSCP (Differentiated Services Code Point) drop-down list. If you choose specific, enter the DSCP (range of 0 to 255).

DSCP is a packet header code that can be used to define the quality of service across the Internet.

Step 11 Click Save.

Step 12 Choose the ACL template to which you want to map the new groups to define a new mapping. All ACL mappings appear on the top of the page, and all ACL rules appear on the bottom.

Step 13 Choose Add Rule Mappings from the Select a command drop-down list. The Add Rule Mapping page appears.

Step 14 Configure the following fields:

- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.
- Direction—Any, Inbound (from client) or Outbound (to client).
- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 15 Click Add. The new mappings populate the bottom table.

Step 16 Click Save.

Step 17 Choose the mappings for which you want to generate rules, and click Generate. This automatically creates the rules.

Note For Export/Import ACL Template from Prime Infrastructure 3.8 release, only ACL Rule configuration will get exported/imported. No ACL Rule-Mappings configuration will be available in the exported/imported template.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure FlexConnect Access Control List to Control Traffic on Controllers

You can create or modify a FlexConnect ACL template for configuring the type of traffic that is allowed by protocol, and the source or destination of the traffic. The FlexConnect ACLs do not support IPv6 addresses.

To configure and apply an Access Control List template to a Controller, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > FlexConnect ACLs.

Step 2 Enter a name for the new FlexConnect ACL.

Step 3 Click Save as New Template.

A FlexConnect ACL template is created. You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All FlexConnect ACL mappings appear on the top of the page, and all FlexConnect ACL rules appear in the bottom.

Step 4 Click Add Rule Mappings, then configure the following fields in the FlexConnect ACL IP Protocol Map page:

- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.
- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 5 Click Add. The new mappings populate the bottom table.

Step 6 Click Save.

Step 7 Choose the mappings for which you want to generate rules, and click Generate. This automatically creates the rules.

Step 8 From the Select a command drop-down list in the FlexConnect ACL page, choose Apply Templates.

The Apply to Controllers page appears.

Step 9 Select Save Config to Flash after apply check box to save the configuration to Flash after applying the FlexConnect ACL to the controller.

Step 10 Select Reboot Controller after apply to reboot the controller once the FlexConnect ACL is applied. This check box is available only when you select the Save Config to Flash after apply check box.

Step 11 Select one or more controllers and click OK to apply the FlexConnect ACL template.

The FlexConnect ACL that you created appears in Configure > Controller Template Launch Pad > IP Address > Security > Access Control > FlexConnect ACLs.

Note For Export/Import ACL Template from Prime Infrastructure 3.8 release, only ACL Rule configuration will get exported/imported. No ACL Rule-Mappings configuration will be available in the exported/imported template.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Manage Bulk Updation of FlexConnect Groups

Create FlexConnect Groups In Bulk

To create multiple FlexConnect groups together as specified in the import file, follow these steps:

Step 1 Click Configuration > Templates > Features & Technologies.

Step 2 In the Templates pane on left, click Features and Technologies > Controller > FlexConnect > FlexConnect Bulk Update.

Step 3 In Template Detail area, select Create FlexConnect Group from the Bulk Operation Type drop-down menu.

Step 4 (Optional) Check the Overwrite checkbox to enable it.

Note If you enable overwrite, FlexConnect Group templates with a source configuration in the .csv file will overwrite any existing duplicate templates in your Prime Infrastructure database.

Step 5 Click Choose File button to select your .csv file.

Step 6 Click Upload to load the .csv file and trigger the process.

Important

- Copying from source copies all remaining configuration except APs.

Based on the parameters chosen. the following table lists out scenarios and their expected results.

Overwrite Enabled	Source Specified	Template Existing	Outcome
Yes	Yes	No	Success Creates new template with source template values
Yes	No	No	Success Creates new template with default values

Overwrite Enabled	Source Specified	Template Existing	Outcome
Yes	Yes	Yes	Success Overwrites the existing template with source template values
Yes	No	Yes	Failure Does not overwrite, as source template is not specified
No	Yes	No	Success Overwrites the existing template with source template values
No	No	No	Success Creates new template with default values
No	Yes	Yes	Failure Does not create template, as it already exists and overwrite is not enabled
No	No	Yes	Failure Does not create template, as it already exists and overwrite is not enabled

Add Users to FlexConnect Groups in Bulk

To add multiple users to FlexConnect groups together as specified in the import file, follow these steps:

Step 1 Click Configuration > Templates > Features & Technologies.

Step 2 In the Templates pane on left, click Features and Technologies > Controller > FlexConnect > FlexConnect Bulk Update.

Step 3 In Template Detail area, select Add Users to FlexConnect Users.

Step 4 (Optional) Check the Replace Existing Users checkbox to enable it.

Note If you enable this, all existing users will be replaced by new users as specified in the import file.

Step 5 Click Choose File button to select your .csv file.

Step 6 Click Upload to load the .csv file and trigger the process.

Based on the parameters chosen.the following table lists out scenarios and their expected results.

Important

Replace Existing Users	User Already Exists	Outcome
Disabled	No	Success Adds new user to the specified FlexConnect group
Disabled	Yes	Failure Does not add because the user already exists
Enabled	No	Success Add new user to the specified FlexConnect group.
Enabled	Yes	Success Replaces exixting user (if any) with the same username with one specified in the .csv file

Add APs to FlexConnect Groups in Bulk

To add ,multiple Access Points to FlexConnect groups together as specified in the import file, follow these steps:

Step 1 Click Configuration > Templates > Features & Technologies.

Step 2 In the Templates pane on left, click Features and Technologies > Controller > FlexConnect > FlexConnect Bulk Update.

Step 3 In Template Detail area, select Add APs to FlexConnect Groups from the Bulk Operation Type drop-down menu.

Step 4 (Optional) Check the Overwrite checkbox to enable it.

Note If you enable overwrite, FlexConnect Group templates with a source configuration in the .csv file will overwrite any existing duplicate templates in your Prime Infrastructure database.

Step 5 Click Choose File button to select your .csv file.

Step 6 Click Upload to load the .csv file and trigger the process.

Based on the parameters chosen. the following table lists out scenarios and their expected results.

Important

Overwrite	AP Associated to	Outcome
Disabled	Same FlexConnect Group	Success Retains AP in the same FlexConnect group
Disabled	Different FlexConnect Group	Failure Does not add AP, as it is associated to another FlexConnect group.
Disabled	No Group	Success Adds AP to the FlexConnect group.
Enabled	Same FlexConnect Group	Success Retains AP in the same FlexConnect group.
Enabled	Different FlexConnect Group	Success Adds AP to the specified FlexConnect group and deletes it from the older FlexConnect group.
Enabled	No Group	Success Adds AP to the FlexConnect group.

Configure Access Control List Traffic Control Between the Controller CPU and NPU

CPU ACL configuration with IPv6 is not supported in this release because all IP addresses of controllers on interfaces use IPv4 except the virtual interface. The existing ACLs are used to set traffic controls between the Central Processing Unit (CPU) and Network Processing Unit (NPU).

To add or modify an existing CPU ACL template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > CPU Access Control List.

Step 2 Select the check box to enable CPU ACL. When CPU ACL is enabled and applied on the controller, displays the details of the CPU ACL against that controller.

Step 3 From the ACL Name drop-down list, choose a name from the list of defined names.

Step 4 From the CPU ACL Mode drop-down list, choose which data traffic direction this CPU ACL list controls. The choices are the wired side of the data traffic, the wireless side of the data traffic, or both wired and wireless.

Step 5 Click Save as New Template.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure Rogue AP and Client Security Policies on Controllers

Rogue templates enable you to configure the rogue policy (for access points and clients) applied to the controller. It also determines whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network.With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.

There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.

Rogue access point rules allow you to define rules to automatically classify rogue access points. applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time). Rogue access point rules also help reduce false alarms.

The new enhancements to the role classification rule are applicable for Cisco WLC 7.4 and later. These enhancements are not applicable to Catalyst 3850, Catalyst 3650, Catalyst 4500 switches, and Cisco 5760 WLAN Controllers (WLC).

To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > Rogue AP Rules.

Rogue classes include the following types:

- Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
- Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
- Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

See Combine Multiple Controller Rogue AP Rules in Rogue AP Rule Groups and the following topics in Cisco Prime Infrastructure Reference Guide for more information.

- Controller > Security > Wireless Protection Policies > Rogue Policies
- Controller > Security > Wireless Protection Policies > Rogue AP Rules
- Controller > Security > Wireless Protection Policies > Ignored Rogue AP

Define Controller Rogue AP Classification Rules

To configure rogue rules on , follow these steps:

1. Create a Rogue AP rule
2. Create a Rogue AP Rule Group that contains all the rules you want to apply
3. Deploy the Rogue AP Rule Group to the controllers

See the section Controller > Security > Wireless Protection Policies > Rogue AP Rules in Cisco Prime Infrastructure Reference Guide.

Related Topics

- Combine Multiple Controller Rogue AP Rules in Rogue AP Rule Groups

Combine Multiple Controller Rogue AP Rules in Rogue AP Rule Groups

A rogue access point rule group template allows you to combine more than one rogue access point rule to controllers. To view current rogue access point rule group templates or create a new rule group, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > Rogue AP Rule Groups.

Step 2 Enter a template name.

Step 3 To add a Rogue AP rule, click to highlight the rule in the left column. Click Add to move the rule to the right column.

Rogue access point rules can be added from the Rogue Access Point Rules section.

Step 4 To remove a rogue access point rule, click to highlight the rule in the right column. Click Remove to move the rule to the left column.

Step 5 Use the Move Up/Move Down buttons to specify the order in which the rules apply. Highlight the desired rule and click Move Up or Move Down to move it higher or lower in the current list.

Step 6 Click Save to confirm the rogue access point rule list.

Step 7 Click Deploy to apply the rule group to the controller.

See View Deployed Rogue AP Rules and the section Controller > Security > Wireless Protection Policies > Rogue AP Rules in Cisco Prime Infrastructure Reference Guide.

View Deployed Rogue AP Rules

You can view and edit the Rogue AP Rules that you previously deployed.

Step 1 Choose Monitor > Network > Network Devices > Wireless Controllers.

Step 2 Click on a Device Name, then select Security > Wireless Protection Policies > Rogue AP Rules.

Step 3 Click on a Rogue AP Rule name to edit the rule.

Step 4 To view Rogue AP alarms, click the Alarm Summary at the top right of the page, then select Rogue AP. You can also choose Dashboard > Wireless > Security to view Rogue AP information.

Configure SIP Snooping for Controllers

Keep the following guidelines in mind when using SIP Snooping:

- SIPs are available only on the Cisco 5500 Series Controllers and on the 1240, 1130, and 11n access points.
- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

To configure SIP Snooping for a controller, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > 802.11 > SIP Snooping.

Step 2 Configure the following fields:

- Port Start
- Port End

If single port is to be used, configure both start and end port fields with same number.

Step 3 Click Save as New Template.

See the following section in Cisco Prime Infrastructure Reference Guide

- Controller > 802.11 > Load Balancing
- Controller > 802.11 > Band Select
- Controller > 802.11 > Preferred Call
- Controller > 802.11 RF Profiles

Create Management Templates

You can create or modify the templates for the following management parameters of the controllers.

- Trap Receivers
- Trap Control
- Telnet and SSH
- Multiple Syslog servers
- Local Management Users
- Authentication Priority

See Configure a Controller's Management Parameters , on page 567, for more information.

Use Microsoft LyncSDN With

LyncSDN configuration is not supported on Virtual and Cisco 2500 Series and Virtual Controllers.

You can create these LyncSDN templates:

- LyncSDN Global Config feature templates

- LyncSDN PolicyFeature templates
- LyncSDN ProfileFeature templates

Related Topics

Configure Controllers to Use Microsoft LyncSDN Diagnostics, on page 429
Configure Controllers to Use Microsoft LyncSDN Policies to Monitor Network Traffic QoS, on page 429
Configure Controllers to Use Microsoft LyncSDN WLAN Profiles , on page 430

Configure Controllers to Use Microsoft LyncSDN Diagnostics

To create parameters to apply to devices using the LyncSDN Global Config feature, follow these steps:

Step 1 Choose Configuration > Features & Technologies > Controller > LyncSDN > LyncSDN Global Config.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.

Step 4 In the Template Detail area, configure the following information:

- Select the LyncServer checkbox to enable or disable the LYNC application on the .
- Enter the port number.
- You can configure support for HTTP/HTTPS communication on for LYNC server. supports only http. For https certificate, you need to provide and approved at Lync server which takes once Lync service is ready from .

Step 5 When you are finished, click Save as Template.

Related Topics

Configure Controllers to Use Microsoft LyncSDN Policies to Monitor Network Traffic QoS, on page 429
Configure Controllers to Use Microsoft LyncSDN WLAN Profiles , on page 430

Configure Controllers to Use Microsoft LyncSDN Policies to Monitor Network Traffic QoS

To create parameters to apply to devices using the LyncSDN Policy feature, follow these steps:

Step 1 Choose Configuration > Features & Technologies > Controller > LyncSDN > LyncSDN Policy.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.

Step 4 In the Template Detail area, configure the following information:

- Choose the policy of audio lync call on WLAN from the Audio drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.
- Choose the policy of video lync call on WLAN from the Video drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.
- Choose the policy of desktop-share lync call on WLAN from the Application-Sharing drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.
- Choose the policy of file transfer lync call on WLAN from the File-Transfer drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.

Step 5 When you are finished, click Save as Template.

Related Topics

Configure Controllers to Use Microsoft LyncSDN Diagnostics, on page 429
Configure Controllers to Use Microsoft LyncSDN WLAN Profiles , on page 430

Configure Controllers to Use Microsoft LyncSDN WLAN Profiles

To create parameters to apply to devices using the LyncSDN Profile feature, follow these steps:

Step 1 Choose Configuration > Features & Technologies > Controller > LyncSDN > LyncSDN Policy.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.

Step 4 In the Template Detail area, click the Wlan Profile check box and select a policy from the LyncSDN Policy drop-down list.

Step 5 When you are finished, click Save as Template.

Related Topics

Configure Controllers to Use Microsoft LyncSDN Diagnostics, on page 429
Configure Controllers to Use Microsoft LyncSDN Policies to Monitor Network Traffic QoS, on page 429

Configure AVC Profiles for Application Classification on Controllers

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1400 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

AVC is supported only on the following controllers:

- Cisco 2500 and 5500 Series Controllers.
- WiSM 2 Controllers
- Cisco Flex 7500 and Cisco 8500 Series Controllers.

To configure the AVC profile template, follow these steps:

Step 1 Choose Configuration > Features & Technologies > Controller > Application Visibility And Control > AVC Profiles.

Step 2 If you want to add a new template, hover the mouse on AVC Profiles and select New or click AVC Profiles. To modify an existing template, click the template name.

Step 3 In the AVC Profile Name text box, enter the AVC Profile Name.

Note You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application. This allows you to configure up to 32 application actions per WLAN. You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs.

Step 4 Under the AVC Rule List, click Add Row to create AVC rules.

- In the Application Name field, enter the name of the application.
- In the Application Group Name field, enter the name of the application group to which the application belongs.
- From the Action drop-down list, choose one of the following:
  - Drop—Drops the upstream and downstream packets corresponding to the chosen application.
  - Mark— Marks the upstream and downstream packets corresponding to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.
  - Rate Limit—If you select Rate Limit as an action, you can specify Average Rate Limit per client and Burst data rate limit. The number of rate limit applications is limited to 3.

The default action is to permit all applications.

- If you select Mark as an action, then choose QoS levels from the DSCP drop-down list. DSCP is a Packet header code that is used to define quality of service across the Internet. The DSCP values are mapped to the following QoS levels:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)— Provides lowest bandwidth for guest services.
  - Custom—Specify the DSCP value. The range is from 0 to 63.
- In the DSCP Value field, enter the value which can be entered only when Custom is chosen from the DSCP drop-down list.
- If you select Rate Limit as an action, you can specify the value in Avg. Rate Limit (in Kbps), which is the average bandwidth limit of that application.
- If you select Rate Limit as an action, you can specify Burst Rate Limit (in Kbps), which is the peak limit of that application

Step 5 Click Save as New Template.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure Devices to Use NetFlow

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing. This protocol collects IP traffic information from network devices to monitor traffic. The NetFlow architecture consists of the following components:

- Collector—An entity that collects all the IP traffic information from various network elements.
- Exporter—A network entity that exports the template with the IP traffic information. The controller acts as an exporter.

To create NetFlow Monitor or Exporter template:

Step 1 Choose Configuration > Templates > Features & Technologies > Controller > Netflow

Step 2 If you want to crate a new Monitor template, hover the mouse cursor over the tool tip next to the Monitor template type and click New.

Step 3 Complete the required fields and Click Save as New Template.

Step 4 If you want to crate a new Exporter template, hover the mouse cursor over the tool tip next to the Exporter template type and click New.

Step 5 Complete the required fields and Click Save as New Template.

Configure Ethernet over GRE (EoGRE) Tunnels on Controllers

Ethernet over GRE (EoGRE) enables tunneling of data traffic from Cisco WLC or Cisco AP to a mobile packet core using EoGRE tunnels.

To add or modify an EoGRE tunneling template, follow these steps:

Step 1 Choose Configuration > Features & Technologies > Controller > Tunneling > EoGRE.

Step 2 Hover your mouse cursor over the tool tip next to the template type and click New to create.

Step 3 Complete the required fields, then and click Save as New Template, specify the folder in which you want to save the template, then click Save.

Step 4 Click Deploy to save and deploy the template to the relevant controller.

Step 5 To verify the status of a template deployment, choose Administration > Dashboards > Job Dashboard.

Step 6 To modify the deployment parameters for any subsequent configuration template deployments, select a configuration job, then click Edit.

Related Topics

Add Controller Templates, on page 401
Delete Controller Templates, on page 401
Apply Controller Templates, on page 402

Configure a Lightweight AP Using Template

To configure a new Lightweight Access Point template, follow these steps:

Step 1 Choose Configuration > Templates > Lightweight Access Points.

Step 2 Choose Add Template from the Select a command drop-down list and click Go.

Step 3 Enter a template name in the text box.

Step 4 Enter a template description in the text box.

Step 5 Click Save as New Template.

Note • You can select Antenna Type only as External in Lightweight AP Templates.

Related Topics

Select the AP Source for AP Template Deployment, on page 433

Select the AP Source for AP Template Deployment

Based on the AP Source selection, the appropriate visualization is loaded on the AP Selection tab.

To select the AP Source:

Step 1 Choose Configuration > Templates > Lightweight Access Points

Step 2 Click the applicable Template Name link in the Lightweight Access Point page.

Step 3 Click the AP Source tab and select the visualization:

- Select APs Manually—If you select this option, you must select APs manually while trying to push the LWAP template configuration to the APs.
- Site Maps—If you select this option, you can select dynamic location based Site Maps for deployment of LWAP template configuration

Configure Autonomous APs Using Templates

To configure a new Autonomous Access Point template, follow these steps:

Step 1 Choose Configuration > Templates > Autonomous Access Points.

Step 2 From the Select a command drop-down list, choose Add Template.

Step 3 Click Go.

Step 4 Enter a Template Name.

Step 5 Enter the applicable CLI commands.

Do not include any show commands in the CLI commands text box. The show commands are not supported.

Step 6 Click Save.

Configure Location Information for Switches Using Templates

You can configure the location template for a switch using the Switch Location Configuration template.

To configure a location template for a switch, follow these steps:

Step 1 Choose Configuration >Templates > Switch Location.

The Switch Location Configuration template page appears.

Step 2 From the Select a command drop-down list, choose Add Template, and click Go.

Step 3 Complete the required fields in the New Template page.

Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates

When you migrate an already-managed autonomous access point to lightweight, its location and antenna information is migrated as well. You do not need to reenter the information. automatically removes the autonomous access point after migration.

The Migration Analysis option does not run during discovery by default. If you prefer to run the migration analysis during discovery, choose Administration > Settings > CLI Session to enable this option.

also supports the migration of autonomous access point to CAPWAP access point.

Choose Configuration > Templates > Autonomous AP Migrationto access this page. To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to lightweight access points. After an access point has been converted to lightweight, the previous status or configuration of the access point is not retained.

To create an autonomous AP migration template, follow these steps:

- Choose Configuration > Autonomous AP Migration
- From the Select a command drop-down list, choose Add Template, then click Go. If you are updating an already existing template, click the applicable template in the Template Name column.
- To view the migration analysis summary, choose Monitor > Tools > Autonomous AP Migration Analysis

For More Information about the field descriptions refer to Cisco Prime Infrastructure Reference Guide

Analyze the Effects of Autonomous AP Migration

To view the Migration Analysis Summary, follow these steps:

Step 1 Choose Configuration > Templates > Autonomous AP Migration.

Step 2 Choose View Migration Analysis Summary from the Select a command drop-down list, and click Go. The Migration Analysis Summary page appears.

The autonomous access points are eligible for migration only if all the criteria have a pass status. A red X designates ineligibility, and a green checkmark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version Criteria—Conversion is supported only in Cisco IOS Release 12.3(7)JA excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root

- root access point
- root fallback repeater
- root fallback shutdown
- root access point only

- Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.
- If an autonomous access point is labeled as ineligible for conversion, you can disable it.

Related Topics

Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates, on page 434

Deploy Configuration Templates

After you create a configuration template, and click Deploy. The following tables shoes specify various deployment options as shown in

Table 46: Template Deployment Options

Option	Description
Device Selection	Displays the list of devices to which you want to apply the template. By Device—List all the supported devices. By Group (Device Types)—List only the supported device groups with supported devices. By Group (Location, User Defined)—List all the device groups even if there are no supported devices. But, each group will list only the supported devices. **Note** Search for By Group option will list only the group which contains the supported devices.
Value Assignment	Allows you to specify a variable other than what was previously defined in the configuration template. Click a name, and the previously defined variables are displayed. To change any of the values, click the variable that you want to change, enter a new value, and click Apply. You can also update the variables for all selected devices. Click All Selected Devices and update variables to apply the changes on all selected devices at the same time. If you want to update variables for a particular device in the list that need not be applicable to other devices, then choose the device and update its variables. All of the other devices will continue to use the variables that were previously defined except for the device for which variables are updated. **Note** The changes that you make apply only to the specific configuration that you are deploying. To change the configuration template for all future deployments, choose Configuration > Templates > Features & Technologies and change the template.
Schedule	Allows you to create a meaningful deployment job name, then specify whether to run the job now or in the future. You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.

Option	Description

Job Option	The following job options are available:
	• Failure Policy:
	  • Ignore failure and continue—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
	  • Stop on failure—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
	• Copy Running Config to Startup—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
	• Archive Config after deploy—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Summary	Summarizes your deployment option selections.

Deployment Flow for Model-Based Configuration Templates

Note This deployment flow is not applicable for Controller based templates.

Step 1 After you create a configuration template, click Deploy. The Deployment wizard page opens.

Step 2 Select the devices on which you want to deploy the template, then click Next to choose the input values.

Step 3 In the Input Values tab, you can toggle between Form and CLI view.

Step 4 After entering the necessary configuration values, click Next or click CLI to confirm the device and template configuration values.

Step 5 Schedule the deployment job using Schedule Deployment tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

Failure Policy

- • Ignore failure and continue—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  - Stop on failure—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
  - Copy Running Config to Startup—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.

- Archive Config after deploy—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 6 Click Next to view the job deployment summary.

Step 7 On the Deployment Summary tab, you will see the CLI view for each of the device.

Step 8 Click Finish to deploy the template.

Step 9 Click Job Status in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Global Variables

The global user variables are variables which are accessible in all scripts. Each user variable must have a name that begins with gv. The name should begin with alphabets. Special characters allowed are dot appended with gv, hyphen and underscore.

You can create, delete or edit a global variable.

Step 1 Choose Configuration > Templates > Global Variable.

Step 2 From the Define Global Variable page, click Add Row.

Step 3 Specify a name, description, type and display label.

Step 4 Click Save to save the new variable.

The global variables created here can be applied while creating the CLI and Features and Technologies templates.

Related Topics

- Create a New Features and Technologies Template Using an Existing Template

Shared Policy Objects

Policy objects enable you to define logical collections of elements. They are reusable, named components that can be used by other objects and policies. They also eliminate the need to define a component each time that you define a policy.

Objects are defined globally. This means that the definition of an object is the same for every object and policy that references it. However, many object types (such as interface roles) can be overridden at the device level. This means that you can create an object that works for most of your devices, then customize the object to match the configuration of a particular device that has slightly different requirements.

To improve efficiency and accuracy in your configuration templates, you can create shared policy objects to include in your configuration templates. You create interface roles or network objects that you can add to your configuration templates.

Related Topics

Define Interface Roles, on page 438
Define Network Objects, on page 438

Create a Security Rule Parameter Map, on page 439
Create a Security Service Group, on page 439
Create a Security Zone, on page 440

Define Interface Roles

Interface roles allow you to define policies to specific interfaces on multiple devices without having to manually define the names of each interface. Interface roles can refer to any of the actual interfaces on the device, including physical interfaces, subinterfaces, and virtual interfaces such as loopback interfaces.

If you create an all-Ethernets interface role, you can define identical advanced settings for every Ethernet interface on the device with a single definition. You add this interface role to a configuration template, then deploy the template to the selected devices to configure the Ethernet interfaces.

Interface roles are especially useful when applying policies to new devices. As long as the devices that you are adding share the same interface naming scheme as existing devices, you can quickly deploy the necessary configuration template containing the interface role to the new devices.

For example, you can use interface roles to define the zones in a zone-based firewall configuration template. You might define an interface role with a naming pattern of DMZ*. When you include this interface role in a template, the configuration is applied to all interfaces whose name begins with “DMZ” on the selected devices. As a result, you can assign a policy that enables anti-spoof checking on all DMZ interfaces to all relevant device interfaces with a single action.

Step 1 Choose Configuration > Templates > Shared Policy Objects.

Step 2 In the Shared Policy Objects pane , choose Shared > Interface Role .

Step 3 From the Interface Role page, click Add Object.

Step 4 From the Add Interface Role page, create matching rules for the interface role.

When you define the zone-based template, for example, all of the interfaces on the device that match the specified rules will become members of the security zone represented by this interface role. You can match interfaces according to their name, description, type, and speed.

Step 5 Click OK to save the configurations.

Related Topics

Shared Policy Objects, on page 437

Define Network Objects

Network objects are logical collections of IP addresses or subnets that represent networks. Network objects make it easier to manage policies.

There are separate objects for IPv4 and IPv6 addresses; the IPv4 object is called “networks/hosts,” and the IPv6 object is called “network/hosts-IPv6.” Except for the address notation, these objects are functionally identical, and in many instances the name network/host applies to either type of object. Note that specific policies require the selection of one type of object over the other, depending on the type of address expected in the policy.

You can create shared policy objects to be used in the following configuration templates:

- Zone-based firewall template
- Application Visibility

Step 1 Choose Configuration > Templates > Shared Policy Objects > Shared > IPv4 Network Object .
Step 2 From the Network Object page, click Add Object and add a group of IP addresses or subnets.
Step 3 Click OK to save the configurations.

Related Topics

Shared Policy Objects, on page 437

Create a Security Rule Parameter Map

To create and use a set of parameter map objects in the firewall rules, do the following:

Step 1 Choose Configuration > Templates > Shared Policy Objects.
Step 2 In the Shared Policy Objects pane , choose Shared > Security Rule Parameter Map .
Step 3 From the Security Rule Parameter Map page, click Add Object.
Step 4 Specify a name and description for the parameter map that is being created.
Step 5 From the parameters list, select the parameters you want to apply and provide a value for each of them.
Step 6 To specify Device Level Override, choose Device Level Override > Add Device .
Step 7 Select the device you wish to add, and click OK.
Step 8 Click OK to save the configurations.

Related Topics

Shared Policy Objects, on page 437

Create a Security Service Group

To create and use a set of parameter map objects in the firewall rules, do the following:

Step 1 Choose Configuration > Templates > Shared Policy Objects.
Step 2 In the Shared Policy Objects pane , choose Shared > Security Service .
Step 3 From the Security Service page, click Add Object.
Step 4 Specify a name and description for the service that is being created.
Step 5 Select the service data from the available list. If you select TCP or UDP, provide a list of port numbers or port ranges (separated by comma).
Step 6 To specify Device Level Override, choose Device Level Override > Add Device.
Step 7 Select the device you wish to add, and click OK.
Step 8 Click OK to save the configurations.

Related Topics

Shared Policy Objects, on page 437

Create a Security Zone

Step 1 Choose Configuration > Templates > Shared Policy Objects.
Step 2 In the Shared Policy Objects pane , choose Shared > Security Zone.
Step 3 From the Security Zone page, click Add Object.
Step 4 Specify a name and description for the security zone that is being created.
Step 5 Specify a set of rules that defines the interfaces that must be attached to the zone.
Step 6 To specify Device Level Override, choose Device Level Override > Add Device .
Step 7 Select the device you wish to add, and click OK.
Step 8 Click OK to save the configurations.

Related Topics

Shared Policy Objects, on page 437

What are Configuration Groups

You might want to associate a set of configuration templates with specific devices. If you have devices that require the same configuration, you can create a configuration group that associates configuration templates with devices. Creating a configuration group allows you to quickly apply new templates without remembering to which devices the new templates should be deployed.

Composite templates allow you to group smaller templates together, but only configuration groups specify the relationship between the templates and the groups of devices to which those templates apply. You can also specify the order in which the templates in the configuration group are deployed to the devices.

Before you create a configuration group, you should:

- Create configuration templates for the devices in your configuration group.
- Determine which devices should be included in the configuration group.

Related Topics

- Create a New Features and Technologies Template Using an Existing Template
- Apply Changes to Groups of NEs Using User Defined Groups

Apply Changes to Groups of NEs Using User Defined Groups

Step 1 Choose Configuration > Templates > Configuration Groups.
Step 2 Complete the required fields. The device types displayed depend on what you select from the Device Type field.
Step 3 Where needed, change a template's order in the group by selecting it and clicking the up or down arrow.
Step 4 Click Save as a New Configuration Group. The possible configuration groups are:

- Success—Indicates that a configuration group has been successfully created.
- Pending—One or more devices in the configuration group have changes that have not yet been deployed. For example, if you add a new device to the configuration group, the status of the new device is Pending. If you modify a configuration template to which the configuration group is associated, all devices in the configuration group have the status Pending.
- Scheduled—Indicates that a configuration group deployment is scheduled. When a configuration group is Scheduled, any devices in the group that are Pending or Failed are changed to Scheduled. If a device is Deployed, it remains Deployed and its status does not change to Scheduled.
- Failure—Deployment has failed for one or more devices in the configuration group.

Related Topics

Create a New Features and Technologies Template Using an Existing Template, on page 385
What are Configuration Groups, on page 440

What is a WLAN Controller Configuration Group

By creating a configuration group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all of the controllers in a group. You can add, delete, or remove configuration groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected configuration groups. You can also save the current configuration to nonvolatile (flash) memory to controllers in selected configuration groups.

Note A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes that controller from any other mobility group to which it is already a member.

By choosing Configuration > Templates > WLAN Controller Configuration Groups, you can view a summary of all configuration groups in the database. Choose Add Configuration Groups from the Select a command drop-down list to display a table with the following columns:

- Group Name—Name of the configuration group.
- Templates—Number of templates applied to the configuration group.

Related Topics

- Create Controller Configuration Groups and Apply Configuration Templates to them

Create Controller Configuration Groups and Apply Configuration Templates to them

To create a configuration group, follow these steps:

Step 1 Choose Configuration > Templates > WLAN Controller Configuration Groups.

Step 2 Fromthe Select a command drop-down list, choose Add Config Group, then click Go.

Step 3 Enter the new configuration group name. It must be unique across all groups.

- If Enable Background Audit is selected, the network and controller audits occur for this configuration group.
- If Enable Enforcement is selected, the templates are automatically applied during the audit if any discrepancies are found.

Step 4 Other templates created in can be assigned to a configuration group. The same WLAN template can be assigned to more than one configuration group. Choose from the following:

- Select and add later—Click to add a template at a later time.
- Copy templates from a controller—Click to copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new configuration group. Only the templates are copied.

Note The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.

Step 5 Click Save. The Configuration Groups page appears.

- After you create a configuration group, allows you to choose and configure multiple controllers by choosing the template that you want to push to the group of controllers.
- General—Allows you to enable mobility group.
- To enable the Background Audit option, set template-based audit in Administration > System > Audit Settings.
- Controllers
- Country/DCA
- Templates—Allows you to select the configuration templates that you have already created.
- Apply/Schedule
- Audit
- Reboot
- Report—Allows you to view the most recent report for this group.

Related Topics

What is a WLAN Controller Configuration Group, on page 441
Add or Remove Controllers from Controller Configuration Groups, on page 442
Set DCA Channels for a Controller Configuration Group, on page 443
Schedule the Deployment of Templates to a Controller Configuration Group, on page 444
Audit Controller Configuration Groups to Ensure Compliance, on page 444
Reboot Configuration Groups, on page 445
View the Status of Template Deployments to Controller Configuration Groups, on page 445

Add or Remove Controllers from Controller Configuration Groups

To add or remove controllers from a configuration group, follow these steps:

Step 1 Choose Configuration > Templates > WLAN Controller Configuration Groups.

Step 2 Click a group name in the Group Name column, then click the Audit tab.

The columns in the table display the IP address of the controller, the configuration group name the controller belongs to, and the mobility group name of the controller.

Step 3 Click to highlight the row of the controller that you want to add to the group, then click Add.

Step 4 To remove a controller from the group, highlight the controller in the Group Controllers area and click Remove.

Step 5 Click the Apply/Schedule tab, click Apply to add or remove the controllers to the configuration groups, then click Save Selection.

Related Topics

What is a WLAN Controller Configuration Group, on page 441
Set DCA Channels for a Controller Configuration Group, on page 443
Schedule the Deployment of Templates to a Controller Configuration Group, on page 444
Audit Controller Configuration Groups to Ensure Compliance, on page 444
View the Status of Template Deployments to Controller Configuration Groups, on page 445

Set DCA Channels for a Controller Configuration Group

You can configure one or more countries on a controller. After countries are configured on a controller, the corresponding 802.11a/n DCA channels are available for selection. At least one DCA channel must be selected for the 802.11a/n network. When the country codes are changed, the DCA channels are automatically changed in coordination.

Note 802.11a/n and 802.11b/n networks for controllers and access points must be disabled before configuring a country on a controller. To disable 802.11a/n or 802.11b/n networks, choose Configure > Controllers, select the desired controller that you want to disable, choose 802.11a/n or 802.11b/g/n from the left sidebar menu, and then choose Parameters. The Network Status is the first check box.

To add multiple controllers that are defined in a configuration group and then set the DCA channels, follow these steps:

Step 1 Choose Configuration > Templates > WLAN Controller Configuration Groups.

Step 2 From the Select a command drop-down list, choose Add Config Groups, then click Go.

Step 3 Create a configuration group by entering the group name and mobility group name.

Step 4 Click Save, then click the Controllers tab.

Step 5 Highlight the controllers that you want to add, and click Add. The controller is added to the Group Controllers page.

Step 6 Click the Country/DCA tab. The Country/DCA page appears. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Step 7 Select the Update Country/DCA check box to display a list of countries from which to choose.

Step 8 Those DCA channels that are currently configured on the controller for the same mobility group are displayed in the Select Country Codes page. The corresponding 802.11a/n and 802.11b/n allowable channels for the chosen country is displayed as well. You can add or delete any channels in the list by selecting or deselecting the channel and clicking Save Selection.

A minimum of 1 and a maximum of 20 countries can be configured for a controller.

Related Topics

What is a WLAN Controller Configuration Group, on page 441
Schedule the Deployment of Templates to a Controller Configuration Group, on page 444

Audit Controller Configuration Groups to Ensure Compliance, on page 444
View the Status of Template Deployments to Controller Configuration Groups, on page 445

Schedule the Deployment of Templates to a Controller Configuration Group

The scheduling function allows you to schedule a start day and time for provisioning.

To apply the mobility groups, mobility members, and templates to all of the controllers in a configuration group, follow these steps:

Step 1 Choose Configuration > Templates > WLAN Controller Configuration Groups.

Step 2 Click a group name in the Group Name column, then choose the Apply/Schedule tab.

Step 3 Click Apply to start the provisioning of mobility groups, mobility members, and templates to all of the controllers in the configuration group. After you apply, you can leave this page or log out of The process continues, and you can return later to this page to view a report.

Note Do not perform any other confi1guration group functions during the provisioning process.

A report is generated and appears in the Recent Apply Report page. It shows which mobility groups, mobility members, or templates were successfully applied to each of the controllers.

Step 4 Enter a starting date in the text box or use the calendar icon to choose a start date.

Step 5 Choose the starting time using the hours and minutes drop-down lists.

Step 6 Click Schedule to start the provisioning at the scheduled time.

Related Topics

What is a WLAN Controller Configuration Group, on page 441
Add or Remove Controllers from Controller Configuration Groups, on page 442
Set DCA Channels for a Controller Configuration Group, on page 443
View the Status of Template Deployments to Controller Configuration Groups, on page 445

Audit Controller Configuration Groups to Ensure Compliance

The Configuration Groups Audit page allows you to verify if the configuration complies of the controller with the group templates and mobility group. During the audit, you can leave this window or log out of . The process continues, and you can return to this page later to view a report.

Do not perform any other configuration group functions during the audit verification.

To perform a configuration group audit, follow these steps:

Step 1 Choose Configuration > Templates > WLAN Controller Configuration Groups.

Step 2 Click a group name in the Group Name column, then click the Audit tab.

Step 3 Click to highlight a controller on the Controllers tab, choose >> (Add), and Save Selection.

Step 4 Click to highlight a template on the Templates tab, choose >> (Add), and Save Selection.

Step 5 Click Audit to begin the auditing process.

A report is generated and the current configuration on each controller is compared with that in the configuration group templates. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

This audit does not enforce configuration to the device. It only identifies the discrepancies.

Step 6 Click Details to view the Controller Audit report details.

Step 7 Double-click a line item to open the Attribute Differences page. This page displays the attribute, its value in , and its value in the controller.

Step 8 Click Retain Prime Infrastructure Value to push all attributes in the Attribute Differences page to the device.

Step 9 Click Close to return to the Controller Audit Report page.

Related Topics

What is a WLAN Controller Configuration Group, on page 441
Add or Remove Controllers from Controller Configuration Groups, on page 442
Schedule the Deployment of Templates to a Controller Configuration Group, on page 444
View the Status of Template Deployments to Controller Configuration Groups, on page 445

Reboot Configuration Groups

Step 1 Choose Configuration > Templates > WLAN Controller Configuration Groups.

Step 2 Click a group name in the Group Name column, then click the Reboot tab.

Step 3 Select the Cascade Reboot check box if you want to reboot one controller at a time, waiting for that controller to come up before rebooting the next controller.

Step 4 Click Reboot to reboot all controllers in the configuration group at the same time. During the reboot, you can leave this page or log out of . The process continues, and you can return later to this page and view a report.

The Recent Reboot Report page shows when each controller was rebooted and what the controller status is after the reboot. If is unable to reboot the controller, a failure is shown.

View the Status of Template Deployments to Controller Configuration Groups

To display all recently applied reports under a specified group name, follow these steps:

Step 1 Choose Configuration > Templates > WLAN Controller Configuration Groups.

Step 2 Click a group name in the Group Name column, then click the Report tab. The Recent Apply Report page displays all recently applied reports including the apply status, the date and time the apply was initiated, and the number of templates. The following information is provided for each individual IP address:

- Apply Status—Indicates success, partial success, failure, or not initiated.
- Successful Templates—Indicates the number of successful templates associated with the applicable IP address.
- Failures—Indicates the number of failures with the provisioning of mobility group, mobility members, and templates to the applicable controller.
- Details—Click Details to view the individual failures and associated error messages.

Step 3 To view the scheduled task reports, click the click here link at the bottom of the page.

Related Topics

What is a WLAN Controller Configuration Group, on page 441
Add or Remove Controllers from Controller Configuration Groups, on page 442
Set DCA Channels for a Controller Configuration Group, on page 443
Schedule the Deployment of Templates to a Controller Configuration Group, on page 444

Create Wireless Configuration Templates

The following sections describe how to create wireless configuration templates for:

- Lightweight access points
- Autonomous access points
- Switches
- Converting autonomous access points to lightweight access points

Related Topics

- Configure Lightweight APs Using Configuration Templates
- Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates
- Configure Location Information for Switches Using Templates

Configure Lightweight APs Using Configuration Templates

To create a template for a lightweight access point, follow these steps:

Step 1 Choose Configuration > Templates > Lightweight Access Points.

Step 2 From the Select a command drop-down list, choose Add Template, then click Go.

Step 3 Enter a name and description for the template and click Save. If you are updating an already existing template, click the applicable template in the Template Name column.

Step 4 Click each of the tabs and complete the required fields.

Related Topics

Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates, on page 434

Configure Device - Based Policies for APs

Use the Policy Configuration Templates page to configure device-based policies on a controller. You can configure policies for a user or a device on the network.

The maximum number of policies that you can configure is 64. Policies are not applied on WLANs and AP groups if AAA override is configured on the controller.

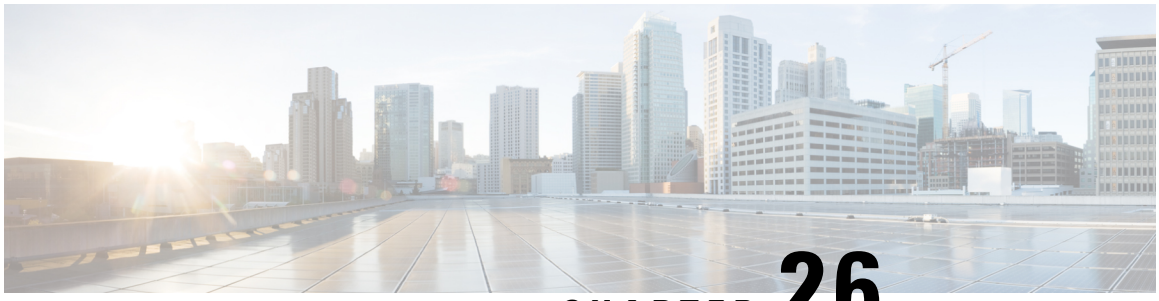
Step 1 Choose Configuration > Templates > Features and Technologies.

Step 2 From the left sidebar menu, choose Features and Technologies > Controller > WLANs > Policy Configuration. The Policy Configuration Template page displays.

Step 3 Complete the following fields:

- Name—Name of the policy template
- Description—Description of the policy template.
- Tags—Search keywords applicable to this template.
- Device Type (validation criteria)—The device product family, series or type used to validate the template (CUWN, for Cisco Unified Wireless Network, is the default).
- Policy Name—Name of the policy.
- Policy Role—The user type or the user group the user belongs to. For example, student, employee.
- EAP Type—EAP authentication method used by the client. The available types are as follows:
  - LEAP
  - EAP-FAST
  - EAP-TLS
  - PEAP
- Device Type—Choose the device type to which this policy applies (e.g., Apple Laptop).
- VLAN ID—VLAN associated with the policy.
- IPv4 ACL—Choose an IPv4 ACL for the policy from the list
- QoS—Choose the policy's Quality of Service level from the list. You can choose one of the follows:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)— Provides the lowest bandwidth for guest services.
- Session Timeout—Maximum amount of time, in seconds, before a client is forced to re-authenticate. The default value is 0 seconds.
- Sleeping Client Timeout—Maximum amount of time, in hours, before a guest client is forced to re-authenticate. The default value is 12 hours. The range is from 1 to 720 hours.

Step 4 When you are finished, click Save as new template.



CHAPTER 26

Configure Wireless Devices

View All Controllers in

You can view a summary of all controllers in the database.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 To use the command buttons at the top of the page, select the check box next to one or more controllers. The following table describes the field available in this page.

Table 47: Wireless Controller Summary Information

Field	Description
Admin Status	Administration status of the wireless controller.
DNS Name	DNS name of the wireless controller.
Last Inventory Collection Status	Status of the last inventory collection.
Last Successful Collection Time	Last successful collection time.
Client Count	Displays the total number of clients currently associated with the controller
Software Type	Displays the software type of all managed devices.
Location	Displays the location information .
Device Name	Name of the controller. Click on a device name to view device details, configure the controller, apply templates, view and schedule configuration archives, and view and update the controller software image.
Reachability	Reachability status is updated based on the last execution information of the Device Status background task.
IP Address/DNS	Local network IP address of the controller management interface. Click the icon under the IP address to launch the controller web user interface in a new browser window.
Device Type	Based on the series, device types are grouped. For example: • WLC2100—21xx Series Wireless LAN Controllers • 2500—25xx Series Wireless LAN Controllers • 4400—44xx Series Wireless LAN Controllers • 5500—55xx Series Wireless LAN Controllers • 7500—75xx Series Wireless LAN Controllers • WiSM—WiSM (slot number, port number) • WiSM2—WiSM2 (slot number, port number)
AP Discovery Status	Indicates whether the AP discovery has completed.
Software Version	The operating system release. version. dot. maintenance number of the code currently running on the controller.
Mobility Group Name	Name of the mobility or WPS group.

Step 3 To view specific information about a controller, click on a Device Name.

Related Topics

Controller-Specific Commands for Configuration Template Deployments, on page 452

Controller-Specific Commands for Configuration Template Deployments

When you choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller and select the checkbox next to one or more devices, the following buttons appear at the top of the page:

- Delete—Allows you to delete a controller.
- Edit—Allows you to edit general parameters, SNMP parameters, Telnet/SSH parameters, HTTP parameters, and IPSec parameters.
- Sync—
- Groups & Sites—Allows you to add and remove controllers from location groups and sites.
- Reboot—Enables you to confirm the restart of your controller after saving configuration changes. You can select these reboot options:
  - Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
  - Reboot APs
  - Swap AP Image
- Download—Allows you to select the following options to download software to controllers.
  - Download Software—Choose from TFTP, FTP, SFTP to download software to the selected controller or all controllers in the selected groups after you have a configuration group established.
  - Download IDS Signatures
  - Download Customized Web Auth
  - Download Vendor Device Certificate
  - Download Vendor CA Certificate
  - Bulk Update Controllers
- Configure
  - Save Config to Flash
  - Discover Templates from Controller
  - emplates Applied to Controller
  - Audit Now
  - Update Credentials

Related Topics

View All Controllers in , on page 450
Check Which Configuration Templates Are Used by Controllers and Remove the Associations, on page 453

Change Controller Credentials Using an Imported CSV File, on page 455
Apply Controller Changes By Rebooting, on page 455
Download Software to Controllers, on page 456

Check Which Configuration Templates Are Used by Controllers and Remove the Associations

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click Configure > Audit Now.

Step 4 Click OK in the pop-up dialog box to remove the template associations from configuration objects in the database as well as template associations for this controller from associated configuration groups (This is a template-based audit only).

You can specify for which configurations you want to have associated templates.

The templates that are discovered do not retrieve management, local, or guest user passwords.

The following rules apply for template discovery:

- Template Discovery discovers templates that are not found in .
- Existing templates are not discovered.
- Template Discovery does not retrieve dynamic interface configurations for a controller. You must create a new template to apply the dynamic interface configurations on a controller.

Related Topics

View Controller Audit Results in a Report, on page 454
View Templates That Have Been Applied to Controllers, on page 461
Discover Existing Templates for Controllers, on page 461
Apply Controller Changes By Rebooting, on page 455
Download Software to Controllers, on page 456
Replacing Controllers While Retaining the IP Address, on page 462

Change Controller Credentials from the Network Devices Table

To update SNMP and Telnet credentials, you must do so on each controller. You cannot update SNMP/Telnet credential details for multiple controllers at the same time.

SNMP write access parameters are needed for modifying controller configuration. With read-only access parameters, configuration can be displayed only and not modified.

To update the SNMP/Telnet credentials, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click Configure > Update Credentials.

Step 4 Complete the required fields, then click OK.

Related Topics

Change Controller Credentials Using an Imported CSV File, on page 455

View Controller Audit Results in a Report

After you perform an audit on a controller, the Audit Report displays the following information:

- Device Name
- Time of Audit
- Audit Status
- Applied and Config Group Template Discrepancies information including the following:
  - Template type (template name)
  - Template application method
  - Audit status (For example, mismatch, identical)
  - Template attribute
  - Value in
  - Value in Controller
  - Other Discrepancies including the following:
  - Configuration type (name)
  - Audit Status (For example, mismatch, identical)
  - Attribute
  - Value in Controller
  - Total enforcements for configuration groups with background audit enabled. If discrepancies are found during the audit in regards to the configuration groups enabled for background audit, and if the enforcement is enabled, this section lists the enforcements made during the controller audit. If the total enforcement count is greater than zero, this number appears as a link. Click the link to view a list of the enforcements made from .
- Failed Enforcements for Configuration Groups with background audit enabled—If the failed enforcement count is greater than zero, this number appears as a link. Click the link to view a list of failure details (including the reason for the failure) returned by the device.
- Restore Values to Controller or Refresh Configuration from Controller—If there are configuration differences found as a result of the audit, you can either click Restore Prime Infrastructure Values to controller or Refresh Config from controller to bring configuration in sync with the controller.
  - Choose Restore Prime Infrastructure Values to Controller to push the discrepancies to the device.

Related Topics

Check Which Configuration Templates Are Used by Controllers and Remove the Associations, on page 453

Change Controller Credentials Using an Imported CSV File

You can update multiple controllers credentials by importing a CSV file.

To update controller(s) information in bulk, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, select Wireless Controllers.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click Download > Bulk Update Controllers.

Step 4 Enter the CSV filename in the Select CSV File text box or click Browse to locate the desired file.

Step 5 Click Update and Sync.

Related Topics

Change Controller Credentials from the Network Devices Table, on page 453
Apply Controller Changes By Rebooting, on page 455
Replacing Controllers While Retaining the IP Address, on page 462

Apply Controller Changes By Rebooting

You should save the current controller configuration prior to rebooting. To reboot a controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, select Wireless Controllers, then click Reboot > Reboot Controllers.

Step 2 Select the required Reboot Controller option:

- Save Config to Flash—Data is saved to the controller in non-volatile RAM (NVRAM) and is preserved in the event of a power cycle. If the controller is rebooted, all applied changes are lost unless the configuration has been saved.
- Reboot APs—Select the check box to enable a reboot of the access point after making any other updates.
- Swap AP Image—Indicates whether or not to reboot controllers and APs by swapping AP images. This could be either Yes or No.

Step 3 Click OK.

Related Topics

Change Controller Credentials from the Network Devices Table, on page 453
Replacing Controllers While Retaining the IP Address, on page 462

Download Software to Controllers

To download software to a controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controllers.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click Download and select one of the following options:

- Download Software TFTP
- Download Software FTP
- Download Software SFTP

Step 4 Complete the required fields.

Step 5 Select the download type. The pre-download option is displayed only when all selected controllers are using Release 7.0.x.x or later.

- Now—Executes the download software operation immediately. If you select this option, proceed with Step 7.
- Scheduled—Specify the scheduled download options.
  - Schedule download to controller—Select this check box to schedule download software to controller.
  - Pre-download software to APs—Select this check box to schedule the pre-download software to APs. The APs download the image and then reboot when the controller reboots. To see Image Predownload status per AP, enable the task in the Administration > Dashboards > Job Dashboard > System Jobs > Wireless Poller > AP Image Pre-Download Status, and run an AP Image Predownload report from the Report Launch Pad.
  - FlexConnect AP Upgrade—Select this option to enable one access point of each model in the local network to download the image. The remaining access points will then download the image from the primary access point using the pre-image download feature over the local network, which reduces the WAN latency.

Step 6 Select the Schedule options.

Schedule enough time (at least 30 minutes) between Download and Reboot so that all APs can complete the software pre-download. If any AP is in pre-download progress state at the time of the scheduled reboot, the controller will not reboot. You must wait for the pre-download to finish for all the APs, and then reboot the controller manually.

Step 7 Enter the FTP credentials including username, password, and port.

You can use special characters such as @, #, ^, *, ~, _, -, +, =, {, }, [,], :, ., and / in the password. You cannot use special characters such as $, ', \, %, &, (,), ;, ", <, >, , , ? , and | as part of the FTP password. The special character "!" (exclamation mark) works when the password policy is disabled.

Step 8 Select whether the file is located on the Local machine or an FTP Server. If you select FTP Server, the software files are uploaded to the FTP directory specified during the installation.

Step 9 Click Download.

If the transfer times out, choose the FTP server option in the File is located on field; the server filename is populated and retries the operation.

Upload Controller Configuration and Log Files to an FTP/TFTP Server

You can upload a controller system configuration to the specified TFP or TFTP server as a file. Both File FTP and TFTP are supported for uploading and downloading files to and from . To upload files from a controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 From the left sidebar menu, choose System > Commands.

Step 4 Select the FTP or TFTP radio button, then select Upload File from Controller and click Go.

Step 5 Complete the required fields.

uses an integral TFTP and FTP server. This means that third-party TFTP and FTP servers cannot run on the same workstation as because and the third-party servers use the same communication port.

Step 6 Click OK. The selected file is uploaded to your TFTP or FTP server and named what you entered in the File Name text box.

Download IDS Signatures to Controllers

can download Intrusion Detection System (IDS) signature files to a controller. If you specify to download the IDS signature file from a local machine, initiates a two-step operation:

1. The local file is copied from the administrator workstation to built-in TFTP server.
2. The controller retrieves that file.

If the IDS signature file is already in the server's TFTP directory, the downloaded web page automatically populates the filename.

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click Download > Download IDS Signatures.

Step 4 Complete the required fields.

Step 5 Click Download.

If the transfer times out, choose the FTP server option in the File is located on field; the server filename is populated and retries the operation.

Related Topics

View All Controllers in , on page 450
Apply Controller Changes By Rebooting, on page 455
Download Software to Controllers, on page 456
Replacing Controllers While Retaining the IP Address, on page 462

Download Compressed Web Authorization Login Page Information to Controllers

You can compress the page and image files used for displaying a web authentication login page, known as webauth bundles, and download the file to a controller.

Controllers accept a .tar or .zip file of up to 1 MB in size. The 1 MB limit includes the total size of uncompressed files in the bundle.

To download customized web authentication bundles to a controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click Download > Download Customized WebAuth.

Step 4 To download an example login.tar bundle file, click on the preview image displayed, then edit the login.html file and save it as a .tar or .zip file. The file contains the pages and image files required for the web authentication display.

Step 5 Download the .tar or .zip file to the controller.

Step 6 Select where the file is located.

If you select local machine, you can upload either a .zip or .tar file type. converts .zip files to .tar files. If you choose a TFTP server download, you can specify a .tar files only.

Step 7 Complete the required fields, then click Download.

If the transfer times out, choose the FTP server option in the File is located on field; the server filename is populated and retries the operation.

After completes the download, you are directed to a new page and are able to authenticate.

Related Topics

View All Controllers in , on page 450
Download Software to Controllers, on page 456
Replacing Controllers While Retaining the IP Address, on page 462

Download Vendor Device Certificates to Controllers

Each wireless device (controller, access point, and client) has its own device certificate. If you want to use your own vendor-specific device certificate, you must download it to the controller.

To download a vendor device certificate to a controller, follow these steps:

Procedure

	Command or Action	Purpose
Step 1	Choose Inventory > Device Management > Network Devices.	
Step 2	Choose Device Type > Wireless Controller (expand Wireless Controller to select a specific controller series).	
Step 3	Click the Device Name of the desired controller.	
Step 4	Click Configuration tab.	
Step 5	Choose System > Commands.	
Step 6	In theUpload/Download Commands are, select the transfer protocol.	
Step 7	Select the certificate you want to install and click Go.	
Step 8	Fill in the requisite details and click OK.	

Related Topics

Download Software to Controllers, on page 456
Replacing Controllers While Retaining the IP Address, on page 462
Download CA Certificates to Controllers, on page 459

Download Vendor Device Certificates to Controllers through TFTP

To download a vendor device certificate via TFTP only, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click Download > Download Vendor Device Certificate.
Step 4 Complete the required fields, then click Download.

Download CA Certificates to Controllers

Controllers and access points have a certificate authority (CA) certificate that is used to sign and validate device certificates. The controller is shipped with a Cisco-installed CA certificate. This certificate might be used by EAP-TLS and EAP-FAST (when not using PACs) to authenticate wireless clients during local EAP

authentication. However, if you want to use your own vendor-specific CA certificate, you must download it to the controller.

To download a vendor CA certificate to the controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click Download > Download Vendor Device Certificate.
Step 4 Complete the required fields, then click Download.

Related Topics

Apply Controller Changes By Rebooting, on page 455
Download Software to Controllers, on page 456
Replacing Controllers While Retaining the IP Address, on page 462
View All Controllers in , on page 450

Save Controller Configuration to Device Flash

To save the configuration to flash memory, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click Configure > Save Config to Flash.

Related Topics

Save Controller Configurations to the Database (Sync), on page 460
Download Software to Controllers, on page 456
Replacing Controllers While Retaining the IP Address, on page 462
Apply Controller Changes By Rebooting, on page 455

Save Controller Configurations to the Database (Sync)

To synchronize the configuration from the controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Select the check box(es) of the applicable controller(s).
Step 3 Click Sync, and Yes to proceed.

Related Topics

Save Controller Configuration to Device Flash, on page 460
Download Software to Controllers, on page 456
Replacing Controllers While Retaining the IP Address, on page 462
Apply Controller Changes By Rebooting, on page 455

Discover Existing Templates for Controllers

To discover current templates, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click Configure > Discover Templates from Controller.

The Discover Templates page displays the number of discovered templates, each template type and each template name. The template discovery tool discovers all features that support templates and are discoverable in Cisco WLC.

Step 4 Select the Enabling this option will create association between discovered templates and the device listed above check box so that discovered templates are associated to the configuration on the device and are shown as applied on that controller.

The template discovery refreshes the configuration from the controller prior to discovering templates.

Step 5 Click OK in the warning dialog box to continue with the discovery.

For the TACACS+ Server templates, the configuration on the controller with same server IP address and port number but different server types are aggregated into one single template with the corresponding Server Types set on the Discovered Template. For the TACACS+ Server templates, the Admin Status on the discovered template reflects the value of Admin Status on the first configuration from the controller with same Server IP address and port number.

View Templates That Have Been Applied to Controllers

You can view all templates currently applied to a specific controller. displays templates applied in the partition only.

To view applied templates, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Select the check box(es) of the applicable controller(s).

Step 3 Click Configure > Templates Applied to a Controller.

The page displays each applied template name, template type, the date the template was last saved, and the date the template was last applied.

Step 4 Click the template name link to view the template details. See Check Which Configuration Templates Are Used by Controllers and Remove the Associations for more information.

Related Topics

Check Which Configuration Templates Are Used by Controllers and Remove the Associations, on page 453
Replacing Controllers While Retaining the IP Address, on page 462

Replacing Controllers While Retaining the IP Address

When you want to replace an old controller model with a new one without changing the IP address, do the following:

1. Delete the old controller from and wait for the confirmation that the device was deleted.
2. Replace the controller with the new model in the setup with same IP address.
3. Re-add the IP address to .

Related Topics

Edit Device Parameters, on page 41

Modify Controller Properties

To change controller properties such as the device name, location, SNMP parameters, or Telnet/SSH parameters, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Select a wireless controller, then click Edit.

Step 3 Modify the fields as desired, then click one of the following buttons:

- Update
- Update & Sync
- Verify Credentials
- Cancel to return to the previous or default settings.

Change Controller General System Properties from the Network Devices Table

To view the general system parameters for a current controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 From the left sidebar menu, choose System > General - System. The general system parameters appear. See Cisco Prime Infrastructure Reference Guide.

Step 4 Make the required changes, then click Save.

Assign Priority to APs When a Controller Fails

When a controller fails, the backup controller configured for the access point suddenly receives a number of Discovery and Join requests. If the controller becomes overloaded, it might reject some of the access points.

By assigning failover priority to an access point, you have some control over which access points are rejected. When the backup controller is overloaded, join requests of access points configured with a higher priority levels take precedence over lower-priority access points.

To configure failover priority settings for access points, you must first enable the AP Failover Priority feature.

To enable the AP Failover Priority feature, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 From the left sidebar menu, choose General - System.

Step 4 From the AP Failover Priority drop-down list, choose Enabled.

Step 5 To configure an access point failover priority, do the following:

a) Choose Configuration > Network > Network Devices, then select an AP Name.

b) From the AP Failover Priority drop-down list, choose the applicable priority (Low, Medium, High, Critical). The default priority is Low.

Configure 802.3 Bridging on a Controller

The controller supports 802.3 frames and applications that use them, such as those typically used for cash registers and cash register servers. However, to make these applications work with the controller, the 802.3 frames must be bridged on the controller.

Support for raw 802.3 frames allows the controller to bridge non-IP frames for applications not running over IP. Only this raw 802.3 frame format is currently supported.

To configure 802.3 bridging using , follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 Choose System > General - System to access the General page.

Step 4 From the 802.3 Bridging drop-down list, choose Enable to enable 802.3 bridging on your controller or Disable to disable this feature. The default value is Disable.

Step 5 Click Save to confirm your changes.

Configure 802.3 Flow Control on a Controller

Flow control is a technique for ensuring that a transmitting entity, such as a modem, does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed.

By default, flow control is disabled. You can only enable a Cisco switch to receive PAUSE frames but not to send them.

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 Choose System > General - System to access the General page.

Step 4 Click Enable in the 802.3x Flow Control field.

Configure Lightweight AP Protocol Transport Mode from the Network Devices Table

Lightweight Access Point Protocol transport mode indicates the communications layer between controllers and access points. Cisco IOS-based lightweight access points do not support Layer 2 lightweight access point mode. These access points can only be run with Layer 3.

To convert a Cisco Unified Wireless Network Solution from Layer 3 to Layer 2 lightweight access point transport mode using user interface, follow these steps. This procedure causes your access points to go offline until the controller reboots and the associated access points re associate to the controller.

Step 1 Make sure that all controllers and access points are on the same subnet.

You must configure the controllers and associated access points to operate in Layer 2 mode before completing the conversion.

Step 2 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 3 Click a Device Name, click the Configuration tab, then choose System > General - System to access the General page.

a) Change lightweight access point transport mode to Layer2 and click Save.

b) If displays the following message, click OK:

Example:

```
Please reboot the system for the CAPWAP Mode change to take effect.
```

Step 4 Select the controller, then click Reboot > Reboot Controllers.

Step 5 Select the Save Config to Flash option.

Step 6 After the controller reboots, follow these steps to verify that the CAPWAP transport mode is now Layer 2:

a) Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
b) Click the device name of the applicable controller.
c) Verify that the current CAPWAP transport mode is Layer2 from the System > General - System page.

You have completed the CAPWAP transport mode conversion from Layer 3 to Layer 2. The operating system software now controls all communications between controllers and access points on the same subnet.

What is Aggressive Load Balancing?

In routing, load balancing refers to the capability of a router to distribute traffic over all its network ports that are the same distance from the destination address. Good load-balancing algorithms use both line speed and reliability information. Load balancing increases the use of network segments, thus increasing effective network bandwidth.

Aggressive load balancing actively balances the load between the mobile clients and their associated access points.

What is Link Aggregation?

Link aggregation allows you to reduce the number of IP addresses needed to configure the ports on your controller by grouping all the physical ports and creating a link aggregation group (LAG). In a 4402 model, two ports are combined to form a LAG whereas in a 4404 model, all four ports are combined to form a LAG.

You cannot create more than one LAG on a controller.

If LAG is enabled on a controller, the following configuration changes occur:

- Any dynamic interfaces that you have created are deleted in order to prevent configuration inconsistencies in the interface database.
- Interfaces cannot be created with the “Dynamic AP Manager” flag set.

The advantages of creating a LAG include the following:

- Assurance that, if one of the links goes down, the traffic is moved to the other links in the LAG. As long as one of the physical ports is working, the system remains functional.
- You do not need to configure separate backup ports for each interface.
- Multiple AP-manager interfaces are not required because only one logical port is visible to the application.

When you make changes to the LAG configuration, the controller has to be rebooted for the changes to take effect.

Prerequisites for Wireless Management

Because of IPsec operation, management via wireless is only available to operators logging in across WPA, Static WEP, or VPN Pass Through WLANs. Wireless management is not available to clients attempting to log in via an IPsec WLAN.

What is a Mobility Anchor Keep Alive Interval?

You can specify the delay between tries for clients attempting to join another access point. This decreases the time it takes for a client to join another access point following a controller failure because the failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

Related Topics

Download Software to Controllers, on page 456
Restore Controller Factory Default Settings, on page 466
Configure the Date and Time on a Controller, on page 466

Restore Controller Factory Default Settings

You can reset the controller configuration to the factory default. This overwrites all applied and saved configuration parameters. You are prompted for confirmation to reinitialize your controller.

All configuration data files are deleted, and upon reboot, the controller is restored to its original non-configured state. This removes all IP configuration, and you need a serial connection to restore its base configuration.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 From the left sidebar menu, choose System > Commands , and from the Administrative Commands drop-down list, choose Reset to Factory Default, and click Go to access this page.

Step 4 After confirming configuration removal, you must reboot the controller and select the Reboot Without Saving option.

Related Topics

Download Software to Controllers, on page 456
Configure the Date and Time on a Controller, on page 466
Apply Controller Changes By Rebooting, on page 455

Configure the Date and Time on a Controller

You can manually set the current time and date on the controller.

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 From the left sidebar menu, choose System > Commands, and from the Configuration Commands drop-down list choose Set System Time, and click Go.

Step 4 Modify the required parameters:

- Current Time—Shows the time currently being used by the system.
- Month/Day/Year—Choose the month/day/year from the drop-down list.
- Hour/Minutes/Seconds—Choose the hour/minutes/seconds from the drop-down list.

- Delta (hours)—Enter the positive or negative hour offset from GMT (Greenwich Mean Time).
- Delta (minutes)—Enter the positive or negative minute offset from GMT.
- Daylight Savings—Select to enable Daylight Savings Time.

Upload a Controller's Configuration and Log Files to a TFTP Server

You can upload files from controllers to a local TFTP (Trivial File Transfer Protocol) server. You must enable TFTP to use the Default Server option on the Administration > System Settings > Server Settings page.

uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as , because the and the third-party TFTP servers use the same communication port.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 From the left sidebar menu, choose System > Commands.

Step 4 From the Upload/Download Commands drop-down list, choose Upload File from Controller, then click Go.

By default, configuration file encryption is disabled. Uploading configuration file is unsecured without encryption.

Step 5 To enable encryption before uploading files, click the link at the bottom of the Upload File from Controller page.

Step 6 Complete the required fields, then click OK. The selected file is uploaded to your TFTP server with the name you specified.

Related Topics

Configure the Date and Time on a Controller, on page 466
Download Software to Controllers, on page 456
Restore Controller Factory Default Settings, on page 466

Download Software To a Controller

You can download configuration files to your controller from a local TFTP (Trivial File Transfer Protocol) server.

Prime Infrastructure uses an integral TFTP server. This means that third-party TFTP servers cannot run on the same workstation as Prime Infrastructure, because the Cisco Prime Infrastructure and the third-party TFTP servers use the same communication port.

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 From the left sidebar menu, choose System > Commands.

Step 4 From the Upload/Download Commands drop-down list, choose Download Config, then click Go.

Step 5 Complete the required fields, then click OK.

Related Topics

Configure the Date and Time on a Controller, on page 466
Upload a Controller's Configuration and Log Files to a TFTP Server , on page 467
Restore Controller Factory Default Settings, on page 466

Configure Interfaces on a Single Controller

To add an interface:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Click a Device Name, then click the Configuration tab.
Step 3 From the left sidebar menu, choose System > Interfaces.
Step 4 From the Select a command drop-down list, choose Add Interface > Go.
Step 5 Complete the required fields, then click Save.

Related Topics

View the Interfaces on a Controller, on page 468
Delete a Dynamic Interface from a Controller, on page 469
Control User Access to Controllers Using a NAC Appliance, on page 470
Configure Guest Account Access to a Wired Controller, on page 474

View the Interfaces on a Controller

To view the existing interfaces:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click a Device Name, then click the Configuration tab.
Step 3 From the left sidebar menu, choose System > Interfaces. The following parameters appear:

- Check box—Check box to select the dynamic interface for deletion. Choose Delete Dynamic Interfaces from the Select a command drop-down list.
- Interface Name —User-defined name for the interface (for example, Management, Service-Port, Virtual).
- VLAN Id—VLAN identifier between 0 (untagged) and 4096, or N/A.
- Quarantine—Select the check box if the interface has a quarantine VLAN ID configured on it.
- IP Address—IP address of the interface.
- Interface Type—Interface Type: Static (Management, AP-Manager, Service-Port, and Virtual interfaces) or Dynamic (operator-defined interfaces).

- AP Management Status—Status of AP Management interfaces and the parameters include Enabled, Disabled, and N/A. Only the management port can be configured as Redundancy Management Interface port.

Related Topics

View and Manage Controller Interface Groups, on page 470

Delete a Dynamic Interface from a Controller

The dynamic interface cannot be deleted if it has been assigned to any interface group. To delete a dynamic interface:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click a Device Name, then click the Configuration tab.

Step 3 From the left sidebar menu, choose System > Interfaces.

Step 4 Select the check box of the dynamic interface that you want to delete and choose Delete Dynamic Interfaces from the Select a command drop-down list.

Step 5 Click OK to confirm the deletion.

Related Topics

View and Manage Controller Interface Groups, on page 470
View the Interfaces on a Controller, on page 468

Apply Interface Changes to Groups of Controllers Using Controller System Interface Groups

Interface groups are logical groups of interfaces. Interface groups facilitate user configuration where the same interface group can be configured on multiple WLANs or while overriding a WLAN interface per AP group. An interface group can exclusively contain either quarantine or non-quarantine interfaces. An interface can be part of multiple interface groups.

Follow these recommendations while configuring controller system interface groups:

- Ensure that the interface group name is different from the interface name.
- Guest LAN interfaces cannot be part of interface groups

The Interface Groups feature is supported by Cisco Wireless Controller software release 7.0.116.0 and later.

Related Topics

View and Manage Controller Interface Groups, on page 470
Control User Access to Controllers Using a NAC Appliance, on page 470

View and Manage Controller Interface Groups

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 From the left sidebar menu, choose System > Interface Groups>.

The following parameters appear:

- Name—User-defined name for the interface group (For example, group1, group2).
- Description—(Optional) Description for the Interface Group.
- Interfaces—Count of the number of interfaces belonging to the group.

Step 4 To view the existing Interface groups, Click the Interface Group Name link.

The Interface Groups Details page appears with the Interface group details as well as the details of the Interfaces that form part of that particular Interface group.

Step 5 To add an interface group, do the following:

a) From the Select a command drop-down list, choose Add Interface Group and click Go.
b) Complete the required fields, then click Add.
c) The Interface dialog box appears.
d) Select the interfaces that you want to add to the group, and click Select.

Step 6 To delete an interface group, do the following:

a) From the Select a command drop-down list, choose Delete Interface Group, and click Go.

Note You cannot delete interface groups that are assigned to WLANs, AP groups, Foreign Controller Mapping for WLANs, WLAN templates and AP group templates.

b) Click OK to confirm the deletion.

Step 7 To remove an Interface from the Interface group, from the Interface Group page, select the Interface and click Remove.

Step 8 Click Save to confirm the changes made.

Related Topics

Apply Interface Changes to Groups of Controllers Using Controller System Interface Groups, on page 469
Control User Access to Controllers Using a NAC Appliance, on page 470

Control User Access to Controllers Using a NAC Appliance

The Cisco Network Admission Control (NAC) appliance, also known as Cisco Clean Access (CCA), is a Network Admission Control (NAC) product that allows network administrators to authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to allowing users onto the network. It identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. The NAC appliance is available in two modes: in-band and out-of-band. Customers can deploy both modes if desired, each geared toward certain types of access (in-band for supporting wireless users and out-of-band for supporting wired users, for example).

Related Topics

Prerequisites for Using SNMP NAC, on page 471
Configure SNMP NAC on a Controller, on page 472

Prerequisites for Using SNMP NAC

Follow these guidelines when using SNMP NAC out-of-band integration:

- The NAC appliance supports up to 3500 users, and the controller supports up to 5000 users. Therefore, multiple NAC appliances might need to be deployed.
- Because the NAC appliance supports static VLAN mapping, you must configure a unique quarantine VLAN for each interface configured on the controller. For example, you might configure a quarantine VLAN of 110 on controller 1 and a quarantine VLAN of 120 on controller 2. However, if two WLANs or guest LANs use the same distribution system interface, they must use the same quarantine VLAN, provided they have one NAC appliance deployed in the network. The NAC appliance supports unique quarantine-to-access VLAN mapping.
- For posture reassessment based on session expiry, you must configure the session timeout on both the NAC appliance and the WLAN, making sure that the session expiry on the WLAN is greater than that on the NAC appliance.
- When a session timeout is configured on an open WLAN, the timing out of clients in the Quarantine state is determined by the timer on the NAC appliance. Once the session timeout expires for WLANs using web authentication, clients deauthenticate from the controller and must perform posture validation again.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.
- If you want to enable NAC on an access point group VLAN, you must first enable NAC on the WLAN. Then you can enable or disable NAC on the access point group VLAN. If you ever decide to disable NAC on the WLAN, be sure to disable it on the access point group VLAN as well.
- NAC out-of-band integration is not supported for use with the WLAN AAA override feature.
- All Layer 2 and Layer 3 authentication occurs in the quarantine VLAN. To use external web authentication, you must configure the NAC appliance to allow HTTP traffic to and from external web servers and to allow the redirect URL in the quarantine VLAN.

For more details, please refer to Cisco NAC Appliance Configuration.

Prerequisites for Using RADIUS NAC

Follow these guidelines when using RADIUS NAC:

- RADIUS NAC is available only for WLAN with 802.1x/WPA/WPA2 Layer 2 security.
- RADIUS NAC cannot be enabled when FlexConnect local switching is enabled.
- AAA override should be enabled to configure RADIUS NAC.

Related Topics

Control User Access to Controllers Using a NAC Appliance, on page 470

Configure SNMP NAC on a Controller

To configure SNMP NAC out-of-band integration, follow this workflow:

1. Configure the quarantine VLAN for a dynamic interface—The NAC appliance supports static VLAN mapping, and you must configure a unique quarantine VLAN for each interface that is configured on the controller.
2. Configure NAC out-of-band support on a WLAN or guest LAN—To enable NAC support on an access point group VLAN, you must first enable NAC on the WLAN or guest LAN.
3. Configure NAC Out-of-band support for a specific AP group—To configure NAC out-of-band support for specific access point groups.

Related Topics

Configure the Quarantine VLANs (SNMP NAC), on page 472
Enable NAC on the WLAN or Guest LAN (SNMP NAC), on page 472
Configure NAC Out-of-Band Support for an AP Group (SNMP NAC), on page 473

Configure the Quarantine VLANs (SNMP NAC)

To configure the quarantine VLAN for a dynamic interface:

Step 1 Choose Configuration > Network > Network DevicesConfiguration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Choose which controller you are configuring for out-of-band integration by clicking it in the IP Address column.

Step 3 Choose System > Interfaces from the left sidebar menu.

Step 4 Click the Interface Name.

Step 5 Choose Add Interface from the Select a command drop-down list and click Go.

Step 6 In the Interface Name text box, enter a name for this interface, such as “quarantine.”

Step 7 In the VLAN ID text box, enter a non-zero value for the access VLAN ID, such as “10.”

Step 8 Select the Quarantine check box if the interface has a quarantine VLAN ID configured on it.

Step 9 Configure any remaining fields for this interface, such as the IP address, netmask, and default gateway.

Note To avoid issues when adding the wireless controller to , the Dynamic Interface should not be in the same subnet as .

Step 10 Enter an IP address for the primary and secondary DHCP server.

Step 11 Click Save.

Related Topics

Enable NAC on the WLAN or Guest LAN (SNMP NAC), on page 472
Configure NAC Out-of-Band Support for an AP Group (SNMP NAC), on page 473

Enable NAC on the WLAN or Guest LAN (SNMP NAC)

To configure NAC out-of-band support on a WLAN or guest LAN, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name.

Step 3 Choose WLANs > WLAN from the left sidebar menu.

Step 4 Choose Add a WLAN from the Select a command drop-down list, and click Go.

Step 5 If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the click here link to create a new template.

Step 6 Click the Advanced tab.

Step 7 To configure SNMP NAC support for this WLAN or guest LAN, choose SNMP NAC from the drop-down list. To disable SNMP NAC support, choose None from the NAC Stage drop-down list, which is the default value.

Step 8 Click Apply to commit your changes.

Related Topics

Configure NAC Out-of-Band Support for an AP Group (SNMP NAC), on page 473
Configure Guest Account Access to a Wired Controller, on page 474

Configure NAC Out-of-Band Support for an AP Group (SNMP NAC)

To configure NAC out-of-band support for a specific AP group, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose WLANs > AP Groups VLAN from the left sidebar menu to open the AP Groups page.

Step 4 Click the name of the desired AP group.

Step 5 From the Interface Name drop-down list, choose the quarantine enabled interface.

Step 6 To configure SNMP NAC support for this AP group, choose SNMP NAC from the Nac State drop-down list. To disable NAC out-of-band support, choose None from the Nac State drop-down list, which is the default value.

Step 7 Click Apply to commit your changes.

Related Topics

Enable NAC on the WLAN or Guest LAN (SNMP NAC), on page 472
Configure Guest Account Access to a Wired Controller, on page 474
Configure the Quarantine VLANs (SNMP NAC), on page 472

View NAC State for a Network Client or User

To see the current state of the client (either Quarantine or Access), follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Clients and Users to open the Clients. Perform a search for clients.

Step 2 Click the MAC address of the desired client to open the Clients > Detail page. The NAC state appears as access, invalid, or quarantine in the Security Information section.

Related Topics

Configure SNMP NAC on a Controller, on page 472

Configure Guest Account Access to a Wired Controller

Wired Guest Access enables guest users to connect to the guest access network from a wired Ethernet connection designated and configured for guest access. Wired guest access ports might be available in a guest office or specific ports in a conference room.

Like wireless guest user accounts, wired guest access ports are added to the network using the Lobby Ambassador feature. Wired Guest Access can be configured in a standalone configuration or in a dual controller configuration employing an anchor and foreign controller. This latter configuration is used to further isolate wired guest access traffic but is not required for deployment of wired guest access.

Wired Guest Access ports initially terminate on a Layer 2 access switch or switch port which is configured with VLAN interfaces for wired guest access traffic. The wired guest traffic is then trunked from the access switch to a wireless LAN controller. This controller is configured with an interface that is mapped to a wired guest access VLAN on the access switch.

If two controllers are being used, the controller (foreign) that receives the wired guest traffic from the switch then forwards the wired guest traffic to an anchor controller that is also configured for wired guest access. After successful hand off of the wired guest traffic to the anchor controller, a bidirectional Ethernet over IP (EoIP) tunnel is established between the foreign and anchor controllers to handle this traffic.

Although wired guest access is managed by anchor and foreign anchors when two controllers are deployed, mobility is not supported for wired guest access clients. In this case, DHCP and web authentication for the client are handled by the anchor controller.

You can specify how much bandwidth a wired guest user is allocated in the network by configuring and assigning a role and bandwidth contract.

Related Topics

- Configure and Enable Wired Guest User Access: Workflow

Configure and Enable Wired Guest User Access: Workflow

To configure and enable the wired guest user access, follow this workflow:

1. Configure a dynamic interface (VLAN) for wired guest access—Create a dynamic interface to enable the wired guest user access.
2. Configure a wired LAN for guest user access—Configure a new LAN, which is a guest LAN.

Related Topics

Configure a Dynamic Interface for Wired Guest User Access, on page 475
Configure a Wired LAN for Guest User Access, on page 475

Configure a Dynamic Interface for Wired Guest User Access

To configure and enable a dynamic interface (VLAN) for wired guest user access on the network:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose System > Interfaces from the left sidebar menu.

Step 4 Choose Add Interface from the Select a command drop-down list, and click Go.

Step 5 Complete the required fields.

Step 6 Click Save.

Related Topics

Configure and Enable Wired Guest User Access: Workflow, on page 474

Configure a Wired LAN for Guest User Access

To configure a wired LAN for guest user access:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click on a Device Name.

Step 3 To configure a wired LAN for guest user access, choose WLANs > WLAN configuration from the left sidebar menu.

Step 4 Choose Add a WLAN from the Select a command drop-down list, and click Go.

Step 5 If you have a template established that you want to apply to this controller, choose the guest LAN template name from the drop-down list. Otherwise, click the click here link to create a new template.

Step 6 In the WLAN > New Template general page, enter a name in the Profile Name text box that identifies the guest LAN. Do not use any spaces in the name entered.

Step 7 Select the Enabled check box for the WLAN Status field.

Step 8 From the Ingress Interface drop-down list, choose the VLAN that you created in Step 3. This VLAN provides a path between the wired guest client and the controller by way of the Layer 2 access switch.

Step 9 From the Egress Interface drop-down list, choose the name of the interface. This WLAN provides a path out of the controller for wired guest client traffic.If you have only one controller in the configuration, choose management from the Egress Interface drop-down list.

Step 10 Click the Security > Layer 3 tab to modify the default security policy (web authentication) or to assign WLAN specific web authentication (login, logout, login failure) pages and the server source.

a) To change the security policy to passthrough, select the Web Policy check box and select the Passthrough radio button. This option allows users to access the network without entering a username or password.

An Email Input check box appears. Select this check box if you want users to be prompted for their e-mail address when attempting to connect to the network.

b) To specify custom web authentication pages, unselect the Global WebAuth Configuration Enabled check box.

When the Web Auth Type drop-down list appears, choose one of the following options to define the web login page for the wireless guest users:

Default Internal—Displays the default web login page for the controller. This is the default value.

Customized Web Auth—Displays custom web login, login failure, and logout pages. When the customized option is selected, three separate drop-down lists for login, login failure, and logout page selection appear. You do not need to define a customized page for all three of the options. Choose None from the appropriate drop-down list if you do not want to display a customized page for that option.

External—Redirects users to an external server for authentication. If you choose this option, you must also enter the URL of the external server in the URL text box.

You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA pane. The RADIUS and LDAP external servers must be already configured to have selectable options in the Security > AAA pane. You can configure these servers on the RADIUS Authentication Servers, TACACS+ Authentication Servers page, and LDAP Servers page.

Step 11 If you selected External as the Web Authentication Type, choose Security > AAA and choose up to three RADIUS and LDAP servers using the drop-down lists.

Step 12 Click Save.

Step 13 Repeat this process if a second (anchor) controller is being used in the network.

Related Topics

Configure and Enable Wired Guest User Access: Workflow, on page 474

Configure a Guest LAN Ingress Interface on a Controller

To create an Ingress interface:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose System > Interfaces from the left sidebar menu.

Step 4 Choose Add Interface from the Select a command drop-down list, and click Go.

Step 5 In the Interface Name text box, enter a name for this interface, such as guestinterface.

Step 6 Enter a VLAN identifier for the new interface.

Step 7 Select the Guest LAN check box.

Step 8 Enter the primary and secondary port numbers.

Step 9 Click Save.

Related Topics

Configure a Guest LAN Egress Interface on a Controller, on page 477

Configure a Guest LAN Egress Interface on a Controller

To create an Egress interface:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose System > Interfaces from the left sidebar menu.

Step 4 Choose Add Interface from the Select a command drop-down list, and click Go.

Step 5 In the Interface Name text box, enter a name for this interface, such as quarantine.

Step 6 In the vlan Id text box, enter a non-zero value for the access VLAN ID, such as 10.

Step 7 Select the Quarantine check box and enter a non-zero value for the Quarantine VLAN identifier, such as 110.

You can have NAC-support enabled on the WLAN or guest WLAN template Advanced tab for interfaces with Quarantine enabled.

Step 8 Enter the IP address, Netmask, and Gateway information.

Step 9 Enter the primary and secondary port numbers.

Step 10 Provide an IP address for the primary and secondary DHCP server.

Step 11 Configure any remaining fields for this interface, and click Save.

You are now ready to create a wired LAN for guest access.

Related Topics

Configure a Guest LAN Ingress Interface on a Controller, on page 476

Configure a Network Route on a Controller Service Port

The Network Route page enables you to add a route to the controller service port. This route allows you to direct all Service Port traffic to the designated management IP address.

Related Topics

View Existing Controller Network Routes, on page 477
Add Network Routes to a Controller, on page 478

View Existing Controller Network Routes

To view existing network routes:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller. .

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose System > Network Route > from the left sidebar menu. The following parameters appear:

- IP Address—The IP address of the network route.
- IP Netmask—Network mask of the route.
- Gateway IP Address—Gateway IP address of the network route.

Related Topics

Configure a Network Route on a Controller Service Port, on page 477

Add Network Routes to a Controller

To add a network route, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose System > Network Route from the left sidebar menu.

Step 4 From the Select a command drop-down list, choose Add Network Route.

Step 5 Click Go.

Step 6 Complete the required fields, then click Save.

Related Topics

Configure a Network Route on a Controller Service Port, on page 477
Configure the Date and Time on a Controller, on page 466

View a Controller's STP Parameters

Spanning Tree Protocol (STP) is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

To view or manage current STP parameters:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 ChooseSystem > Spanning Tree Protocol from the left sidebar menu. The Spanning Tree Protocol page displays the following parameters:

- Protocol Spec—The current protocol specification.
- Admin Status—Select this check box to enable.
- Priority—The numerical priority number of the ideal switch.
- Maximum Age (seconds)—The amount of time (in seconds) before the received protocol information recorded for a port is discarded.

- Hello Time (seconds)—Determines how often (in seconds) the switch broadcasts its hello message to other switches.
- Forward Delay (seconds)—The time spent (in seconds) by a port in the learning/listening states of the switches.

Related Topics

Configure a Network Route on a Controller Service Port, on page 477
Change Controller General System Properties from the Network Devices Table, on page 462

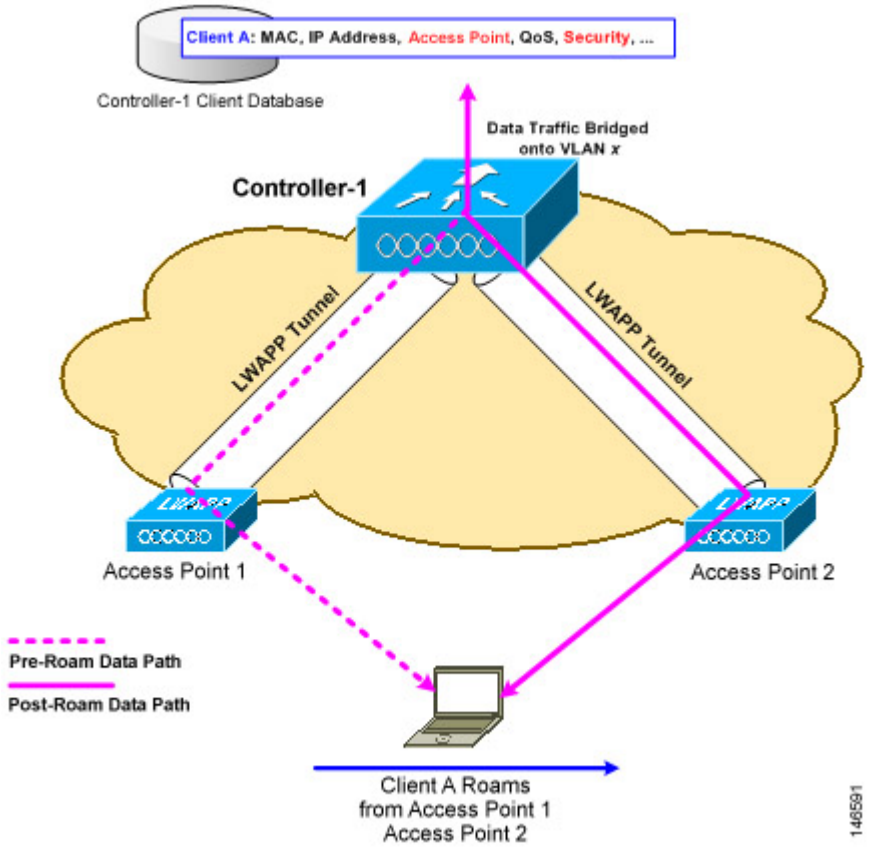
What is Mobility?

Mobility, or roaming, is an ability of a wireless client to maintain its association seamlessly from one access point to another, securely and with as little latency as possible, in a wireless network. When a wireless client is associated to and authenticated by an access point, a controller places an entry for that client in its client database. This entry includes the MAC and IP addresses of the client, security context and associations, quality of service (QoS) contexts, the WLANs, and the associated access point. The controller uses this information to forward frames and manage traffic to and from the wireless client.

What is Intra-Controller Roaming?

When the wireless client moves its association from one access point to another, the controller simply updates the client database with the newly associated access point. If necessary, new security context and associations are established as well. The folowing figure illustrates a wireless client roaming from one access point to another when both access points are connected to the same controller. Figure 146591

Figure 11: Intra-Controller Roaming



Related Topics

What is Mobility?, on page 479
What are Mobility Groups?, on page 483
What is Inter-Controller Roaming?, on page 480

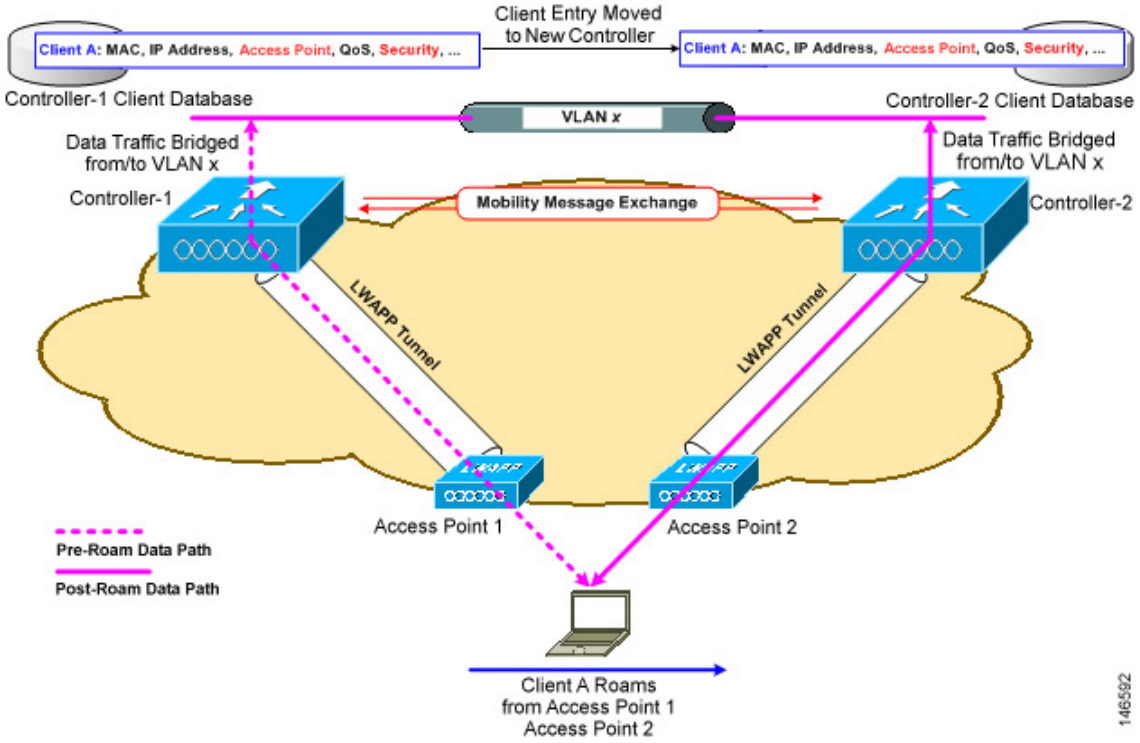
What is Inter-Controller Roaming?

When a client roams from an access point connected to one controller to an access point connected to a different controller, the process also varies based on whether the controllers are operating on the same subnet. The following figure illustrates inter-controller roaming , which occurs when the wireless LAN interfaces of a controller are on the same IP subnet.

When the client is associated to an access point connected to a new controller, the new controller exchanges mobility messages with the original controller, and the client database entry is moved to the new controller. New security context and associations are established if necessary, and the client database entry is updated for the new access point. This process remains invisible to the user.

All clients configured with 802.1X/Wi-Fi Protected Access (WPA) security complete a full authentication to comply with the IEEE standard.

Figure 12: Inter-Controller Roaming



Related Topics

What is Mobility?, on page 479
What are Mobility Groups?, on page 483
What is Intra-Controller Roaming?, on page 479
Prerequisites for Adding Controllers to Mobility Groups, on page 484

What is Inter-Subnet Roaming?

Inter-subnet roaming is similar to inter-controller roaming in that the controllers exchange mobility messages on how the client roams. However, instead of moving the client database entry to the new controller, the original controller marks the client with an “Anchor” entry in its own client database. The database entry is copied to the new controller client database and marked with a “Foreign” entry in the new controller. The roam remains invisible to the wireless client, and the client maintains its original IP address.

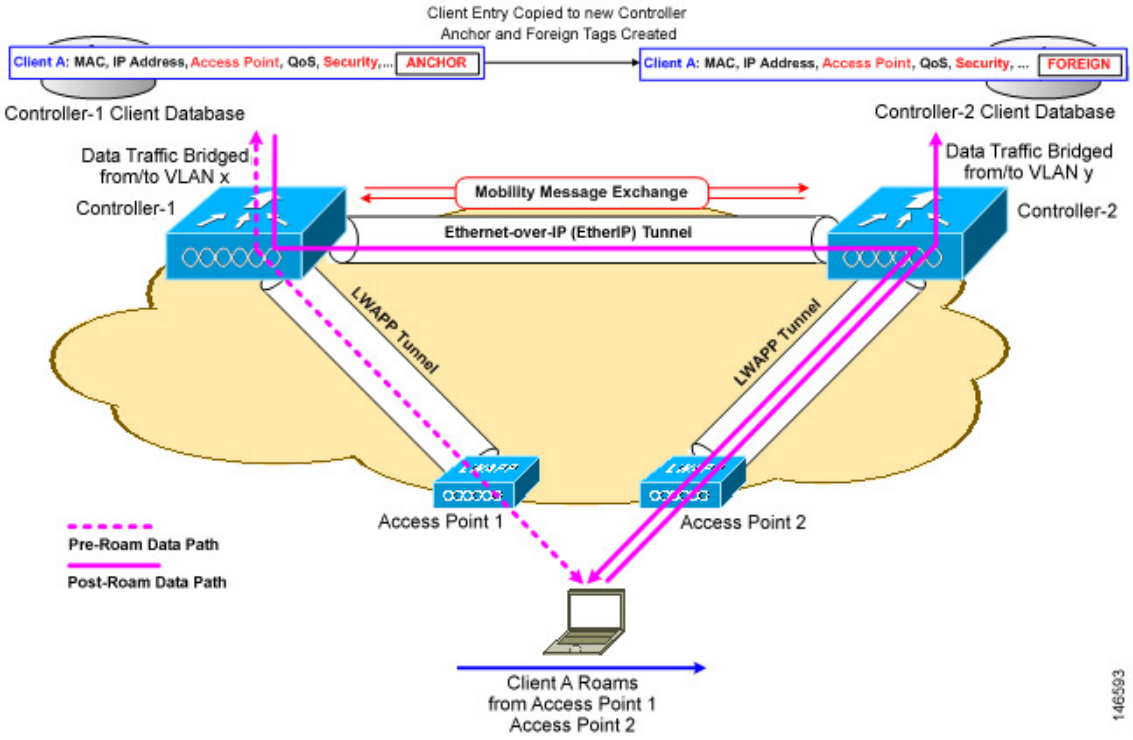
After an inter-subnet roam, data flows in an asymmetric traffic path to and from the wireless client. Traffic from the client to the network is forwarded directly into the network by the foreign controller. Traffic to the client arrives at the anchor controller, which forwards the traffic to the foreign controller in an EtherIP tunnel. The foreign controller then forwards the data to the client. If a wireless client roams to a new foreign controller, the client database entry is moved from the original foreign controller to the new foreign controller, but the original anchor controller is always maintained. If the client moves back to the original controller, it becomes local again.

In inter-subnet roaming, WLANs on both anchor and foreign controllers need to have the same network access privileges and no source-based routing or source-based firewalls in place. Otherwise, the clients might have network connectivity problems after the handoff.

Inter-subnet roaming does not support multicast traffic such as one used by Spectralink phones while using push-to-talk.

The following figure 146593 illustrates inter-subnet roaming , which occurs when the wireless LAN interfaces of a controller are on different IP subnets.

Figure 13:



Related Topics

What is Mobility?, on page 479
What are Mobility Groups?, on page 483
What is Intra-Controller Roaming?, on page 479
What is Inter-Controller Roaming?, on page 480
Prerequisites for Adding Controllers to Mobility Groups, on page 484

What is Symmetric Tunneling?

With symmetric mobility tunneling, the controller provides inter-subnet mobility for clients roaming from one access point to another within a wireless LAN. The client traffic on the wired network is directly routed by the foreign controller. If a router has Reverse Path Filtering (RPF) enabled (which provides additional checks on incoming packets), the communication is blocked. Symmetric mobility tunneling allows the client traffic to reach the controller designated as the anchor, even with RPF enabled. All controllers in a mobility group should have the same symmetric tunneling mode.

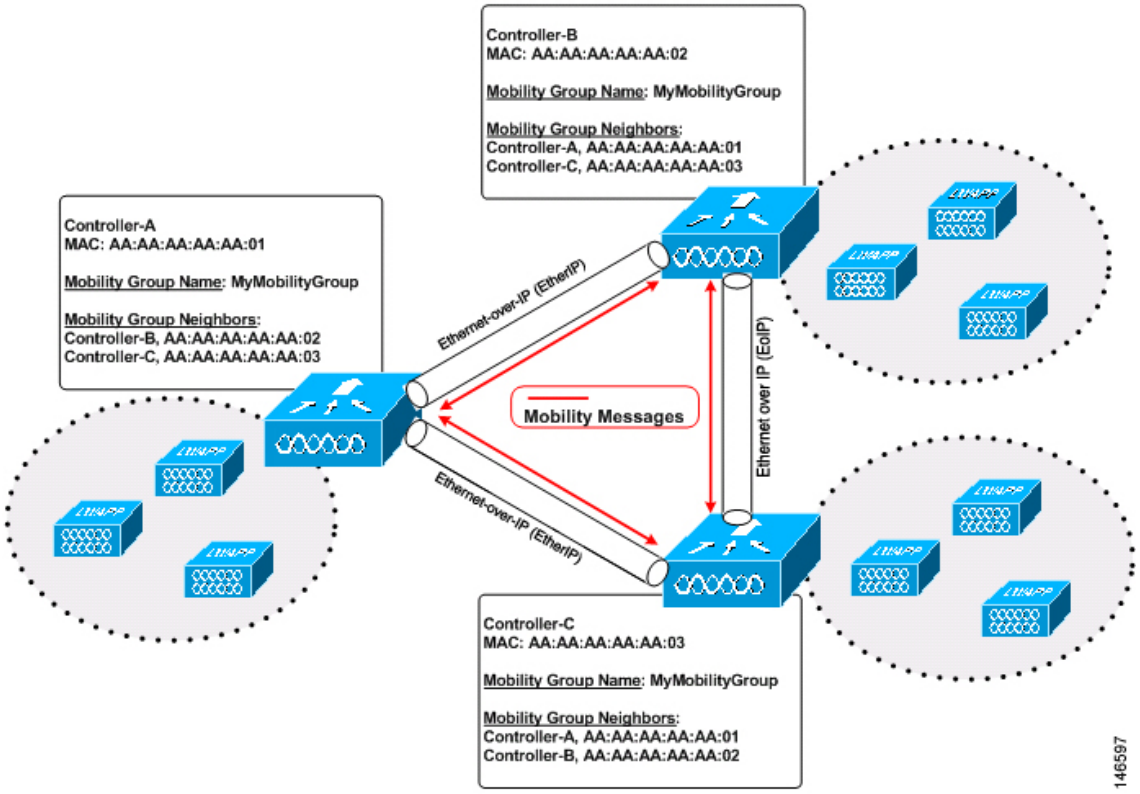
With this feature, the time it takes for a client to join another access point following a controller failure is decreased because a failure is quickly identified, the clients are moved away from the problem controller, and the clients are anchored to another controller.

What are Mobility Groups?

A set of controllers can be configured as a mobility group to allow seamless client roaming within a group of controllers. This enables multiple controllers to dynamically share information and forward data traffic when inter-controller or inter-subnet roaming occurs. Controllers can share the context and state of clients and controller loading information With this information, the network can support inter-controller wireless LAN roaming and controller redundancy. Clients do not roam across mobility groups

The following figure shows an example of a mobility group.

Figure 14: Single Mobility Group



As shown in the above figure, each controller is configured with a list of the other members of the mobility group. Whenever a new client joins a controller, the controller sends out a unicast message to all of the controllers in the mobility group. The controller to which the client was previously connected passes on the status of the client. All mobility exchange traffic between controllers is carried over a CAPWAP tunnel.

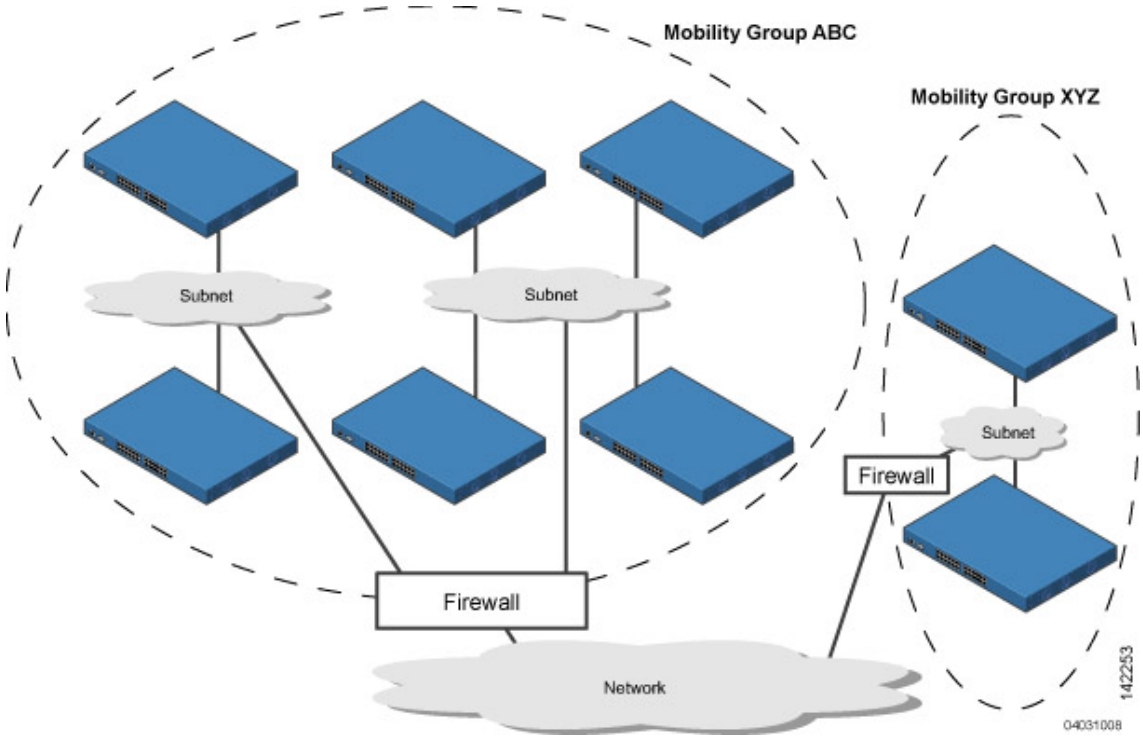
Examples:

1. A 4404-100 controller supports up to 100 access points. Therefore, a mobility group consisting of 24 4404-100 controllers supports up to 2400 access points (24 * 100 = 2400 access points).
2. A 4402-25 controller supports up to 25 access points, and a 4402-50 controller supports up to 50 access points. Therefore, a mobility group consisting of 12 4402-25 controllers and 12 4402-50 controllers supports up to 900 access points (12 * 25 + 12 * 50 = 300 + 600 = 900 access points).

Mobility groups enable you to limit roaming between different floors, buildings, or campuses in the same enterprise by assigning different mobility group names to different controllers within the same wireless

network. The following figure shows the results of creating distinct mobility group names for two groups of controllers.

Figure 15: Two Mobility Groups



The controllers in the ABC mobility group recognize and communicate with each other through their access points and through their shared subnets. The controllers in the ABC mobility group do not recognize or communicate with the XYZ controllers, which are in a different mobility group. Likewise, the controllers in the XYZ mobility group do not recognize or communicate with the controllers in the ABC mobility group. This feature ensures mobility group isolation across the network. Clients might roam between access points in different mobility groups, provided they can detect them. However, their session information is not carried between controllers in different mobility groups.

Related Topics

Prerequisites for Adding Controllers to Mobility Groups, on page 484
How Controller Mobility Group Messaging Works, on page 485

Prerequisites for Adding Controllers to Mobility Groups

Before you add controllers to a mobility group, you must verify that the following prerequisites are met for all controllers that are to be included in the group:

- All controllers must be configured for the same CAPWAP transport mode (Layer 2 or Layer 3).
- IP connectivity must exist between the management interfaces of all controllers.
- All controllers must be configured with the same mobility group name.
- All controllers must be configured with the same virtual interface IP address.

- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.
- If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

Related Topics

What are Mobility Groups?, on page 483
How Controller Mobility Group Messaging Works, on page 485

How Controller Mobility Group Messaging Works

The controller provides inter-subnet mobility for clients by sending mobility messages to other member controllers. There can be up to 72 members in the list with up to 24 in the same mobility group. In Prime Infrastructure and controller software releases 5.0, two improvements have been made to mobility messaging, each of which is especially useful when sending messages to the full list of mobility members:

- Sending Mobile Announce messages within the same group first and then to other groups in the list

The controller sends a Mobile Announce message to members in the mobility list each time a new client associates to it. In the software releases prior to 5.0, the controller sends this message to all members in the list irrespective of the group to which they belong. However, in the software release 5.0, the controller sends the message only to those members that are in the same group as the controller and then includes all of the other members while sending retries.

- Sending Mobile Announce messages using multicast instead of unicast

In and controller software releases prior to 5.0, the controller might be configured to use multicast to send the mobile announce messages, which requires sending a copy of the messages to every mobility member. This behavior is not efficient because many messages (such as Mobile Announce, Pairwise Primary Key (PPK) Update, AP List Update, and Intrusion Detection System (IDS) Shun) are meant for all members in the group. In and controller software releases 5.0, the controller uses multicast mode to send the Mobile Announce messages. This behavior allows the controller to send only one copy of the message to the network, which destines it to the multicast group containing all the mobility members. To derive the maximum benefit from multicast messaging, We recommend that it be enabled or disabled on all group members.

Related Topics

What are Mobility Groups?, on page 483
Prerequisites for Adding Controllers to Mobility Groups, on page 484
Configuring Mobility Groups: Workflow, on page 485

Configuring Mobility Groups: Workflow

Whenever you configure a Mobility Group, follow this workflow:

1. Make sure you have gathered the information you need and that the participating controller are properly configured, as explained in Prerequisites for Adding Controllers to Mobility Groups, on page 484.
2. Add individual controllers to the Mobility Group. You may need to add them manually if no Mobility Groups exist or no controllers are listed when you try to add them from the Configuration > Network > Network Devices page.
3. Set the scale and messaging parameters for the Mobility Group.

Prerequisites for Adding Controllers to Mobility Groups

Before you add controllers to a mobility group, you must verify that the following prerequisites are met for all controllers that are to be included in the group:

- All controllers must be configured for the same CAPWAP transport mode (Layer 2 or Layer 3).
- IP connectivity must exist between the management interfaces of all controllers.
- All controllers must be configured with the same mobility group name.
- All controllers must be configured with the same virtual interface IP address.
- You must have gathered the MAC address and IP address of every controller that is to be included in the mobility group. This information is necessary because you will be configuring all controllers with the MAC address and IP address of all the other mobility group members.
- If it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be in the same mobility group.

Related Topics

What are Mobility Groups?, on page 483
How Controller Mobility Group Messaging Works, on page 485

View the Controllers That Belong to a Mobility Group

To view current mobility group members:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose System > Mobility Groups from the left sidebar menu.

Related Topics

Add Controllers to a Mobility Group from the Network Devices Table, on page 486

Add Controllers to a Mobility Group from the Network Devices Table

To add a mobility group member from a list of existing controllers:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click on a Device Name, then click the Controller tab.

Step 3 Choose System > Mobility Groups from the left sidebar menu.

Step 4 From the Select a command drop-down list, choose Add Group Members.

Step 5 Click Go.

Step 6 Select the check box(es) for the controller to be added to the mobility group.

Step 7 Click Save.

Step 8 If no controllers are listed in Step 6, then you can manually add one by doing the following:

a) Click the click here link from the Mobility Group Member details page.

b) In the Member MAC Address text box, enter the MAC address of the controller to be added.
c) In the Member IP Address text box, enter the management interface IP address of the controller to be added.

   If you are configuring the mobility group in a network where Network Address Translation (NAT) is enabled, enter the IP address sent to the controller from the NAT device rather than the controller management interface IP address. Otherwise, mobility fails among controllers in the mobility group.

d) Enter the multicast group IP address to be used for multicast mobility messages in the Multicast Address text box. The local mobility member group address must be the same as the local controller group address.
e) In the Group Name text box, enter the name of the mobility group.
f) Click Save.

   Repeat the above steps for the remaining Cisco Wireless Controller devices.

Related Topics

View the Controllers That Belong to a Mobility Group, on page 486

Configure Multicast Mode for Messages to Mobility Members

Before You Begin

You must configure Mobility Groups prior setting up the mobility scalability parameters.

To set the mobility message parameters:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the Device Name of a controller whose software version is 5.0 or later.

Step 3 From the left sidebar menu, choose System > General.

Step 4 From the Multicast Mobility Mode drop-down list, specify if you want to enable or disable the ability for the controller to use multicast mode to send Mobile Announce messages to mobility members.

Step 5 If you enabled multicast messaging by setting multicast mobility mode to enabled, you must enter the group IP address at the Mobility Group Multicast-address field to begin multicast mobility messaging. You must configure this IP address for the local mobility group but it is optional for other groups within the mobility list. If you do not configure the IP address for other (non-local) groups, the controllers use unicast mode to send mobility messages to those members.

Step 6 Click Save.

Related Topics

Configure Multicast Mode and IGMP Snooping on a Controller, on page 497
Change Controller General System Properties from the Network Devices Table, on page 462

Add an NTP Server to a Controller

To add a new NTP Server:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose System > Network Time Protocol.

Step 4 From the Select a command drop-down list, choose Add NTP Server.

Step 5 Click Go.

Step 6 From the Select a template to apply to this controller drop-down list, choose the applicable template to apply to this controller.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 462

Configure Controllers for Mesh Network Background Scanning

Background scanning allows Cisco Aironet 1510 Access Points to actively and continuously monitor neighboring channels for more optimal paths and parents. Because the access points are searching on neighboring channels as well as the current channel, the list of optimal alternate paths and parents is greater.

Identifying this information prior to the loss of a parent results in a faster transfer and the best link possible for the access points. Additionally, access points might switch to a new channel if a link on that channel is found to be better than the current channel in terms of fewer hops, stronger signal-to-noise ratio (SNR), and so on.

Background scanning on other channels and data collection from neighbors on those channels are performed on the primary backhaul between two access points:

The primary backhaul for 1510s operate on the 802.11a link.

Background scanning is enabled on a global basis on the associated controller of the access point. Latency might increase for voice calls when they are switched to a new channel.

In the EMEA regulatory domain, locating neighbors on other channels might take longer given DFS requirements.

Related Topics

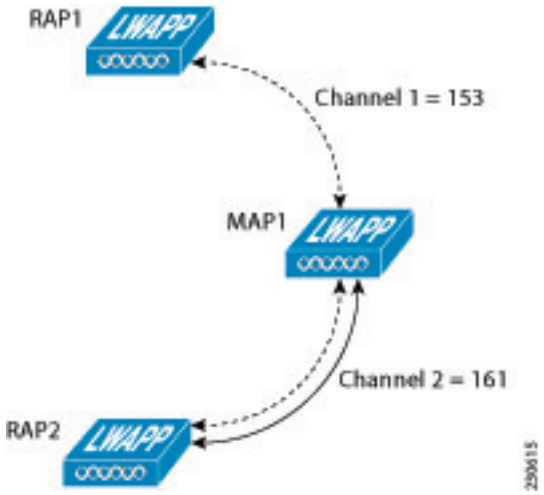
Mesh Network Background Scanning Scenarios, on page 488
Enable Mesh Network Background Scanning on Controllers, on page 489

Mesh Network Background Scanning Scenarios

A few scenarios are provided below to better illustrate how background scanning operates.

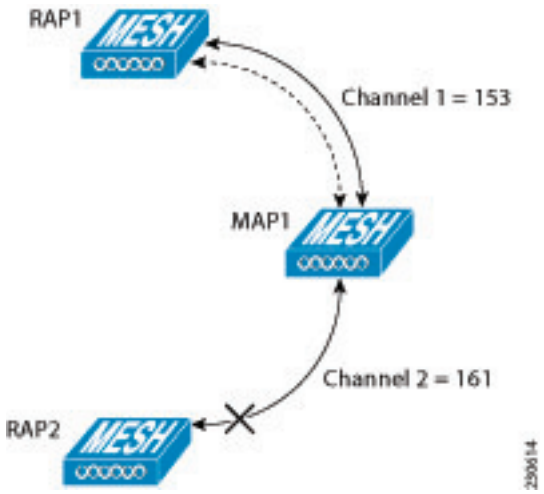
In the following figure, when the mesh access point (MAP1) initially comes up, it is aware of both root access points (RAP1 and RAP2) as possible parents. It chooses RAP2 as its parent because the route through RAP2 is better in terms of hops, SNR, and so on. After the link is established, background scanning (once enabled) continuously monitors all channels in search of a more optimal path and parent. RAP2 continues to act as parent for MAP1 and communicates on channel 2 until either the link goes down or a more optimal path is located on another channel.

Figure 16: Mesh Access Point (MAP1) Selects a Parent



In the following figure230614, the link between MAP1 and RAP2 is lost. Data from ongoing background scanning identifies RAP1 and channel 1 as the next best parent and communication path for MAP1 so that link is established immediately without the need for additional scanning after the link to RAP2 goes down.

Figure 17: Background Scanning Identifies a New Parent



Related Topics

Enable Mesh Network Background Scanning on Controllers, on page 489

Enable Mesh Network Background Scanning on Controllers

To enable background scanning on an AP1510 RAP or MAP:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click an IP address of the applicable controller.

Step 3 Choose Mesh > Mesh Settings from the left sidebar menu.

Step 4 Select the Background Scanning check box to enable background scanning or unselect it to disable the feature. The default value is disabled.

Step 5 This feature eliminates the time consuming task of finding a parent across channels by scanning all the channels. The off-channel procedure transmits broadcast packets on selected channels (at a periodicity of 3 seconds, with a maximum of 50 milliseconds per off-channel) and receives packets from all 'reachable' neighbors. This keeps the child MAP updated with neighbor information across channels enabling it to 'switch' to a new neighbor and use it as a parent for the uplink. The 'switch' need not be triggered from parent loss detection, but on identifying a better parent while the child MAP still has its current parent uplink active.

Step 6 Click Save.

Related Topics

Mesh Network Background Scanning Scenarios, on page 488

Configure Controller QoS Profiles

To make modifications to the quality of service profiles:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click an IP address of the applicable controller.

Step 3 From the left sidebar menu, choose System > QoS Profiles. The following parameters appear:

- Bronze—For Background
- Gold—For Video Applications
- Platinum—For Voice Applications
- Silver—For Best Effort

Step 4 Click the applicable profile to view or edit profile parameters.

Step 5 Click Save.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 462

Information About Internal DHCP Server

Cisco Controllers have built-in DHCP (Dynamic Host Configuration Protocol) relay agents. However, when you desire network segments that do not have a separate DHCP server, the controllers can have built-in DHCP scopes that assign IP addresses and subnet masks to wireless client. Typically, one controller can have one or more DHCP scopes that each provide a range of IP addresses.

Note This feature is applicable for Cisco Mobility Express Release 8.3 and later.

Viewing Current DHCP Scopes

To view current DHCP (Dynamic Host Configuration Protocol) scopes, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose System > DHCP Scopes. The following parameters appear:

- Scope Name
- Pool Address
- Lease Time
- Pool Usage. This is displayed only for Cisco Mobility Express DHCP scopes.

Configuring DHCP Scopes

To add a new DHCP Scope, follow these steps.

Procedure

	Command or Action	Purpose
Step 1	Choose Configuration > Network > Network Devices > Device Type > Wireless Controller.	
Step 2	Click the Device Name of the applicable controller.	
Step 3	From the left sidebar menu, choose System > DHCP Scopes.	
Step 4	From the Select a command drop-down list, choose Add DHCP Scope to add a new DHCP scope, and click Go.	
Step 5	In the Scope Name text box, enter a name for the new DHCP scope.	
Step 6	In the VLAN-ID text box, enter the VLAN ID.	
Step 7	In the Lease Time text box, enter the amount of time (from 0 to 65,536 seconds) that an IP address is granted to a client.	
Step 8	In the Network text box, enter the network served by this DHCP scope. This IP address is used by the management	

	Command or Action	Purpose
	interface with Netmask applied, as configured on the Interfaces page.	
Step 9	In the Netmask text box, enter the subnet mask assigned to all wireless clients.	
Step 10	In the Pool Start Address text box, enter the starting IP address in the range assigned to the clients. This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.	
Step 11	In the Pool End Address text box, enter the ending IP address in the range assigned to the clients. This pool must be unique for each DHCP scope and must not include the static IP addresses of routers or other servers.	
Step 12	In the Default Gateway text box, enter the IP address of the optional gateway.	
Step 13	In the DNS Domain Name text box, enter the optional DNS name of this DHCP scope for use with one or more DNS servers.	
Step 14	In the DNS Servers text box, enter the IP address of the optional DNS server. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope.	
Step 15	Click Save.	

Deleting DHCP Scopes

Note To delete a DHCP scope, you must first disable it's Admin status.

Procedure

	Command or Action	Purpose
Step 1	Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.	
Step 2	Click the Device Name of the applicable controller.	
Step 3	From the left sidebar menu, choose System > DHCP Scopes.	
Step 4	Select the check box of the DHCP Scope that you want to delete.	
Step 5	From the Select a command drop-down list, choose Delete DHCP Scopes, click Go.	

Exporting DHCP Scope Details

Procedure

	Command or Action	Purpose
Step 1	Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.	
Step 2	Click the Device Name of the applicable controller.	
Step 3	From the left sidebar menu, choose System > DHCP Scopes.	
Step 4	From the Select a command drop-down list, choose DHCPLeases, click Go.	
Step 5	Check the check box next to Mac Address, and Click Export to export the DHCP scope details as a csv file.	

View a Controller's Local Network Templates Used for Controller User Authentication

To view current local net user roles on a controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose System > User Roles.

The Local Net User Role parameters appear.

Step 4 Click a Template Name to view the User Role details.

Related Topics

Configure a Controller's Local Network Templates Used for Controller User Authentication , on page 493

Configure a Controller's Local Network Templates Used for Controller User Authentication

To add a new local net user role to a controller:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose System > User Roles.

Step 4 From the Select a command drop-down list, choose Add User Role.

Step 5 Select a template from the Select a template to apply to this controller drop-down list.

Step 6 Click Apply.

Related Topics

View a Controller's Local Network Templates Used for Controller User Authentication, on page 493
Change Controller General System Properties from the Network Devices Table, on page 462

Configure a Controller Username and Password for APs Connecting to the Controller

The AP Username Password page enables you to set a global password that all access points inherit as they join a controller. When you are adding an access point, you can also choose to accept this global username and password or override it on a per-access point basis.

Also in controller software release 5.0, after an access point joins the controller, the access point enables console port security and you are prompted for your username and password whenever you log into the access point console port. When you log in, you are in non-privileged mode and you must enter the enable password to use the privileged mode.

To establish a global username and password, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the Device Name of a controller with a Release 5.0 or later.

Step 3 From the left sidebar menu, choose System > AP Username Password.

Step 4 Enter the username and password that you want to be inherited by all access points that join the controller.

For Cisco IOS access points, you must also enter and confirm an enable password.

Step 5 Click Save.

Configure CDP on a Controller

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

CDP is enabled on the Ethernet and radio ports of a bridge by default.

Global Interface CDP configuration is applied to only the APs with CDP enabled at AP level.

To configure a Global CDP, perform the following steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose System > Global CDP Configuration from the left sidebar menu. The Global CDP Configuration page appears.

Step 4 Configure the required fields in the Global CDP Configuration page. In the Global CDP group box, configure the following parameters:

- CDP on controller—Choose enable or disable CDP on the controller. This configuration cannot be applied on WiSM2 controllers.
- Global CDP on APs—Choose to enable or disable CDP on the access points.
- Refresh-time Interval (seconds)—In the Refresh Time Interval field, enter the time in seconds at which CDP messages are generated. The default is 60.
- Holdtime (seconds)—Enter the time in seconds before the CDP neighbor entry expires. The default is 180.
- CDP Advertisement Version—Enter which version of the CDP protocol to use. The default is v1.

Step 5 In the CDP for Ethernet Interfaces group box, select the slots of Ethernet interfaces for which you want to enable CDP.

CDP for Ethernet Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 6 In the CDP for Radio Interfaces group box, select the slots of Radio interfaces for which you want to enable CDP.

CDP for Radio Interfaces fields are supported for Controller Release 7.0.110.2 and later.

Step 7 Click Save.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 462

Configure 802.1X Authentication for Controllers

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future.

If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

To enable global supplicant credentials, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose System > AP 802.1X Supplicant Credentials.

Step 4 Select the Global Supplicant Credentials check box.

Step 5 Enter the supplicant username.

Step 6 Enter and confirm the applicable password.

Step 7 Select the Supplicant EAP Type from the dropdown menu.

Note Applicable for controllers and MEs with versions 8.7 onwards.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 462
Configure a Device's 802.11 Parameters , on page 556

Configure 802.1X Authentication for Controllers

You can configure 802.1X authentication between lightweight access points and the switch. The access point acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning. You can set global authentication settings that all access points inherit as they join the controller. This includes all access points that are currently joined to the controller and any that join in the future.

If desired, you can override the global authentication settings and assign unique authentication settings for a specific access point.

To enable global supplicant credentials, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose System > AP 802.1X Supplicant Credentials.

Step 4 Select the Global Supplicant Credentials check box.

Step 5 Enter the supplicant username.

Step 6 Enter and confirm the applicable password.

Step 7 Select the Supplicant EAP Type from the dropdown menu.

Note Applicable for controllers and MEs with versions 8.7 onwards.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 462
Configure a Device's 802.11 Parameters , on page 556

Configure DHCP on a Controller

To configure DHCP (Dynamic Host Configuration Protocol) information for a controller:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose System > DHCP.

Step 4 Add or modify the following parameters:

- DHCP Option 82 Remote Id Field Format—Choose AP-MAC, AP-MAC-SSID, AP-ETHMAC, or AP-NAME-SSID from the drop-down list.

To set the format for RemoteID field in DHCP option 82If Ap-Mac is selected, then set the RemoteID format as AP-Mac. If Ap-Mac-ssid is selected, then set the RemoteID format as AP-Mac:SSID.

- DHCP Proxy—Select the check box to enable DHCP by proxy.

When DHCP proxy is enabled on the controller, the controller unicasts DHCP requests from the client to the configured servers. Consequently, at least one DHCP server must be configured on either the interface associated with the WLAN or the WLAN itself.

Step 5 Enter the DHCP Timeout in seconds after which the DHCP request times out. The default setting is 5. Allowed values range from 5 to 120 seconds. DHCP Timeout is applicable for Controller Release 7.0.114.74 and later.

Step 6 Click Save.

Once saved, you can click Audit to perform an audit on this controller.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 462

Configure Multicast Mode and IGMP Snooping on a Controller

provides an option to configure IGMP (Internet Group Management Protocol) snooping and timeout values on the controller.

IGMP

To configure multicast mode and IGMP snooping for a controller:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the Device Name of the desired controller.

Step 3 From the left sidebar menu, choose System > Multicast.

Step 4 From the Ethernet Multicast Support drop-down list, choose the applicable Ethernet multicast support (Unicast or Multicast).

Step 5 If Multicast is selected, enter the multicast group IP address.

Step 6 Select the Global Multicast Mode check box to make the multicast mode available globally.

IGMP Snooping and timeout can be set only if Ethernet Multicast mode is Enabled. Select to enable IGMP Snooping.

Step 7 Choose Enable from the Multicast Mobility Mode drop-down list to change the IGMP snooping status or to set the IGMP timeout. When IGMP snooping is enabled, the controller gathers IGMP reports from the clients and then sends each access point a list of the clients listening to any multicast group. The access point then forwards the multicast packets only to those clients.

The timeout interval has a range of 3 to 300 and a default value of 60. When the timeout expires, the controller sends a query to all WLANs. Those clients which are listening in the multicast group then send a packet back to the controller.

Step 8 If you enabled the Multicast Mobility Mode, enter the mobility group multicast address.

Step 9 Select the Multicast Direct check box to enable videos to be streamed over a wireless network.

Step 10 Choose Enable from the Multicast Mobility Mode drop-down list to change MLD configuration.

Step 11 Select the Enable MLD Snooping check box to enable IPv6 MLD snooping. If you have selected this check box, configure the following parameters:

- MLD Timeout—Enter the MLD timeout value in seconds. The timeout has a range of 3 to 7200 and a default value of 60.
- MLD Query Interval—Enter the MLD query interval timeout value in seconds. The interval has a range of 15 to 2400 and a default value of 20.

Internet Group Management Protocol (IGMP) snooping enables you to limit the flooding of multicast traffic for IPv4. For IPv6, Multicast Listener Discovery (MLD) snooping is used.

Step 12 Configure the Session Banner information, which is the error information sent to the client if the client is denied or dropped from a Media Stream.

Step 13 Click Save.

Once saved, you can click Audit to perform an audit on this controller.

Related Topics

Change Controller General System Properties from the Network Devices Table, on page 462

Configure a Controller ‘s Advanced Timers to Reduce Failure Detection Time

Advanced timer configuration for FlexConnect and local mode is available for the controller on .

This feature is only supported on Release 6.0 controllers and later.

To configure the advanced timers, follow these steps:

Step 1 Choose Configuration > Network > Network Devices , then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Choose the controller for which you want to set timer configuration.

Step 3 From the left sidebar menu, choose System > AP Timers.

Step 4 In the AP Timers page, click the applicable Access Point Mode link: Local Mode or FlexConnect Mode.

Step 5 Configure the necessary parameters in the Local Mode AP Timer Settings page or in the FlexConnect Mode AP Timer Settings page accordingly.

- AP timer settings for Local Mode—To reduce the failure detection time, you can configure the fast heartbeat interval (between the controller and the access point) with a smaller timeout value. When the fast heartbeat timer expires (at every heartbeat interval), the access point determines if any data packets have been received from the controller within the last interval. If no packets have been received, the access point sends a fast echo request to the controller. You can then enter a value between 10 and 15 seconds.
- AP timer settings for FlexConnect—Once selected, you can configure the FlexConnect timeout value. Select the AP Primary Discovery Timeout check box to enable the timeout value. Enter a value between 30 and 3600 seconds. 5500 series controllers accept access point fast heartbeat timer values in the range of 1-10.

Step 6 Click Save.

Related Topics

Create WLANs on a Controller, on page 499

Create WLANs on a Controller

Because controllers can support 512 WLAN configurations, provides an effective way to enable or disable multiple WLANs at a specified time for a given controller.

To view a summary of the wireless local access networks (WLANs) that you have configured on your network, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click the Device Name of the applicable controller.

Step 3 From the left sidebar menu, choose WLANs > WLAN Configuration.

Step 4 Configure the required fields in the Configure WLAN Summary page.

Related Topics

View the WLANs Configured on a Controller, on page 499
Add Security Policies to WLANs on a Controller, on page 500
Configure Mobile Concierge (802.11u) on a Controller, on page 501
Add a WLAN to a Controller, on page 503
Delete a WLAN from a Controller, on page 504
Change the Admin Status of a Controller's WLANs, on page 504
View a Controller WLAN's Mobility Anchors, on page 505
Configure a Controller's WLAN AP Groups, on page 508

View the WLANs Configured on a Controller

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the Device Name of the wireless controller whose WLAN configurations you want to see.

Step 3 Click the Configuration tab.

Step 4 Under Features, chooseWLANs > WLAN Configuration. The WLAN Configuration summary page appears, displaying the list of WLANs currently configured on the controller, including each:

- WLAN ID
- The name of the WLAN configuration profile
- WLAN SSID
- The names of any active security policies
- The WLAN current administrative status (enabled or disabled)
- A link to the list of all currently scheduled WLAN configuration tasks

Step 5 To view WLAN configuration details, click the WLAN ID. The WLAN Configuration details page appears.

Step 6 Use the tabs (General, Security, QoS, and Advanced) to view or edit parameters for the WLAN. Whenever you change a parameter, click Save.

Related Topics

Add Security Policies to WLANs on a Controller, on page 500
Configure Mobile Concierge (802.11u) on a Controller, on page 501
Add a WLAN to a Controller, on page 503
Delete a WLAN from a Controller, on page 504
Change the Admin Status of a Controller's WLANs, on page 504
View a Controller WLAN's Mobility Anchors, on page 505

Add Security Policies to WLANs on a Controller

Step 1 Navigate to WLAN Configuration details page as described in View the WLANs Configured on a Controller.

Step 2 Click Policy Mappings tab.

Step 3 Click Add Row.

Step 4 Select a policy name that you want to map to the WLAN, from the drop-down list.

Step 5 Enter the priority. The priority ranges from 1 to 16.

Two policies cannot have the same priority.

Step 6 Click Save.

If you want to delete a policy, select the check box corresponding to the policy that you want to delete and click Delete.

Related Topics

View the WLANs Configured on a Controller, on page 499
Configure Mobile Concierge (802.11u) on a Controller, on page 501
Add a WLAN to a Controller, on page 503
Delete a WLAN from a Controller, on page 504
Change the Admin Status of a Controller's WLANs, on page 504
View a Controller WLAN's Mobility Anchors, on page 505

Configure Mobile Concierge (802.11u) on a Controller

Cisco Mobile Concierge is a solution that enables 802.1X-capable clients to interwork with external networks without pre-authorization. Mobile Concierge provides service availability information to clients that can help them to associate to available networks more quickly, easily, and securely.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:

- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click the Device Name of the wireless controller on which you want to configure Mobile Concierge.

Step 3 Click the Configuration tab.

Step 4 Under Features, choose WLANs > WLAN Configuration> . The WLAN Configuration summary page appears, displaying the list of WLANs currently configured on the controller,

Step 5 Click the WLAN ID of the WLAN on which you want to configure Mobile Concierge.

Step 6 Click the Hot Spot tab.

Step 7 Click the 802.11u Configuration sub-tab and complete the fields as follows:

a) Select the 802.11u Status check box to enable 802.11u on the WLAN.

b) Select the Internet Access check box to enable this WLAN to provide Internet services.

c) From the Network Type drop-down list, choose the appropriate description for the 802.11u service you want to configure on this WLAN. The following options are available:

- Private Network
- Private Network with Guest Access
- Chargeable Public Network
- Free Public Network
- Emergency Services Only Network
- Personal Device Network
- Test or Experimental
- Wildcard

d) Choose the authentication type that you want to configure for the 802.11u parameters on this network:

- Not configured
- Acceptance of Terms and Conditions
- Online Enrollment
- DNS Redirection
- HTTP/HTTPS Redirection

e) In the HESSID field, enter the Homogeneous Extended Service Set Identifier value. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS.

f) In the IPv4 Address Type field, choose the method of assigning IPv4 addresses:

- Not Available
- Public
- Port Restricted
- Single NAT Private
- Double NAT Private
- Port Restricted and Single NAT Private
- Port Restricted and Double NAT Private
- Unknown

g) In the IPv6 Address Type field, choose the method of assigning IPv6 addresses:

- Not Available
- Available
- Unknown

Step 8 Click the Others sub-tab and complete the fields as follows:

a) In the OUI List group box, click Add Row and enter the following details:

- OUI name
- Is Beacon
- OUI Index

Click Save to add the OUI (Organizationally Unique Identifier) entry to this WLAN.

b) In the Domain List group box, click Add Row and enter the following details:

- Domain Name—The domain name operating in the 802.11 access network.
- Domain Index—Choose the domain index from the drop-down list.

Click Save to add the domain entry to this WLAN.

c) In the Cellular section, click Add Row and enter the following details:

- Country Code—The 3-character cellular country code.
- Network Code—The 3-character cellular network code.

Click Save to add the cellular entry to this WLAN.

Step 9 Click the Realm sub-tab and complete the fields as follows:

a) Click Add Row and enter the realm name.
b) Click Save to add the realm entry to this WLAN.

Step 10 Click the Service Advertisements sub-tab and complete the fields as follows:

a) Select the MSAP Enable check box to enable service advertisements.
b) If you enable MSAP, enter the server index for this WLAN. The server index field uniquely identifies an MSAP server instance serving a venue that is reachable through the BSSID.

MSAP (Mobility Services Advertisement Protocol) is designed to be used primarily by mobile devices that are configured with a set of policies for establishing network services. These services are available for devices that offer higher-layer services, or network services that are enabled through service providers. Service advertisements use MSAP to provide services to mobile devices prior to association to a Wi-Fi access network. This information is conveyed in a service advertisement. A single-mode or dual-mode mobile device queries the network for service

advertisements before association. The device's network discovery and the selection function may use the service advertisements in its decision to join the network.

Step 11 Click the Hotspot 2.0 sub-tab and complete the fields as follows:

a) Choose the Enable option from the HotSpot2 Enable drop-down list.

b) In the WAM Metrics group box, specify the following:

- WAN Link Status—The link status. The valid range is 1 to 3.
- WAN SIM Link Status—The symmetric link status. For example, you can configure the uplink and downlink to have different speeds or same speeds.
- Up Link Speed—The uplink speed. The maximum value is 4,194,304 kbps.
- Down Link Speed—The downlink speed. The maximum value is 4,194,304 kbps.

c) In the Operator Name List, click Add Row and enter the following details:

- Operator Name—Specify the name of the 802.11 operator.
- Operator Index—Select an operator index. The range is from 1 to 32.
- Language Code—An ISO-14962-1997 encoded string defining the language. This string is a three character language code.

Click Save to add the operator to the list.

d) In the Port Config List, click Add Row and enter the following details:

- IP Protocol—The IP protocol that you want to enable. The following options are ESP, FTP, ICMP, and IKEV2.
- Port No—The port number that is enabled on this WLAN.
- Status—The status of the port.

Click Save to add the port configuration to the list.

Step 12 Click Save to save the Mobile Concierge configuration.

Related Topics

View the WLANs Configured on a Controller, on page 499
Add a WLAN to a Controller, on page 503
Delete a WLAN from a Controller, on page 504
Change the Admin Status of a Controller's WLANs, on page 504
Add Security Policies to WLANs on a Controller, on page 500
View a Controller WLAN's Mobility Anchors, on page 505

Add a WLAN to a Controller

Step 1 Choose Configuration > Template > Features & Technologies > Controller > WLANsWLAN Configuration.

Step 2 Hover your mouse cursor over the tool tip next to the template type and click New.

Step 3 Complete the required fields in the General, Security, QoS, Advanced, HotSpot, Policy Mappings tabs, and then click Save as New Template.

Step 4 Proceed to deploy the template by click Deploy.

Related Topics

View the WLANs Configured on a Controller, on page 499
Configure Mobile Concierge (802.11u) on a Controller, on page 501
Delete a WLAN from a Controller, on page 504
Change the Admin Status of a Controller's WLANs, on page 504
Add Security Policies to WLANs on a Controller, on page 500
View a Controller WLAN's Mobility Anchors, on page 505
Configure a Controller's WLAN AP Groups, on page 508

Delete a WLAN from a Controller

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Click the Device Name of the appropriate controller.
Step 3 From the left sidebar menu, choose WLANs > WLAN Configuration.
Step 4 Select the check boxes of the WLANs that you want to delete.
Step 5 Choose Select a command > Delete a WLAN > Go.
Step 6 Click OK to confirm the deletion.

Related Topics

View the WLANs Configured on a Controller, on page 499
Configure Mobile Concierge (802.11u) on a Controller, on page 501
Add a WLAN to a Controller, on page 503
Change the Admin Status of a Controller's WLANs, on page 504
Add Security Policies to WLANs on a Controller, on page 500
View a Controller WLAN's Mobility Anchors, on page 505

Change the Admin Status of a Controller's WLANs

lets you change the status of more than one WLAN at a time on any given controller. You can select multiple WLANs and select the date and time for that status change to take place.

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.
Step 2 Click the Device Name of the appropriate controller.
Step 3 From the left sidebar menu, choose WLANs > WLAN Configuration.
Step 4 Select the check boxes of the WLANs that you want to schedule for a status change.
Step 5 From the Select a command drop-down list, choose Schedule Status to open the WLAN Schedule Task Detail page.

The selected WLANs are listed at the top of the page.

Step 6 Enter a Scheduled Task Name to identify this status change schedule.
Step 7 Choose the new Admin Status (Enabled or Disabled) from the drop-down list.

Step 8 Choose the schedule time using the hours and minutes drop-down lists.

Step 9 Click the calendar icon to choose a schedule date or enter the date in the text box (MM/DD/YYYY).

Step 10 Select the appropriate Recurrence radio button to determine the frequency of the status change (Daily, Weekly, or No Recurrence).

Step 11 Click Submit to initiate the status change schedule.

Related Topics

View the WLANs Configured on a Controller, on page 499
Configure Mobile Concierge (802.11u) on a Controller, on page 501
Add a WLAN to a Controller, on page 503
Delete a WLAN from a Controller, on page 504
Add Security Policies to WLANs on a Controller, on page 500
View a Controller WLAN's Mobility Anchors, on page 505

View a Controller WLAN's Mobility Anchors

Mobility anchors are controllers defined as anchors for WLANs. Clients (that is, any 802.11 mobile station, such as a laptop) are always attached to one of the anchors.

You can use mobility anchors to restrict a WLAN to a single subnet, regardless of the client's network entry point. Users can access a public or guest WLAN throughout the enterprise but will still be restricted to a specific subnet. You can also use guest WLANs to provide geographical load balancing, as WLANs can represent a particular section of a building (such as a lobby, restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller encapsulates the packets and forwards them to the client.

A 2000 series controller cannot be designated as an anchor for a WLAN. However, a WLAN created on a 2000 series controllers can have a 4100 series controller or a 4400 series controller as its anchor.

The L2TP Layer 3 security policies are unavailable for WLANs configured with a mobility anchor.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose WLANs > WLAN Configuration.

Step 4 Click a WLAN ID to view the parameters for a specific WLAN.

Step 5 Click the Advanced tab.

Step 6 Click the Mobility Anchors link. displays the IP address and current status (for example, reachable) for each anchor.

Related Topics

View the WLANs Configured on a Controller, on page 499
Configure Mobile Concierge (802.11u) on a Controller, on page 501
Add a WLAN to a Controller, on page 503
Delete a WLAN from a Controller, on page 504
Change the Admin Status of a Controller's WLANs, on page 504
Add Security Policies to WLANs on a Controller, on page 500

Configuring 802.11r Fast Transition

An 802.11r-enabled WLAN provides faster and better roaming experience for wireless client devices. However, legacy devices that do not recognize fast transition (FT) authentication key-management (AKM) in a robust secure network information exchange (in beacons and probe responses) cannot join the 802.11r-enabled WLAN.

Procedure

	Command or Action	Purpose
Step 1	Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller to view all the wireless controllers.	
Step 2	Click the name of the corresponding controller.	
Step 3	From the left sidebar menu, choose WLANs > WLAN Configurationto access the WLAN Configuration page.	
Step 4	Click the corresponding WLAN ID to view the parameters for that specific WLAN.	
Step 5	Choose Security > Layer 2tab.	
Step 6	From the Layer 2 Security drop-down list, choose WPA+WPA2.	The Authentication Key Management parameters for Fast Transition are displayed
Step 7	Check or uncheck the Fast Transition check box to enable or disable Fast Transition. Fast Transition is enabled by default when you create a new WLAN, from Cisco WLC Release 8.3onwards. However, the existing WLANs will retain the current configuration when Cisco WLC upgrades to Release 8.3 from an earlier release.	
Step 8	Check or uncheck the Over the DS check box to enable or disable Fast Transition over a distributed system. This option is available only if you enable Fast Transition or if Fast Transition is adaptive.	

	Command or Action	Purpose
Step 9	In the Reassociation Timeout text box, enter the number of seconds after which the reassociation attempt of a client to an AP should time out. The valid range is 1 to 100 seconds.	This option is available only if you enable Fast Transition.
Step 10	Under Authentication Key Management, choose FT 802.1X or FT PSK. Check or uncheck corresponding check boxes to enable or disable the keys. If you check the FT PSK check box, from the PSK Format drop-down list, choose ASCII or HEX and enter the key value.	When Fast Transition adaptive is enabled, you can use only 802.1X and PSK.
Step 11	Click Save to save your settings.	

Configure Fastlane QoS

The Fastlane QoS feature provides better Quality of Service (QoS) treatment for Apple clients, when compared to other wireless clients. This feature is disabled by default.

Note Enable or disable this feature only during a maintenance window, when not many clients are connected. This is because there will be a disruption in service when all the WLANs and the network are disabled and enabled again.

Procedure

	Command or Action	Purpose
Step 1	Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.	
Step 2	Click the name of the corresponding controller.	
Step 3	From the left sidebar menu, choose WLANs > WLAN Configuration.	
Step 4	Click the corresponding WLAN ID to view the parameters for that specific WLAN.	
Step 5	Click theQoS tab.	
Step 6	Check the Fastlane check box to enable Fastlane QoS.	
Step 7	Click Save to save your settings.	

Disable Fastlane QoS

Note Fastlane must be disabled on all the WLANs before disabling Fastlane QoS.

Procedure

	Command or Action	Purpose
Step 1	Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.	
Step 2	Click Device Name of the appropriate controller.	
Step 3	From the left sidebar menu, choose WLANs > WLAN Configuration.	
Step 4	From the Select a Command drop-down list, choose Disable Fastlane.	
Step 5	Click Save to save your settings.	

Configure a Controller's WLAN AP Groups

Site-specific VLANs or AP (access point) groups allow you to segment WLANs into different broadcast domains. This will allow you to minimize the total number of broadcast domains, which permits more effective load balancing and bandwidth allocation.

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose WLAN > AP Groups. The AP groups summary page displays.

This page displays a summary of the AP groups configured on your network.

From here you can remove or view details of an AP group.

Step 4 Click the AP group name on the Access Points tab to view or edit its access point(s).

Step 5 Click the WLAN Profiles tab to view, edit, add, or delete WLAN profiles.

Related Topics

Create Controller WLAN AP Groups, on page 509
Delete Controller WLAN AP Groups, on page 510
Create WLANs on a Controller, on page 499
Audit Controller WLAN AP Groups to Locate Configuration Differences , on page 511

Create Controller WLAN AP Groups

Use the AP Groups detail page to add AP (access point) groups. Note that if the target controller is earlier than version 5.2, AP Groups are called AP Group VLANs .

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose WLAN > AP Groups.

Step 4 Choose Select a command > Add AP Groups > Go. The AP Groups details page displays.

Step 5 Create a new AP group, as follows:

a) Enter a name for the AP group.
b) Enter a description for the new AP group (this group description is optional).

Step 6 Add access points to the new AP group, as follows:

a) Click the Access Points tab.
b) Click Add. The Access Point page displays a list of available access points.
c) Select the check boxes of the access points you want to add.
d) Click Select.

Step 7 Add a WLAN profile, as follows:

a) Click the WLAN Profiles tab.
b) Click Add.

To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.

Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.

The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

c) Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.
d) Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.

To display all available interfaces, delete the current interface in the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

e) Select the NAC Override check box, if applicable. NAC override is disabled by default.
f) Specify the policy configuration parameters by clicking the Add/Edit link.

- Policy Name—Name of the policy.
- Policy Priority—Configure policy priority between 1 and 16. No two policies can have same priority.

Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.

g) When access points and WLAN profiles are added, click Save.

Step 8 (Optional): Add an RF profile, as follows:

a) Click the RF Profiles tab:

b) Complete the fields as follows:

- 802.11a—Choose an RF profile for APs with 802.11a radios.
- 802.11b—Choose an RF profile for APs with 802.11b radios.

Step 9 Add Hyperlocation configuration parameters, as follows:

- Click the Location Settings tab and configure the following:
  - Hyperlocation— By enabling this option, all the APs associated to that controller which have the Hyperlocation module will be enabled.
  - Packet Detection RSSI Minimum—Adjust this value to filter out weak RSSI readings from location calculation.
  - Scan Count Threshold for Idle Client Detection—The maximum permissible count of the idle clients detected while scanning.
  - NTP Server IP Address—Enter the valid NTP server IP address.This IP address is used by all APs for time synchronization.

Step 10 When you are finished adding APs, WLAN profiles, and RF profiles to the new AP Group, click Save.

Changing the WLAN-interface mapping in an AP Group removes the local VLAN mapping for FlexConnect APs in this group. These mappings need to be reconfigured after applying this change.

Related Topics

Configure a Controller's WLAN AP Groups, on page 508
Delete Controller WLAN AP Groups, on page 510
Audit Controller WLAN AP Groups to Locate Configuration Differences , on page 511

Delete Controller WLAN AP Groups

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose WLAN > AP Groups.

Step 4 Select the check box(es) of the AP Groups that you want to delete.

Step 5 Choose Select a command > Delete AP Groups > Go.

Step 6 Click OK to confirm the deletion.

Related Topics

Configure a Controller's WLAN AP Groups, on page 508
Create Controller WLAN AP Groups, on page 509
Audit Controller WLAN AP Groups to Locate Configuration Differences , on page 511

Audit Controller WLAN AP Groups to Locate Configuration Differences

It is possible for difference to occur between the values has stored for an AP group and the actual values stored in the current controller and access points device configurations. Auditing the AP group will help you determine if this has occurred and resolve them.

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose WLAN > AP Groups.

Step 4 Click the name of the access point group that you want to audit.

Step 5 Click Audit.

The Audit button is located at the bottom of the page, next to the Save and Cancel buttons

Related Topics

Create Controller WLAN AP Groups, on page 509
Delete Controller WLAN AP Groups, on page 510
Create WLANs on a Controller, on page 499

Information About Captive Portal Bypassing

A captive portal is a web page where users are redirected to when they connect to a network, which usually displays information about Terms of Service and also used for login Authentication WISPr is a draft protocol that enables users to roam between different wireless service providers. Some devices (for example, Apple iOS devices) have a mechanism using which they can determine if the device is connected to Internet, based on an HTTP WISPr request made to a designated URL. This mechanism is used for the device to automatically open a web browser when a direct connection to the Internet is not possible. This enables the user to provide his credentials to access the Internet. The actual authentication is done in the background every time the device connects to a new SSID.

The client device (Apple IOS device) sends a WISPr request to the controller, which checks for the user agent details and then triggers an HTTP request with a web authentication interception in the controller. After verification of the IOS version and the browser details provided by the user agent, the controller allows the client to bypass the captive portal settings and provides access to the Internet.

This HTTP request triggers a web authentication interception in the controller as any other page requests are performed by a wireless client. This interception leads to a web authentication process, which will be completed normally. If the web authentication is being used with any of the controller splash page features (URL provided by a configured RADIUS server), the splash page may never be displayed because the WISPr requests are made at very short intervals, and as soon as one of the queries is able to reach the designated server, any web redirection or splash page display process that is performed in the background is aborted, and the device processes the page request, thus breaking the splash page functionality. For example, Apple introduced an iOS feature to facilitate network access when captive portals are present. This feature detects the presence of a captive portal by sending a web request on connecting to a wireless network. This request is directed to

http://www.apple.com/library/test/success.html for Apple IOS version 6 and older, and to several possible target URLs for Apple IOS version 7 and later. If a response is received, then the Internet access is assumed to be available and no further interaction is required. If no response is received, then the Internet access is assumed to be blocked by the captive portal and Apple's Captive Network Assistant (CNA) auto-launches the pseudo-browser to request portal login in a controlled window. The CNA may break when redirecting to an ISE captive portal. The controller prevents this pseudo-browser from popping up.

You can now configure the controller to bypass WISPr detection process so the web authentication interception is only done when a user requests a web page leading to splash page load in user context, without the WISPr detection being performed in the background.

Configuring Captive Network Portal Bypass

Procedure

	Command or Action	Purpose
Step 1	Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.	
Step 2	Click a Device Name, then click the Configuration tab.	
Step 3	Choose System > General - System to access the General page.	
Step 4	From the Captive Network Assistant Bypass drop-down list, choose Enable.	

Configuring Captive Network Portal Bypass Per WLAN

Procedure

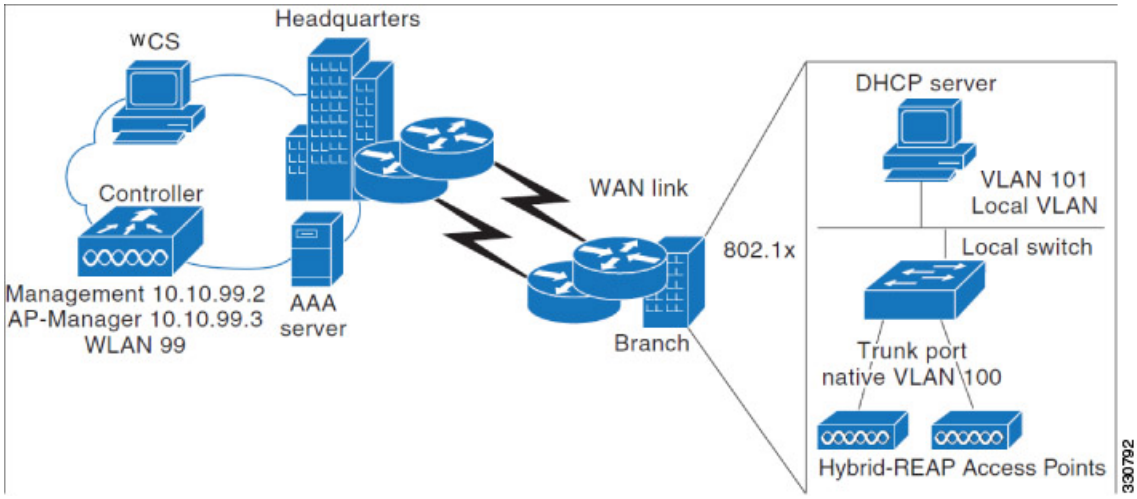
	Command or Action	Purpose
Step 1	Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.	
Step 2	Click a Device Name.	
Step 3	Choose WLANs > WLAN Configuration from the left sidebar menu.	
Step 4	Click the WLAN ID.	
Step 5	Click the Security > Layer 3 tab to modify the default security policy.	
Step 6	From the Captive Network Assistant Bypass drop-down list, choose Enable.	
Step 7	Click Save.	

Configure and Monitor APs Using FlexConnect

FlexConnect enables you to configure and control APs in a remote location from the corporate office through a wide area network (WAN) link without deploying a controller in each office. The FlexConnect APs switch client data traffic and perform client authentication locally when their connection to the controller is lost. When they are connected to the controller, they can also send traffic back to the controller.

The following figure illustrates a typical FlexConnect deployment.

Figure 18: FlexConnect Deployment



Related Topics

Supported Devices for FlexConnect, on page 513
Prerequisites for Using FlexConnect, on page 514
How FlexConnect Performs Authentication, on page 514
FlexConnect Operation Modes: Connected and Standalone, on page 515
FlexConnect States, on page 515

Supported Devices for FlexConnect

FlexConnect is supported only on these components:

- 1130AG, 1240AG, 1142, and 1252 APs
- Cisco 2000, and 4400 series controllers,
- Catalyst 3750G Integrated Wireless LAN Controller Switch
- Cisco Wireless Services Module (WiSM)
- Controller Network Module for Integrated Services Routers

Related Topics

Prerequisites for Using FlexConnect, on page 514
How FlexConnect Performs Authentication, on page 514
FlexConnect Operation Modes: Connected and Standalone, on page 515
FlexConnect States, on page 515

Prerequisites for Using FlexConnect

Follow these guidelines when you configure FlexConnect:

- You can deploy FlexConnect with either a static IP address or a DHCP address. The DHCP server must be available locally and must be able to provide the IP address for the AP during bootup.
- The maximum transmission unit (MTU) must be at least 500 bytes.
- Round-trip latency must not exceed 300 milliseconds (ms) between the AP and the controller. If the 300 milliseconds round-trip latency cannot be achieved, configure the AP to perform local authentication.
- The controller can send multicast packets in the form of unicast or multicast packets to the AP. In FlexConnect mode, the AP can receive multicast packets only in unicast form.
- FlexConnect supports CCKM full authentication but not CCKM fast roaming.
- FlexConnect supports a 1-1 network address translation (NAT) configuration and port address translation (PAT) for all features except true multicast. Multicast is supported across NAT boundaries when configured using the Unicast option.
- VPN, IPsec, L2TP, PPTP, Fortress authentication, and Cranite authentication are supported for locally switched traffic if these security types are accessible locally at the AP.
- NAC out-of-band integration is supported only on WLANs configured for FlexConnect central switching. It is not supported for use on WLANs configured for FlexConnect local switching.
- For FlexConnect APs, the interface mapping at the controller for WLANs configured for FlexConnect local switching is inherited at the AP as the default VLAN tagging. This can be easily changed per SSID and per FlexConnect AP. Non-FlexConnect APs tunnel all traffic back to the controller, and VLAN tagging is dictated by each interface mapping of the WLAN
- VLAN is not enabled on the FlexConnect AP by default. When FlexConnect is enabled, the AP inherits the VLAN ID associated to the WLAN. This configuration is saved in the AP and received after the successful join response. By default, the native VLAN is 1. One native VLAN must be configured per FlexConnect AP in a VLAN-enabled domain. Otherwise, the AP cannot send and receive packets to and from the controller. When the client is assigned a VLAN from the RADIUS server, that VLAN is associated to the locally switched WLAN.

Related Topics

How FlexConnect Performs Authentication, on page 514

How FlexConnect Performs Authentication

A FlexConnect AP searches for a controller on booting up. The AP joins the controller, downloads the latest software image from the controller and configuration information, and initializes the radio. It saves the downloaded configuration in non-volatile memory for use in standalone mode.

A FlexConnect AP identifies the controller IP address in one of the following ways:

- If the AP has been assigned an IP address from a DHCP server, it discovers a controller through the regular CAPWAP discovery process [Layer 3 broadcast, over-the-air provisioning (OTAP), DNS, or DHCP option 43]. OTAP does not work when the AP is booting up for the first time.
- If the AP has been assigned a static IP address, it discovers a controller through any of the CAPWAP discovery process methods except DHCP option 43. If the AP is unable to discover a controller through Layer 3 broadcast or OTAP, we recommend DNS resolution. With DNS, any AP with a static IP address that knows of a DNS server can find at least one controller.
- If you want the AP to discover a controller from a remote network where CAPWAP discovery mechanisms are not available, you can use priming. This method enables you to specify (through the AP command-line interface) the controller to which the AP should connect.

Related Topics

Supported Devices for FlexConnect, on page 513
Prerequisites for Using FlexConnect, on page 514
FlexConnect Operation Modes: Connected and Standalone, on page 515
FlexConnect States, on page 515

FlexConnect Operation Modes: Connected and Standalone

The two modes of operation for FlexConnect APs are:

- Connected mode— In this mode the FlexConnect AP has CAPWAP connectivity with the controller.
- Standalone mode—In this mode the controller is unreachable and the FlexConnect AP enters standalone mode and authenticates clients by itself.

When a FlexConnect AP enters standalone mode:

-
  - All clients that are on centrally switched WLANs are disassociated.
  - For 802.1X or web-authentication WLANs, existing clients are not disassociated, but the FlexConnect AP stops sending beacons when the number of associated clients reaches zero.
  - Disassociation messages are sent to new clients associating to 802.1X or web-authentication WLANs.
  - Controller-dependent activities such as 802.1X authentication, NAC, and web authentication (guest access) are disabled, and the AP does not send any Intrusion Detection System (IDS) reports to the controller.
  - Radio Resource Management (RRM) features (such as neighbor discovery; noise, interference, load, and coverage measurements, use of the neighbor list, and rogue containment and detection) are disabled. However, a FlexConnect AP supports dynamic frequency selection in standalone modes.

The FlexConnect AP maintains client connectivity even after entering standalone mode. However, once the AP reestablishes a connection with the controller, it disassociates all clients, applies new configuration information from the controller, and reallows client connectivity.

The LEDs on the AP change as the device enters different FlexConnect modes.

Related Topics

Supported Devices for FlexConnect, on page 513
Prerequisites for Using FlexConnect, on page 514
How FlexConnect Performs Authentication, on page 514
FlexConnect States, on page 515

FlexConnect States

The FlexConnect WLAN can be in any one of the following states depending on the configuration and state of controller connectivity:

- Central authentication, central switching—In this state, the controller handles client authentication, and all client data tunnels back to the controller. This state is valid only in connected mode.
- Central authentication, local switching—In this state, the controller handles client authentication, and the FlexConnect AP switches data packets locally. This state is supported only when the FlexConnect AP is in connected mode.
- Local authentication, local switching—In this state, the FlexConnect AP handles client authentication and switches client data packets locally. The authentication capabilities are present in the AP itself and

thus reduces the latency requirements. Local authentication can only be enabled on the WLAN of a FlexConnect AP that is in local switching mode.This state is valid in standalone mode and connected mode.

Local authentication is useful when the following conditions cannot be met:

- • A minimum bandwidth of 128 kbps.
  • Round trip latency no greater than 100 ms.
  • Maximum transmission unit (MTU) no smaller than 500 bytes.

Local authentication does not support:

- • Guest Authentication.
  • RRM information.
  • Local radius.
  • Roaming till the WLC and the other FlexConnect APs in the group are updated with the client information.
- Authentication down, switching down—In this state, the WLAN disassociates existing clients and stops sending beacon and probe responses. This state is valid only in standalone mode.
- Authentication down, local switching—In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive. This state is valid only in standalone mode.

The WLANS enter the following states when a FlexConnect AP enters the standalone mode:

- Local authentication, local switching state if the WLANs are configured as open, shared, WPA-PSK, or WPA2-PSK authentication and continue new client authentications.
- Authentication down, switching down state if the WLANs configured to central switching.
- Authentication down, local switching state if the WLANs configured to local-switch.

Related Topics

Supported Devices for FlexConnect, on page 513
Prerequisites for Using FlexConnect, on page 514
How FlexConnect Performs Authentication, on page 514
FlexConnect Operation Modes: Connected and Standalone, on page 515
How to Set Up and Use FlexConnect: Workflow, on page 516

How to Set Up and Use FlexConnect: Workflow

To configure FlexConnect, you must follow the instructions in this section in the following order:

1. Configure a Remote Switch for FlexConnect
2. Configure a Centrally-Switched WLAN Controller for FlexConnect
3. Configure a Locally-Switched WLAN Controller for FlexConnect
4. Configure a Centrally-Switched WLAN Controller for Guest Access
5. Configure FlexConnect on an AP
6. Connect Client Devices to the WLANs (FlexConnect)

Configure a Remote Switch for FlexConnect

To prepare the switch at the remote site, follow these steps:

Step 1 Connect the AP that is enabled for FlexConnect to a trunk or access port on the switch.

Step 2 Configure the switch to support the FlexConnect AP.

Related Topics

Example: Configure FlexConnect on Switches at Remote Sites, on page 517
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 519

Example: Configure FlexConnect on Switches at Remote Sites

In this sample configuration:

- The FlexConnect AP is connected to trunk interface FastEthernet 1/0/2 with native VLAN 100. The AP needs IP connectivity on the native VLAN.
- The remote site has local servers/resources on VLAN 101.
- A DHCP pool is created in the local switch for both VLANs in the switch.
- The first DHCP pool (NATIVE) is used by the FlexConnect AP, and the second DHCP pool (LOCAL-SWITCH) is used by the clients when they associate to a WLAN that is locally switched.

The addresses in this sample configuration are for illustration purposes only. The addresses that you use must fit into your upstream network.

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1

!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1

!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

Related Topics

Configure a Remote Switch for FlexConnect, on page 516
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 519

Configure a Centrally-Switched WLAN Controller for FlexConnect

To create a centrally switched WLAN:

Step 1 Choose Configuration > Network > Network Devices > Wireless Controllers.

Step 2 Click the Device Name of the appropriate controller.

Step 3 From the left sidebar menu, choose WLAN > WLAN Configuration to access the WLAN Configuration page.

Step 4 Choose Add a WLAN from the Select a command drop-down list, and click Go.

Cisco APs can support up to 16 WLANs per controller. However, some Cisco APs do not support WLANs that have a WLAN ID greater than 8. In such cases when you attempt to create a WLAN the following message is displayed:

Not all types of AP support WLAN ID greater than 8, do you wish to continue?

Click OK to creates a WLAN with the next available WLAN ID.

If you have earlier deleted a WLAN that has a WLAN ID less than 8, then that ID is applied to the next created WLAN.

Step 5 Choose a template from the drop-down list to apply it to the controller.

To create a new WLAN template, click Click here link to be redirected to the template creation page.

Step 6 Choose WPA1+WPA2 from the Layer 2 Security drop-down list.

Step 7 Check the Status check box under General Policies to enable the WLAN.

If NAC is enabled and you have created a quarantined VLAN for use with this, make sure to select it from the Interface drop-down list under General Policies. Also, check the Allow AAA Override check box to ensure that the controller validates a quarantine VLAN assignment.

Step 8 Click Save.

Related Topics

Configure a Remote Switch for FlexConnect, on page 516
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 519

Configure a Locally-Switched WLAN Controller for FlexConnect

To create a locally switched WLAN:

Step 1 Create a new WLAN as described in Configure a Centrally-Switched WLAN Controller for FlexConnect , Step 1 to Step 5.

Step 2 Click the WLAN ID and modify the configuration parameters.

Choose WPA1+WPA2 from the Layer 2 Security drop-down list. Make sure you choose PSK authentication key management and enter a preshared key.

Step 3 Check the Admin Status check box to this WLAN.

Step 4 Check the FlexConnect Local Switching check box to enable local switching.

Step 5 Click Save to commit your changes.

Related Topics

Configure a Remote Switch for FlexConnect, on page 516
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 519

Configure a Centrally-Switched WLAN Controller for Guest Access

To create a Centrally Switched WLAN for Guest Access to tunnel guest traffic to the controller:

Step 1 Create a new WLAN as described in Configure a Centrally-Switched WLAN Controller for FlexConnect , Step 1 to Step 5.

Step 2 Click the WLAN to modify the following configuration parameters:

a) Choose None from the Layer 2 Security and Layer 3 Security drop-down lists on the Security tab.
b) Check the Web Policy check box.
c) Select Authentication.
d) Configure a preauthentication access control list (ACL) on the WLAN if you are using an external web server, and then choose this ACL as the WLAN preauthentication ACL.

Step 3 Check the Status check box under General Policies to enable the WLAN.

Step 4 Click Save to commit your changes.

What to do next

Related Topics

- Configure a Remote Switch for FlexConnect
- Configure a Centrally-Switched WLAN Controller for FlexConnect
- Configure a Locally-Switched WLAN Controller for FlexConnect
- Configure a Centrally-Switched WLAN Controller for Guest Access
- (templates chapter)

Related Topics

Configure a Remote Switch for FlexConnect, on page 516
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 518
Configure the Web Auth Authentication Type for a Controller WLAN, on page 414

Add Guests to a Centrally-Switched WLAN (FlexConnect)

To add a local user:

Step 1 Configuration > Templates > Features & Technologies , then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Select Security > AAA > Local Net Users from the left sidebar menu.

Step 3 Complete the required fields.

Step 4 From the Profile drop-down list, choose the appropriate SSID.

Step 5 Enter a description of the guest user account.

Step 6 Click Save as New Template.

Related Topics

Configure a Centrally-Switched WLAN Controller for Guest Access, on page 519

Configure FlexConnect on an AP

To configure an AP for FlexConnect, follow these steps:

Step 1 Add the AP physically to the network.

Step 2 Select Configuration > Wireless technologies > Access Point Radios.

Step 3 Select the AP from the AP Name list.

Step 4 Select Configuration > Templates > Lightweight Acess Points or Autonomous Access Points if the AP Mode field does not display FlexConnect.

If the AP Mode field displays FlexConnect skip to Step 8.

Step 5 Select the AP from the AP Name list. The Lightweight AP Template Detail page appears.

Step 6 Check the FlexConnect Mode supported check box to view all the profile mappings.

If you are changing the mode to FlexConnect and if the AP is not already in FlexConnect mode, all other FlexConnect parameters are not applied on the AP.

Step 7 Check VLAN Support check box and enter the number of the native VLAN on the remote network in the Native VLAN ID text box.

Step 8 Click the Apply/Schedule tab to save your changes.

Step 9 Click the Edit link in the Locally Switched VLANs section to change the number of VLANs from which a client IP address is obtained.

Step 10 Click Save to save your changes.

Repeat this procedure for any additional APs that need to be configured for FlexConnect at the remote site.

Related Topics

Configure a Remote Switch for FlexConnect, on page 516
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 518

Connect Client Devices to the WLANs (FlexConnect)

Follow the instructions for your client device to create profiles that connect to the WLANs you created while configuring the controller.

In our example, you create three profiles on the client:

1. To connect to the centrally switched WLAN, create a client profile that uses WPA/WPA2 with PEAP-MSCHAPV2 authentication. When the client becomes authenticated, it gets an IP address from the management VLAN of the controller.
2. To connect to the locally switched WLAN, create a client profile that uses WPA/WPA2 authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the local switch.
3. To connect to the centrally switched WLAN for Guest Access, create a profile that uses open authentication. When the client becomes authenticated, it gets an IP address from VLAN 101 on the network local to the AP. After the client connects, the local user types any HTTP address in the web browser. You are automatically directed to the controller to complete the web-authentication process. When the web login page appears, enter the username and password.

To see if data traffic of the client is being locally or centrally switched, choose Monitor > Devices > Clients.

Related Topics

Configure a Remote Switch for FlexConnect, on page 516
Configure a Centrally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Locally-Switched WLAN Controller for FlexConnect, on page 518
Configure a Centrally-Switched WLAN Controller for Guest Access, on page 519

Create AP Groups to Use with FlexConnect

FlexConnect enables you to configure and control APs in a remote location through a wide area network (WAN) link without deploying a controller in each location. There is no deployment restriction on the number of FlexConnect APs per location, but you can organize and group the APs.

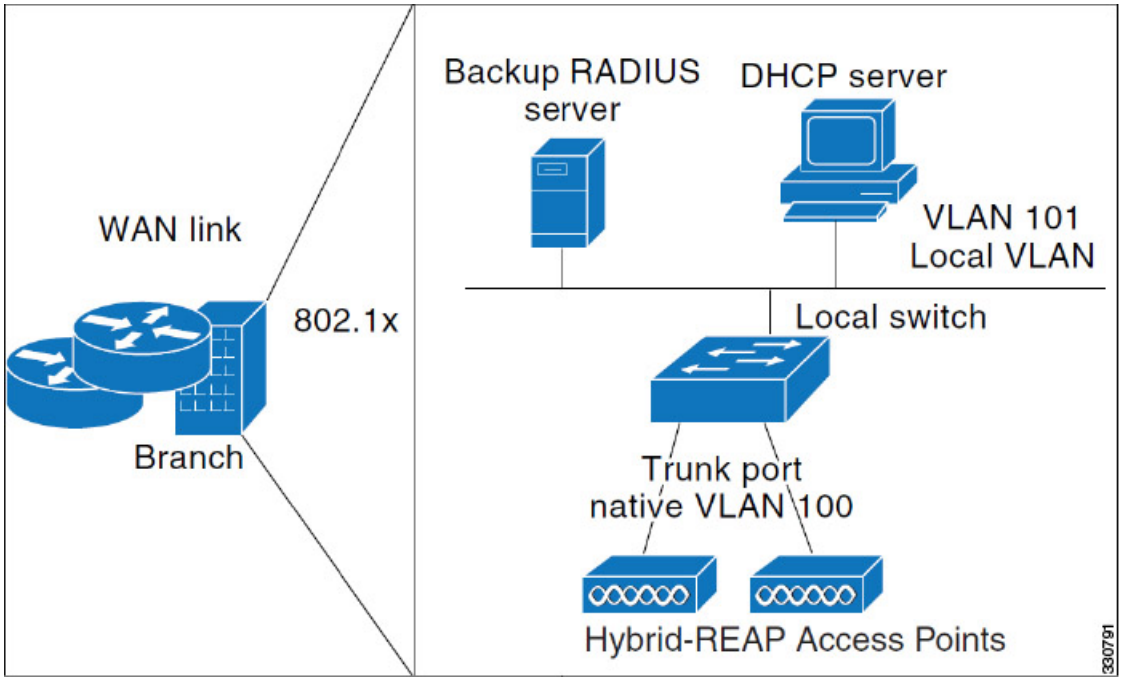
By forming AP groups with similar configurations, a procedure such as CCKM fast roaming can be processed faster than going through the controller individually.

For example, to activate CCKM fast roaming, the FlexConnect APs must know the CCKM cache for all devices that could associate with it. If you have a controller with 300 APs and 1000 devices that can potentially connect, it is quicker and more practical to process and send the CCKM cache for the FlexConnect group rather than for all 1000 devices. One particular FlexConnect group could focus on a small number of APs so that devices in that group connect to and roam between those few APs. With the established group, features such as CCKM cache and backup RADIUS are configured for the entire FlexConnect group rather than being configured in each AP.

All of the FlexConnect APs in a group share the same WLAN, backup RADIUS server, CCKM, and local authentication configuration information. This feature is helpful if you have multiple FlexConnect APs in a remote office or on the floor of a building and you want to configure them all at once. For example, you can configure a backup RADIUS server for a FlexConnect group rather than having to configure the same server on each AP.

The following figure illustrates a typical FlexConnect group deployment with a backup RADIUS server in the branch office.

Figure 19: FlexConnect Group Deployment



Related Topics

- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and CCKM
- FlexConnect Groups and Local Authentication
- Audit Controller FlexConnect AP Groups to Locate Configuration Differences

FlexConnect Groups and Backup RADIUS Servers

You can configure the controller to allow a FlexConnect AP in standalone mode to perform full 802.1x authentication to a backup RADIUS server. You can either configure a primary RADIUS server or both a primary and secondary RADIUS server.

Related Topics

- FlexConnect Groups and CCKM
- FlexConnect Groups and Local Authentication
- Audit Controller FlexConnect AP Groups to Locate Configuration Differences

FlexConnect Groups and CCKM

FlexConnect groups are required for CCKM fast roaming. When you configure your WLAN for CCKM fast secure roaming, EAP-enabled clients securely roam from one access point to another without the need to re-authenticate with the RADIUS server. Using CCKM, an access point uses a fast re-keying technique that enables Cisco client devices to roam from one access point to another typically in under 150 milliseconds. CCKM fast secure roaming ensures that there is no perceptible delay in time-sensitive applications. The

FlexConnect access points obtains the CCKM cache information for all the clients that might associate so they can process it quickly instead of sending it back to the controller.

For example, if you have a controller with 300 APs and 100 clients that might associate, sending the CCKM cache for all 100 clients is not practical. If you create a FlexConnect group comprising a limited number of APs, the clients roam only among those four APs, and the CCKM cache is distributed among those four APs only when the clients associate to one of them.

CCKM fast roaming between FlexConnect and non-FlexConnect APs is not supported.

Related Topics

- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and Local Authentication
- Audit Controller FlexConnect AP Groups to Locate Configuration Differences

FlexConnect Groups and Local Authentication

You can configure the controller to allow a FlexConnect AP in standalone mode to perform LEAP or EAP-FAST authentication for up to 20 statically configured users. The controller sends the static list of usernames and passwords to each FlexConnect AP when it joins the controller. Each AP in the group authenticates only its own associated clients.

This feature is ideal for customers who are migrating from an autonomous AP network to a lightweight FlexConnect AP network and are not interested in maintaining a large user database nor adding another hardware device to replace the RADIUS server functionality available in the autonomous AP.

LEAP or EAP-FAST authentication can be used in conjunction with the FlexConnect backup RADIUS server. If a FlexConnect group is configured with both a backup RADIUS server and local authentication, the FlexConnect AP always attempts to authenticate clients using the primary backup RADIUS server first, followed by the secondary backup RADIUS server (if the primary is not reachable), and finally the FlexConnect AP itself (if the primary and secondary RADIUS servers are not reachable).

Related Topics

- FlexConnect Groups and Backup RADIUS Servers
- FlexConnect Groups and CCKM
- Audit Controller FlexConnect AP Groups to Locate Configuration Differences

View Existing FlexConnect AP Groups

You can view a list of existing FlexConnect AP groups. To verify that an individual AP belongs to a FlexConnect group, click the Users configured in the group link. It takes you to the FlexConnect AP Group page, which shows the names of the groups and the APs that belong to it.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose FlexConnect > FlexConnect AP Groups. The FlexConnect AP Groups page opens.

Step 4 Click the group name to view details about the FlexConnect AP group.

Related Topics

Audit Controller WLAN AP Groups to Locate Configuration Differences , on page 511

Configure FlexConnect AP Groups

To configure a FlexConnect AP group, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose FlexConnect > FlexConnect AP Groups.

Step 4 From the Select a command drop-down list, click Add FlexConnect AP Group to open the FlexConnect AP Group > Add From Template pane.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click Apply.

Step 7 Configure the required FlexConnect AP Group parameters. You can add, edit, or remove any of the following mappings by clicking the required tab:

- VLAN-ACL Mapping—Valid VLAN ID range is 1-4094.
- WLAN-ACL Mapping—Select the FlexConnect access control list for external web authentication. You can add up to a maximum of 16 WebAuth ACLs.
- WebPolicy ACL—Select the FlexConnect access control list to be added as a web policy. You can add up to a maximum of 16 Web-Policy ACLs.
- Local Split
- Central DHCP
  - Central DHCP—When you enable this feature, the DHCP packets received from APs are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
  - Override DNS—You can enable or disable the overriding of the DNS server address on the interface assigned to the locally switched WLAN. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP, not from the controller.
  - NAT-PAT—You can enable or disable Network Address Translation (NAT) and Port Address Translation (PAT) on locally switched WLANs. You must enable Central DHCP Processing to enable NAT and PAT.

Step 8 To see if an individual access point belongs to a FlexConnect group, click the Users configured in the group link. The FlexConnect AP Group page shows the names of the groups and the access points that belong in it.

Step 9 Click Save.

Step 10 To delete an existing FlexConnect AP group, select the check box of the group you want to remove, and choose Delete FlexConnect AP Group from the Select a command drop-down list.

Related Topics

View Existing FlexConnect AP Groups, on page 523

Audit Controller FlexConnect AP Groups to Locate Configuration Differences

If the FlexConnect configuration changes over a period of time either on or the controller, you can audit the configuration. The changes are visible on subsequent screens. You can choose to synchronize the configuration by refreshing or the controller.

Related Topics

Configure FlexConnect AP Groups, on page 524
View Existing FlexConnect AP Groups, on page 523

Default FlexConnect Group

Default FlexConnect Group is a container where FlexConnect APs, which are not part of any administrator configured FlexConnect group, are added automatically when they join the controller. The Default FlexConnect Group is created and stored when the controller comes up (after upgrading from a previous release). You cannot add or delete this group manually. Also, you cannot manually add or delete access points to the Default FlexConnect Group. The APs in Default FlexConnect Group inherits the common configuration of the group. Any change in the group configuration is propagated to all the APs in the group.

When an administrator created group is deleted, all the APs from that group are moved to the Default FlexConnect Group and inherits the configuration of this group. Similarly, APs removed manually from other groups are also added to the Default FlexConnect Group.

When an AP from the Default FlexConnect Group is added to a customized group, the existing configuration (from Default FlexConnect Group) is deleted and the configuration from the customized group is pushed to the AP. If there is a standby controller, the Default FlexConnect Group and its configuration is also synchronized to it.

When an AP is converted from local to FlexConnect mode, and if it is not part of any administrator configured FlexConnect group, then it becomes part of Default FlexConnect group.

Note Efficient AP Image Upgrade feature is not supported with the Default FlexConnect AP group.

Related Topics

- Move APs from Default FlexConnect AP Group to another FlexConnect Group
- Default FlexConnect Group

Move APs from Default FlexConnect AP Group to another FlexConnect Group

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose FlexConnect > FlexConnect AP Groups.

Step 4 From the FlexConnect AP Groups, click the Group Name.

Step 5 In the FlexConnect AP tab, click + Add AP. The Add FlexConnect AP page shows the APs from the default FlexConnect group.

Step 6 Select any of the AP Name and click Add.

The selected AP will automatically added to the new group and gets deleted from the default FlexConnect group.

Step 7 Click Save.

Related Topics

Default FlexConnect Group, on page 525

Delete FlexConnect AP Group

Note You cannot delete the default FlexConnect group.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose FlexConnect > FlexConnect AP Groups.

Step 4 Click a Group Name and select Delete FlexConnect AP Group from the Select a Command drop-down list.

Step 5 Click OK to confirm the deletion.

Related Topics

Default FlexConnect Group, on page 525
Configure and Monitor APs Using FlexConnect, on page 513

Configure Security Settings for a Controller or Device

- Configure Client Exclusion Policies on Controllers
- View Cisco-Supplied IDS Signatures Applied to Controllers
- Create Custom IDS Signatures
- Configure a Controller's AP Authentication and Management Frame Protection
- Configure a Access Control List

Configure TFTP File Encryption for a Controller

You can configure file encryption to ensure that data is encrypted when you upload or download controller configuration files from a TFTP server.

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > File Encryption.

Step 4 Check the File Encryption check box.

Step 5 In the Encryption Key field, enter a text string of exactly 16 characters. Reenter the key in the Confirm Encryption Key field.

Step 6 Click Save.

Related Topics

Configure Security Settings for a Controller or Device, on page 526

Configure AAA Security for a Controller

This section describes how to configure controller security AAA parameters and contains the following topics:

- Configure Controller AAA General Parameters
- View Controller AAA RADIUS Auth Servers
- View Controller AAA RADIUS Acct Servers
- Configure AAA RADIUS Fallback Parameters on a Controller
- Configure AAA LDAP Servers on a Controller
- Configure AAA TACACS Servers on a Controller, on page 532
- View Controller AAA Local Net Users
- Configure AAA MAC Filtering on a Controller
- Configure AAA AP/MSE Authorization on a Controller
- Configure AAA Web Auth on a Controller

Configure Controller AAA General Parameters

The General page allows you to configure the local database entries on a controller.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > General - AAA.

Step 4 Enter the maximum number of allowed database entries. The valid range is 512 - 2048.

Step 5 In the Mgmt User Re-auth Interval, set the termination interval for management users.

Step 6 Reboot your server to apply the changes.

Related Topics

Configure AAA Security for a Controller, on page 527

View Controller AAA RADIUS Auth Servers

You can view a summary of existing RADIUS authentication servers

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Auth Servers. The following RADIUS Auth Servers parameters appear:

- Server Index—Access priority number for the RADIUS server (display only). Click to go to Configure IPaddr > RADIUS Authentication Server.
- Server Address—IP address of the RADIUS server (read-only).
- Port Number—Controller port number (read-only).
- Admin Status—Enable or Disable.
- Network User—Enable or Disable.
- Management User—Enable or Disable.

Related Topics

Configure AAA Security for a Controller, on page 527
Add AAA Auth Servers to a Controller, on page 528

Add AAA Auth Servers to a Controller

To add an authentication server, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Auth Servers.

Step 4 From the Select a command drop-down list, choose Add Auth Server to open the Radius Authentication Server > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click Apply.

To create a new template for Radius authentication servers, choose Configuration > Templates > Features and Technologies.

Related Topics

Configure AAA Security for a Controller, on page 527
View Controller AAA RADIUS Acct Servers, on page 529

View Controller AAA RADIUS Acct Servers

To view a summary of existing RADIUS accounting servers, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Acct Servers. RADIUS Acct Server parameters include the following:

- Server Index—Access priority number for the RADIUS server (read-only). Click to open the Radius Acct Servers Details page.
- To edit or audit the current accounting server parameters, click the Server Index for the applicable accounting server.
- Server Address—IP address of the RADIUS server (read-only).
- Port Number—Controller port number (read-only).
- Admin Status—Enable or Disable.
- Network User—Enable or Disable.

Related Topics

Configure AAA Security for a Controller, on page 527
Add an AAA Accounting Server to a Controller, on page 529

Add an AAA Accounting Server to a Controller

To add an accounting server, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Acct Servers.

Step 4 From the Select a command drop-down list, choose Add Acct Server to open the Radius Acct Servers Details > Add From Template page.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 From the drop-down list, choose a controller on which to apply to this template.

Step 7 Click Apply.

To create a new template for Radius accounting servers, choose Configuration > Templates > Features and Technologies > Controller > Security > AAA > RADIUS Acct Servers.

Related Topics

Configure AAA Security for a Controller, on page 527
View Controller AAA RADIUS Acct Servers, on page 529

Delete an AAA Accounting Server from a Controller

To delete an accounting server, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Acct Servers.

Step 4 Select the check box(es) for the applicable accounting server(s).

Step 5 From the Select a command drop-down list, choose Delete Acct Server.

Step 6 Click Go.

Step 7 Click OK in the pop-up dialog box to confirm the deletion.

Related Topics

Configure AAA Security for a Controller, on page 527
View Controller AAA RADIUS Acct Servers, on page 529

Configure AAA RADIUS Fallback Parameters on a Controller

To configure RADIUS fallback parameters, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > RADIUS Fallback.

Step 4 Make the required changes, then click Save.

Step 5 Click Audit to check the present configuration status of and the controller.

Related Topics

Configure AAA Security for a Controller, on page 527

Configure AAA LDAP Servers on a Controller

You can add and delete LDAP servers to controllers. supports LDAP configuration for both an anonymous or authenticated bind.

To access the LDAP Servers page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > LDAP Servers.

This page displays LDAP servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose an LDAP server for deletion.
- Server Index—A number assigned to identify the LDAP server. Click the index number to go the LDAP server configuration page.
- Server Address—The LDAP server IP address.
- Port Number—The port number used to communicate with the LDAP server.
- Admin Status—Server template status.
- Indicates if use of the LDAP server template is enabled or disabled.

Step 4 Click on a column title to toggle whether the information in sorted in ascending or descending order.

Related Topics

Configure AAA Security for a Controller, on page 527
Configure New AAA LDAP Bind Requests on a Controller, on page 532

Add AAA LDAP Servers to a Controller

To add an LDAP Server, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > LDAP Servers.

Step 4 From the Select a command drop-down list, choose Add LDAP Server.

Step 5 Click Go.

Related Topics

Configure AAA Security for a Controller, on page 527

Delete AAA LDAP Servers from a Controller

To delete the LDAP Server, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > LDAP Servers.

Step 4 Select the check box(es) of the LDAP servers that you want to delete.

Step 5 From the Select a command drop-down list, choose Delete LDAP Servers.

Step 6 Click Go.

Related Topics

Configure AAA Security for a Controller, on page 527

Configure New AAA LDAP Bind Requests on a Controller

supports LDAP configuration for both an anonymous or authenticated bind. A bind is a socket opening that performs a lookup.

To configure LDAP bind requests, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > LDAP Servers.

Step 4 Click a value under the Server Index column.

Step 5 From the Bind Type drop-down list, choose Authenticated or Anonymous. If you choose Authenticated, you must enter a bind username and password as well.

Step 6 In the Server User Base DN text box, enter the distinguished name of the subtree in the LDAP server that contains a list of all the users.

Step 7 In the Server User Attribute text box, enter the attribute that contains the username in the LDAP server.

Step 8 In the Server User Type text box, enter the ObjectType attribute that identifies the user.

Step 9 In the Retransmit Timeout text box, enter the number of seconds between retransmissions. The valid range is 2 to 30 seconds, and the default value is 2 seconds.

Step 10 Select the Admin Status check box if you want the LDAP server to have administrative privileges.

Step 11 Click Save.

Related Topics

Configure AAA Security for a Controller, on page 527

Configure AAA TACACS Servers on a Controller

You can delete TACACS+ servers from the controllers. To access the TACACS+ Servers page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > TACACS+ Servers.

This page displays TACACS+ servers currently used by this controller and contains the following parameters:

- Check box—Select the check box to choose a TACACS+ server for deletion.
- Server Type—The TACACS+ server type—accounting, authorization, or authentication.

- Server Index—A number assigned to identify the TACACS+ server and set its use priority. Click the index number to go the TACACS+ server configuration page.
- Server Address—The TACACS+ server IP address.
- Port Number—The port number used to communicate with the TACACS+ server.
- Admin Status—Server template status. Indicates if use of the TACACS+ server template is enabled.

Step 4 Choose Delete TACACS+ Servers from the Select a command drop-down list, then click Go to delete all TACACS+ servers with a selected check box from the controller.

Step 5 Click on a column title to toggle whether the information in sorted in ascending or descending order.

Related Topics

Configure AAA Security for a Controller, on page 527

View Controller AAA Local Net Users

You can view summary of the existing local network user controllers for clients who are allowed to access a specific WLAN. This is an administrative bypass of the RADIUS authentication process. Layer 3 Web Authentication must be enabled. The client information is passed to the RADIUS authentication server first, and if the client information does not match a RADIUS database entry, this local database is polled. Clients located in this database are granted access to network services if the RADIUS authentication fails or does not exist.

To view existing local network users, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > Local Net Users. The Local Net Users page displays the following local net user parameters:

- Username—User-defined identification.
- WLAN ID—Any WLAN ID, 1 through 16; 0 for all WLANs; 17 for third-party WLAN that this local net user is allowed to access.
- Description—Optional user-defined description.

Related Topics

Configure Local EAP on a Controller, on page 537
Delete AAA Local Net Users from a Controller, on page 533

Delete AAA Local Net Users from a Controller

To delete a local net user, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > Local Net Users.

Step 4 Select the check box(es) for the applicable local net user(s).

Step 5 From the Select a command drop-down list, choose Delete Local Net Users.

Step 6 Click Go.

Step 7 Click OK in the dialog box to confirm the deletion.

Related Topics

Configure AAA Security for a Controller, on page 527

Configure AAA MAC Filtering on a Controller

You can view MAC Filter information. You cannot use MAC address in the broadcast range.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > MAC Filtering. The MAC Filtering page displays the following parameters:

- MAC Filter Parameters
  - RADIUS Compatibility Mode—User-defined RADIUS server compatibility: Cisco ACS, FreeRADIUS, or Other.
  - MAC Delimiter—The MAC delimiters can be Colon (xx:xx:xx:xx:xx:xx), Hyphen (xx-xx-xx-xx-xx-xx), Single Hyphen (xxxxxx-xxxxxx), or No Delimiter (xxxxxxxxxxxx), as required by the RADIUS server.
- MAC Filters
  - MAC Address—Client MAC address. Click to open Configure IPaddr > MAC Filter.
  - WLAN ID—1 through 16, 17 = Third-party AP WLAN, or 0 = all WLANs.
  - Interface—Displays the associated Interface Name.
  - Description—Displays an optional user-defined description.

Step 4 From the Select a command drop-down list, choose Add MAC Filters to add a MAC Filter, Delete MAC Filters to delete the template(s), or Edit MAC Filter Parameters to edit the MAC Filters.

Step 5 Click Go.

Related Topics

Configure AAA Security for a Controller, on page 527

Configure AAA AP/MSE Authorization on a Controller

The AP/MSE Authorization page displays the access point policies and the list of authorized access points along with the type of certificate that an access point uses for authorization.

You cannot use MAC address in the broadcast range.

To access the AP/MSE Authorization page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > AP or MSE Authorization. The AP/MSE Authorization page displays the following parameters:

- AP Policies
  - Authorize APs—Enabled or Disabled.
  - Accept SSC-APs—Enabled or Disabled.
- AP/MSE Authorization
  - AP/MSE Base Radio MAC Address—The MAC address of the authorized access point. Click the AP/MSE Base Radio MAC Address to view AP/MSE Authorization details.
  - Type
  - Certificate Type—MIC or SSC.
  - Key Hash—The 40-hex long SHA1 key hash. The key hash is displayed only if the certificate type is SSC.

Related Topics

Configure AAA Security for a Controller, on page 527
Edit AAA AP/MSE Policies on a Controller, on page 535

Edit AAA AP/MSE Policies on a Controller

To edit AP/MSE Authorization access point policies, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > AP or MSE Authorization.

Step 4 From the Select a command drop-down list, select Edit AP Policies, then click Go.

Step 5 Edit the following parameters, if necessary:

- Authorize APs—Select the check box to enable access point authorization.
- Accept SSC-APs—Select the check box to enable the acceptance of SSE access points.

Step 6 Click Save to confirm the changes, Audit to perform an audit on these device values, or Cancel to close this page with no changes.

Related Topics

Configure AAA Security for a Controller, on page 527

Configure AAA Web Auth on a Controller

The Web Auth Configuration page enables the user to configure the web auth configuration type. If the type is configured as customized, the user downloaded web auth replaces the controller-provided internal web auth page.

To access the Web Auth Configuration page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > Web Auth Configuration.

Step 4 Select the Web Auth Type from the drop-down list.

Step 5 Configure the web auth parameters depending on the type chosen:

- Default Internal
  - Custom Redirect URL—URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page.
  - Logo Display—Enable or disable logo display.
  - Web Auth Page Title—Title displayed on web authentication page.
  - Web Auth Page Message—Message displayed on web authentication page.
- Customized Web Auth

  You can download an example login page and customizing the page. If you are using a customized web authentication page, it is necessary to download the example login.tar bundle file from the server, edit the login.html file and save it as either a .tar or .zip file, then download the .tar or .zip file to the controller.

  Click the preview image to download this sample login page as a TAR. After editing the HTML you might click here to redirect to the Download Web Auth page. See the Download Compressed Web Authorization Login Page Information to Controllers for more information.
- External
  - External Redirect URL—Location of the login.html on an external server on the network.

    If there are not any external web auth servers configured, you have the option of configuring one.

Configure an AAA Password Policy on a Controller

This page enables you to determine your password policy.

To make modifications to an existing password policy, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > AAA > Password Policy.

Step 4 Modify the password policy parameters as appropriate.

Step 5 Click Save.

If you disable password policy options, you see a "Disabling the strong password check(s) will be a security risk as it allows weak passwords" message.

Related Topics

Configure AAA Security for a Controller, on page 527

Configure Local EAP on a Controller

Local EAP is an authentication method that allows users and wireless clients to be authenticated locally. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down.

When you enable local EAP, the controller serves as the authentication server and the local user database, making it independent of an external authentication server. Local EAP retrieves user credentials from the local user database or the LDAP backend database to authenticate users.

Related Topics

Configure Local EAP General Parameters on a Controller, on page 537
View the Local EAP Profiles Used By a Controller, on page 538
Configure Local EAP General EAP-Fast Parameters on a Controller
Configure Local EAP General Network Users Priority on a Controller, on page 539

Configure Local EAP General Parameters on a Controller

You can specify a timeout value for local EAP. You can then add a template with this timeout value or make changes to an existing template.

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then re-authenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

To specify a timeout value for local EAP, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Local EAP > General - Local EAP.

Step 4 Enter the Local Auth Active Timeout in the Local Auth Active Timeout text box (in seconds). Local Auth Active Timeout refers to the timeout period during which Local EAP is always used after all Radius servers are failed.

Step 5 The following values should be adjusted if you are using EAP-FAST, manual password entry, one-time password, or 7920/7921 phones.

You must increase the 802.1x timeout values on the controller (default=2 seconds) for the client to obtain the PAC using automatic provisioning. We recommend the default timeout on the Cisco ACS server of 20 seconds.

- Local EAP Identify Request Timeout =1 (in seconds)
- Local EAP Identity Request Maximum Retries=20 (in seconds)
- Local EAP Dynamic Wep Key Index=0
- Local EAP Request Timeout=20 (in seconds)
- Local EAP Request Maximum Retries=2
- EAPOL-Key Timeout=1000 (in milli-seconds)
- EAPOL-Key Max Retries=2
- Max-Login Ignore Identity Response

Roaming fails if these values are not set the same across multiple controllers.

Step 6 Click Save.

Related Topics

Configure Local EAP on a Controller, on page 537
View the Local EAP Profiles Used By a Controller, on page 538
Configure Local EAP General EAP-Fast Parameters on a Controller
Configure Local EAP General Network Users Priority on a Controller, on page 539

View the Local EAP Profiles Used By a Controller

You can apply a template for a local EAP profile or make modifications to an existing template.

The LDAP backend database supports only these local EAP methods: EAP-TLS and EAP-FAST with certificates. LEAP and EAP-FAST with PACs are not supported for use with the LDAP backend database.

To view existing local EAP profiles, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Local EAP > Local EAP Profiles. The Local EAP Profiles page displays the following parameters:

- EAP Profile Name—User-defined identification.
- LEAP—Authentication type that leverages Cisco Key Integrity Protocol (CKIP) and MMH message integrity check (MIC) for data protection. A username and password are used to perform mutual authentication with the RADIUS server through the access point.
- EAP-FAST—Authentication type (Flexible Authentication via Secure Tunneling) that uses a three-phased tunnel authentication process to provide advanced 802.1x EAP mutual authentication. A username, password, and PAC (protected access credential) are used to perform mutual authentication with the RADIUS server through the access point.
- TLS—Authentication type that uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data. It requires a client certificate for authentication.
- PEAP—Protected Extensible Authentication Protocol.

Related Topics

Configure Local EAP on a Controller, on page 537
Add Local EAP Profiles to a Controller, on page 539

Add Local EAP Profiles to a Controller

To add a local EAP profile, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Local EAP > Local EAP Profile.

Step 4 From the Select a command drop-down list, choose Add Local EAP Profile.

Step 5 Choose a template from the Select a template to apply to this controller drop-down list.

Step 6 Click Apply.

Related Topics

Configure Local EAP on a Controller, on page 537
Configure Local EAP General Parameters on a Controller, on page 537
View the Local EAP Profiles Used By a Controller, on page 538
Configure Local EAP General EAP-Fast Parameters on a Controller
Configure Local EAP General Network Users Priority on a Controller, on page 539

Configure Local EAP General Network Users Priority on a Controller

To specify the order that LDAP and local databases use to retrieve user credential information, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Devices Groups menu on the left, select Device Type> Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Local EAP > Network Users Priority

Step 4 Use the left and right pointing arrows to include or exclude network credentials in the right-most list.

Step 5 Use the up and down buttons to determine the order credentials are attempted.

Step 6 Click Save.

Related Topics

Configure Local EAP on a Controller, on page 537
Configure Local EAP General Parameters on a Controller, on page 537
Configure a Controller's Web Auth Certificates, on page 540
Configure IP Sec CA Certificates on Controllers, on page 544

Configure a Controller's Web Auth Certificates

You can download a web authorization certificate or regenerate the internally-generated web auth certificate.

Caution Each certificate has a variable-length embedded RSA Key. The RSA key can vary from 512 bits, which is relatively insecure, through thousands of bits, which is very secure. When you are obtaining a new certificate from a certificate authority (such as the Microsoft CA), make sure the RSA key embedded in the certificate is at least 768 Bits.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Web Auth Certificate.

Step 4 Click Download Web Auth Certificate to access the Download Web Auth Certificate to Controller page.

Related Topics

Configure Local EAP General Parameters on a Controller, on page 537
Configure Local EAP on a Controller, on page 537

Configure a Controller User Login Policies

To configure the user login policies for controllers, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > User Login Policies.

Step 4 Enter the maximum number of concurrent logins allowed for a single username.

Step 5 Click Save.

Configure a Device's Manually Disabled Clients

The Disabled Clients page enables you to view excluded (blocklisted) client information.

Clients who fail to authenticate three times when attempting to associate are automatically blocked, or excluded, from further association attempts for an operator-defined timeout. After the Excluded timeout, the client is allowed to retry authentication until it associates or fails authentication and is excluded again.

You cannot use MAC address in the broadcast range.

To access the Manually Disabled Clients page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Manually Disabled Clients. The Manually Disabled Clients page displays the following parameters:

- MAC Address—Disabled Client MAC addresses. Click a list item to edit the disabled client description.
- Description—Optional description of disabled client.

Configure a Controller's Access Control Lists (ACLs)

You can view, edit, or add a new access control list (ACLs) for controllers.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Access Control Lists.

a) Check the check box to delete one or more ACLs

or

b) Click an ACL item to view its parameters.

Configure Controller ACL Rules, on page 541
Add ACL Security for Controller CPUs, on page 543

Configure Controller ACL Rules

You can create and modify access control list Access Control Lists (ACL) rules applied to controllers.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Access Control Lists.

Step 4 Click an ACL name to view and modify the parameters.

Step 5 Optionally check the check box to access control list rules.

Create New Controller ACL Rules

Step 1 Choose Device Type > Wireless Controller, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Access Control Lists.

Step 4 Click an ACL name.

Step 5 Click an applicable Seq#, or choose Add New Rule to access this page.

Configure Controller ACL Rules, on page 541
Add ACL Security for Controller CPUs, on page 543

Configure FlexConnect ACL Security for Controllers

The ACLs on FlexConnect provide a mechanism to cater to the need for access control at the FlexConnect access point for protection and integrity of locally switched data traffic from the access point.

Add FlexConnect ACLs on Controllers, on page 542
Delete FlexConnect ACLs for Controllers, on page 542

Add FlexConnect ACLs on Controllers

To add an Access Control List for FlexConnect access points, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > FlexConnect ACLs.

Step 4 From the Select a command drop-down list, choose Add FlexConnect ACLs.

Step 5 Click Go.

You cannot add a FlexConnect ACL if there is no template created. If you try to create an FlexConnect ACL when there are no templates available, you are redirected to the New Controller Templates page where you can create a template for FlexConnect ACL.

Step 6 Choose a template from the drop-down list to apply to the controller, and click Apply.

The FlexConnect ACL that you created appears in Configure > Controllers > IP Address > Security > FlexConnect ACLs.

Configure FlexConnect ACL Security for Controllers, on page 542

Delete FlexConnect ACLs for Controllers

To delete a FlexConnect ACL, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller .

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > FlexConnect ACLs.

Step 4 From the FlexConnect ACLs page, select one or more FlexConnect ACLs to delete.

Step 5 From the Select a command drop-down list, choose Delete FlexConnect ACLs.

Step 6 Click Go.

Configure FlexConnect ACL Security for Controllers, on page 542

Add ACL Security for Controller CPUs

Access control lists (ACLs) can be applied to the controller CPU to control traffic to the CPU.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > CPU Access Control Lists.

Step 4 Select the Enable CPU ACL check box to enable the CPU ACL. The following parameters are available:

- ACL Name—Choose the ACL to use from the ACL Name drop-down list.
- CPU ACL Mode—Choose which data traffic direction this CPU ACL list controls.

Configure FlexConnect ACL Security for Controllers, on page 542
Configure a Controller's Access Control Lists (ACLs), on page 541
Configure Controller ACL Rules, on page 541

View a Controller's Configured IDS Security Sensors

When the sensors identify an attack, they alert the controller to shun the offending client. When you add a new IDS (Intrusion Detection System) sensor, you register the controller with that IDS sensor so that the sensor can send shunned client reports to the controller. The controller also polls the sensor periodically.

To view IDS sensors, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > IDS Sensor Lists.

The IDS Sensor page lists all IDS sensors that have been configured for this controller. Click an IP address to view details for a specific IDS sensor.

Configure IP Sec CA Certificates on Controllers

A Certificate Authority (CA) certificate is a digital certificate issued by one certificate authority (CA) for another certification CA.

Import IP Sec Certificates to Controllers, on page 544
Paste IP Sec Certificates to Controllers, on page 544

Import IP Sec Certificates to Controllers

To import a CA certificate from a file, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 2 Click the device name of the applicable controller.
Step 3 From the left sidebar menu, choose Security > IP Sec Certificates > CA Certificate.
Step 4 Click Browse to navigate to the applicable certificate file.
Step 5 Click Open, then click Save.

Configure IP Sec CA Certificates on Controllers, on page 544

Paste IP Sec Certificates to Controllers

To paste a CA certificate directly, follow these steps:

Step 1 Copy the CA certificate to your computer clipboard.
Step 2 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 3 Click the device name of the applicable controller.
Step 4 From the left sidebar menu, choose Security > IP Sec Certificates > CA Certificate.
Step 5 Select the Paste check box.
Step 6 Paste the certificate directly into the text box.
Step 7 Click Save.

Configure IP Sec CA Certificates on Controllers, on page 544
Configure Network Identity (ID) Certificates on Controllers, on page 544
Configure a Controller's Web Auth Certificates, on page 540

Configure Network Identity (ID) Certificates on Controllers

This page lists the existing network Identity (ID) certificates by certificate name. An ID certificate can be used by web server operators to ensure secure server operation. ID certificates are available only if the controller is running Cisco Unified Wireless Network Software Version 3.2 or higher.

Import IP Sec Certificates to Controllers, on page 544
Paste IP Sec Certificates to Controllers, on page 544

Import ID Certificates to Controllers

To import an ID certificate from a file, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Configuration > Network > Network Devices.
Step 2 Click the device name of the applicable controller.
Step 3 From the left sidebar menu, choose Security > IP Sec Certificates > ID Certificate.
Step 4 From the Select a command drop-down list, choose Add Certificate.
Step 5 Click Go.
Step 6 Enter the Name and Password.
Step 7 Click Browse to navigate to the applicable certificate file.
Step 8 Click Open, then click Save.

Configure Network Identity (ID) Certificates on Controllers, on page 544

Paste ID Certificates to Controllers

To paste an ID certificate directly, follow these steps:

Step 1 Copy the ID certificate to your computer clipboard.
Step 2 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.
Step 3 Click the device name of the applicable controller.
Step 4 From the left sidebar menu, choose Security > IP Sec Certificates > ID Certificate.
Step 5 From the Select a command drop-down list, choose Add Certificate.
Step 6 Click Go.
Step 7 Enter the Name and Password.
Step 8 Select the Paste check box.
Step 9 Paste the certificate directly into the text box.
Step 10 Click Save.

Configure IP Sec CA Certificates on Controllers, on page 544
Configure Network Identity (ID) Certificates on Controllers, on page 544

Configure Wireless Protection Policies on Controllers

This section describes the wireless protection policy configurations and contains the following topics:

- Configure a Controller's AP Authentication and Management Frame Protection

Configure Rogue AP Policies on Controllers

You can set up policies for rogue access points. Make sure that rogue detection is enabled on the desired access points. Rogue detection is enabled by default for all access points joined to a controller (except for OfficeExtend access points). However, in software Release 6.0 or later, you can enable or disable rogue detection for individual access points by selecting or unselecting the Rogue Detection check box in the Access Point Details page.

Rogue detection is disabled by default for OfficeExtend access points because these access points, which are deployed in a home environment, are likely to detect a large number of rogue devices

To access the Rogue Policies page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Wireless Protection Policies > Rogue Policies. The following parameters appear:

- Rogue Location Discovery Protocol—RLDP determines whether or not the rogue is connected to the enterprise wired network. Choose one of the following from the drop-down list:
  - Disable—Disables RLDP on all access points. This is the default value.
  - All APs—Enables RLDP on all access points.
  - Monitor Mode APs—Enables RLDP only on access points in monitor mode.
- Rogue APs
  - Expiration Timeout for Rogue AP and Rogue Client Entries (seconds)—Enter the number of seconds after which the rogue access point and client entries expire and are removed from the list. The valid range is 240 to 3600 seconds and the default value is 1200 seconds.

    If a rogue access point or client entry times out, it is removed from the controller only if its rogue state is Alert or Threat for any classification type.
  - Rogue Detection Report Interval—Enter the time interval in seconds at which the APs should send the rogue detection report to the controller. Valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
  - Rogue Detection Minimum RSSI—Enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. Valid range is -70 dBm to -128 dBm, and the default value is -128 dBm. This feature is applicable to all the AP modes.

    There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.
  - Rogue Detection Transient Interval—Enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient

interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.

- Rogue Clients
  - Validate rogue clients against AAA—Select the check box to use the AAA server or local database to validate if rogue clients are valid clients. The default value is unselected.
  - Detect and report Adhoc networks—Select the check box to enable ad-hoc rogue detection and reporting. The default value is selected.

View Rogue AP Policies on Controllers, on page 547
Configure Client Exclusion Policies on Controllers, on page 547
View Cisco-Supplied IDS Signatures Applied to Controllers, on page 548
Create Custom IDS Signatures, on page 552
Configure a Controller's AP Authentication and Management Frame Protection , on page 553
Configure Wireless Protection Policies on Controllers , on page 545

View Rogue AP Policies on Controllers

This page enables you to view and edit current Rogue AP Rules.

To access the Rogue AP Rules page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Wireless Protection Policies > Rogue AP Rules. The Rogue AP Rules displays the Rogue AP Rules, the rule types (Malicious or Friendly), and the rule sequence.

Step 4 Click a Rogue AP Rule to view or edit its details.

Configure Client Exclusion Policies on Controllers, on page 547
View Cisco-Supplied IDS Signatures Applied to Controllers, on page 548
Create Custom IDS Signatures, on page 552
Configure a Controller's AP Authentication and Management Frame Protection , on page 553
Configure Wireless Protection Policies on Controllers , on page 545

Configure Client Exclusion Policies on Controllers

This page enables you to set, enable, or disable the client exclusion policies applied to the controller.

To access the Client Exclusion Policies page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Wireless Protection Policies > Client Exclusion Policies. The following parameters appear:

- Excessive 802.11a Association Failures—If enabled, clients are excluded on the sixth 802.11 association attempt, after five consecutive failures.
- Excessive 802.11a Authentication Failures—If enabled, clients are excluded on the sixth 802.11 authentication attempt, after five consecutive failures.
- Excessive 802.11x Authentication Failures—If enabled, clients are excluded on the fourth 802.1X authentication attempt, after three consecutive failures.
- Excessive 802.11 Web Authentication Failures—If enabled, clients are excluded on the fourth web authentication attempt, after three consecutive failures.
- IP Theft Or Reuse—If enabled, clients are excluded if the IP address is already assigned to another device.

Step 4 Click Save to save the changes made to the client exclusion policies and return to the previous page or click Audit to compare values with those used on the controller.

View Rogue AP Policies on Controllers, on page 547
View Cisco-Supplied IDS Signatures Applied to Controllers, on page 548
Create Custom IDS Signatures, on page 552
Configure a Controller's AP Authentication and Management Frame Protection , on page 553
Configure Wireless Protection Policies on Controllers , on page 545

Configure a Device's IDS Signatures

You can configure IDS Signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, an appropriate mitigation action is initiated.

Cisco supports 17 standard signatures on controllers.

View Cisco-Supplied IDS Signatures Applied to Controllers, on page 548
Create Custom IDS Signatures, on page 552
Configure a Controller's AP Authentication and Management Frame Protection , on page 553

View Cisco-Supplied IDS Signatures Applied to Controllers

The Standard Signature Parameters page shows the list of Cisco-supplied signatures that are currently on the controller.

To access the Standard Signatures page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Wireless Protection Policies > Standard Signatures. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Step 4 Click a signature name to view individual parameters and to enable or disable the signature.

Related Topics

Configure a Device's IDS Signatures, on page 548
Upload IDS Signature Files From Controllers, on page 550
Enabling and Disabling All IDS Signatures on a Controller, on page 550

Download IDS Signature Files to Controllers

To download a signature file, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Wireless Protection Policies > Standard Signatures or Security > Wireless Protection Policies > Custom Signatures.

Step 4 From the Select a command drop-down list, choose Download Signature Files.

Step 5 Click Go.

Step 6 Copy the signature file (*.sig) to the default directory on your TFTP server.

Step 7 Choose Local Machine from the File is Located On. If you know the filename and path relative to the server root directory, you can also choose TFTP server.

Step 8 Enter the maximum number of times the controller should attempt to download the signature file in the Maximum Retries.

Step 9 Enter the maximum amount of time in seconds before the controller times out while attempting to download the signature file in the Timeout.

Step 10 The signature files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click Browse to navigate to it. A “revision” line in the signature file specifies whether the file is a Cisco-provided standard signature file or a site-tailored custom signature file (custom signature files must always have revision=custom).

If the transfer times out for some reason, choose the TFTP server option in the File Is Located On field, and the server filename is populated for you and retried. The local machine option initiates a two-step operation. First, the local file is copied from the administrator workstation to own built-in TFTP server. Then the controller retrieves that file. For later operations, the file is already in server TFTP directory, and the downloaded web page now automatically populates the filename.

Step 11 Click OK.

Related Topics

Configure a Device's IDS Signatures, on page 548

Upload IDS Signature Files From Controllers

You can upload a signature file from controllers. Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the signature download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port cannot be routed.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port cannot be routed.
- A third-party TFTP server cannot run on the same computer as because built-in TFTP server and third-party TFTP server use the same communication port:

Step 1 Obtain a signature file from Cisco (standard signature file).

Step 2 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 3 Click the device name of the applicable controller.

Step 4 From the left sidebar menu, choose Security > Wireless Protection Policies > Standard Signatures or Security > Wireless Protection Policies > Custom Signatures.

Step 5 From the Select a command drop-down list, choose Upload Signature Files from controller.

Step 6 Specify the TFTP server name being used for the transfer.

Step 7 If the TFTP server is new, enter the TFTP IP address in the Server IP Address field.

Step 8 Choose Signature Files from the File Type drop-down list.

The signature files are uploaded to the root directory which was configured for use by the TFTP server. You can change to a different directory at the Upload to File field (this field only shows if the Server Name is the default server). The controller uses this local filename as a base name and then adds _std.sig as a suffix for standard signature files and _custom.sig as a suffix for custom signature files.

Step 9 Click OK.

Configure a Device's IDS Signatures, on page 548
Download IDS Signatures to Controllers, on page 457

Enabling and Disabling All IDS Signatures on a Controller

This command enables all signatures that were individually selected as enabled. If this text box remains unselected, all files are disabled, even those that were previously enabled. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.

To enable all standard and custom signatures currently on the controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the Select a command drop-down list, choose Edit Signature Parameters.

Step 4 Click Go.

Step 5 Select the Enable Check for All Standard and Custom Signatures check box.

Step 6 Click Save.

Configure a Device's IDS Signatures, on page 548

Enabling and Disabling Single IDS Signatures on a Controller

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the Select a command drop-down list, choose Edit Signature Parameters.

Step 4 Click an applicable Name for the type of attack you want to enable or disable.

The Standard Signature parameters page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. The following parameters are displayed in both the signature page and the detailed signature page:

- Precedence—The order, or precedence, in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Description—A more detailed description of the type of attack that the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. One possibility is None , where no action is taken, and another is Report, to report the detection.
- Frequency—The signature frequency or the number of matching packets per interval that must be identified at the detecting access point level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 50 packets per interval.
- Quiet Time—The length of time (in seconds) after which no attacks have been detected at the individual access point level, and the alarm can stop. This time appears only if the MAC information is all or both. The range is 60 to 32,000 seconds and the default value is 300 seconds.
- MAC Information—Whether the signature is to be tracked per network or per MAC address or both at the detecting access point level.
- MAC Frequency—The signature MAC frequency or the number of matching packets per interval that must be identified at the controller level before an attack is detected. The range is 1 to 32,000 packets per interval and the default value is 30 packets per interval.
- Interval—Enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds and the default value is 1 second.

- Enable—Select this check box to enable this signature to detect security attacks or unselect it to disable this signature.
- Signature Patterns—The pattern that is being used to detect a security attack.

Step 5 From the Enable drop-down list, choose Yes. Because you are downloading a customized signature, you should enable the files named with the _custom.sgi and disable the standard signature with the same name but differing suffix. For example, if you are customizing broadcast probe flood, you want to disable broadcast probe flood in the standard signatures but enable it in custom signatures.

Step 6 Click Save.

Configure a Device's IDS Signatures, on page 548
Configure Rogue AP Policies on Controllers, on page 546
View Rogue AP Policies on Controllers, on page 547
Create Custom IDS Signatures, on page 552
Configure Client Exclusion Policies on Controllers, on page 547
Configure a Controller's AP Authentication and Management Frame Protection , on page 553

Create Custom IDS Signatures

The Custom Signature page shows the list of customer-supplied signatures that are currently on the controller.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Wireless Protection Policies > Custom Signatures. This page displays the following parameters:

- Precedence—The order in which the controller performs the signature checks.
- Name—The type of attack the signature is trying to detect.
- Frame Type—Management or data frame type on which the signature is looking for a security attack.
- Action—What the controller is directed to do when the signature detects an attack. For example:
  - None—No action is taken.
  - Report—Report the detection.
- State—Enabled or Disabled.
- Description—A more detailed description of the type of attack the signature is trying to detect.

Step 4 Click a signature Name to view individual parameters and to enable or disable the signature.

Configure a Device's IDS Signatures, on page 548
Configure Rogue AP Policies on Controllers, on page 546
View Rogue AP Policies on Controllers, on page 547
Configure a Controller's AP Authentication and Management Frame Protection , on page 553

Configure a Controller's AP Authentication and Management Frame Protection

You can set the access point authentication policy and Management Frame Protection (MFP).

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > Wireless Protection Policies > AP Authentication and MFP.

This page displays the following fields:

- RF Network Name—Not an editable text box. The RF Network Name entered in the General parameters page is displayed here.
- Protection Type—From the drop-down list, choose one of the following authentication policies:
  - None—No access point authentication policy.
  - AP Authentication—Apply authentication policy.
  - MFP—Apply Management Frame Protection.
  - Alarm Trigger Threshold—(Appears only when AP Authentication is selected as the Protection Type). Set the number of hits to be ignored from an alien access point before raising an alarm.

The valid range is from 1 to 255. The default value is 255.

Configure a Device's IDS Signatures, on page 548
Configure Rogue AP Policies on Controllers, on page 546
View Rogue AP Policies on Controllers, on page 547
Create Custom IDS Signatures, on page 552
View Cisco-Supplied IDS Signatures Applied to Controllers, on page 548

URL ACL Configuration

URL filtering feature allows you to control access to Internet websites. It does so by permitting or denying access to specific websites based on information contained in a URL access control list (ACL). The URL filtering then restricts access based on the ACL list.

Using location based filtering, APs are grouped under various AP groups and WLAN profiles separate trusted and non-trusted clients within the same SSID. This forces re-authentication and new VLAN when a trusted client moves to a non-trusted AP or vice-versa.

The Wireless Controller (WLC) supports up to 64 ACLs and each ACL can contain up to 100 URLs. These ACLs are configured to either allow or deny requests, and can be associated with different interfaces (ex: WLAN, LAN), thus increasing effective filtering. Policies can be implemented locally on a WLAN or an AP group that is different from the applied global policy.

The number of rules (URLs) supported in each ACL varies for different WLCs:

- Cisco 5508 WLC and WiSM2 support 64 rules in per URL ACL.
- Cisco 5520, 8510, and 8540 WLCs support 100 rules per URL ACL.

Restrictions for URL Filtering and NAT

- Not supported on Cisco 2504 WLCs, vWLC, and Mobility Express.
- Supports WLAN Central Switching and not Local switching.
- Not supported in Flex mode with local switching.
- URL name is limited to 32 characters in length.
- No AVC Profile for the matched URLs. ACL Actions support for the Matched URLs.
- Allowed list and Blocked list can be created using the "*" implicit rule in the ACL to allow or deny requests respectively.
- HTTPS URLs are not supported.
- ACL may fail to filter in the following situations:
  - URL is across fragmented packets.
  - IP packets are fragmented.
  - Direct IP address or proxy setup used instead of URL
- These are currently not supported. If any URL matches with these conditions, it will not be considered for filtering.
  - Wildcard URLs (ex: www.uresour*loc.com)
  - Sub-URL (ex: www.uresour*loc.com/support)
  - Sub-Domain (ex: reach.url.com or sub1.url.com)
- If there is any duplicate URL present while creating the template, then the duplicate URL Rule is not considered

Configure a Access Control List

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Security > URL ACLs.

This page displays the following fields:

- Checkbox—Use the check box to select one or more URL ACLs to delete.
- URL ACL Name—User-defined name of this template. Click the URL ACL item to view the description.

Step 4 Click an URL ACL.

Step 5 Under Rules, click Add Row to add URL ACL rules.

- In the URL text box, enter the name for the URL ACLs.
- From the Rule Action, drop-down list, select Allow or Deny from the drop-down list.

Step 6 Click Save.

Configure Security Settings for a Controller or Device, on page 526
Delete an URL ACL, on page 555

Delete an URL ACL

To delete an URL ACL, follow these steps:

Step 1 Choose Configuration > Network > Network Devices.

Step 2 Click a controller Device Name.

Step 3 From the left sidebar menu, choose Security > URL ACLs.

Step 4 From the URL ACLs page, select one or more URL ACLs to delete.

Step 5 From the Select a command drop-down list, choose Delete URL ACLs.

Step 6 Click Go.

Note If you want to clear the counters for an ACL, from the select a command drop-down list, choose Clear Counters.

Related Topics

Configure a Access Control List, on page 554

Flexible Radio Assignment

Flexible Radio Assignment (FRA) is a new core algorithm added to Radio Resource Management (RRM) to analyze the NDP measurements and manage the hardware used to determine the role of the new Flexible Radio (2.4 GHz, 5 GHz, or Monitor) on Cisco Aironet 2800 and 3800 Series Access Points.

The FRA feature allows for either manual configuration of capable APs or for these APs to intelligently determine the operating role of the integrated radios based on the available RF environment. APs with flexible radio can automatically detect when a high number of devices are connected to a network and changes the dual radios in the access point from 2.4 GHz/5 GHz to 5 GHz/5 GHz to serve more clients. The AP performs this task while still monitoring the network for security threats and RF Interference that affects performance. FRA improves mobile user experience for high-density networks. This feature also reduces 2.4-GHz cell congestion by marking some of the 2.4GHz radios as redundant and switching them to 5GHz (client-serving role) or monitor role (2.4GHz and 5GHz). Use the CLI or GUI to configure the radio role.

An AP with flexible radio can operate in the following modes:

- Default operating mode—One radio serves clients in 2.4 GHz mode, while the other serves clients in 5 GHz mode.
- Dual 5 GHz Mode—Both radios operate in the 5 GHz band, actively serving clients to maximize the benefits of 802.11ac Wave 2 and to increase client device capacity.
- Wireless Security Monitoring—One radio serves 5 GHz clients and the other radio scans both 2.4 GHz and 5 GHz bands for wIPS attackers, CleanAir interferers, and rogue devices.

Configure Flexible Radio Assignment

Procedure

	Command or Action	Purpose
Step 1	Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.	
Step 2	Click the device name of the applicable controller.	

Step 3	From the left sidebar menu, choose 802.11 > Flexible Radio Assignment. Configure the following in the Flexible Radio Assignment page:
	• Flexible Radio Assignment—The FRA feature is disabled by default. Check the check box to enable FRA and configure the following parameters.
	• Sensitivity—Adjust the FRA sensitivity threshold. This sets the percentage of COF required o consider a radio as redundant. Supported values are:
	  • Low
	  • Medium
	  • High
	• Interval—Set the FRA run interval. Valid range is 1 hour to 24 hours. Default setting is 1 hour. FRA depends on DCA and hence the FRA interval cannot be lesser than the DCA interval.	

Configure a Device's 802.11 Parameters

This section describes the following sections:

- Set Multiple Country Codes on 802.11 Controllers
- Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing)
- Enable Band Selection to Reduce AP Channel Interference
- Ensure IP Multicast Delivery Using MediaStream
- Create RF Profiles That Can Be Used by AP Groups

Set Multiple Country Codes on 802.11 Controllers

To set multiple country support for a single controller that is not part of a mobility group, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose 802.11 > General from the left sidebar menu.

Step 4 Select the check box to choose which country you want to add. Access points are designed for use in many countries with varying regulatory requirements. You can configure a country code to ensure that it complies with your country regulations.

Access points might not operate properly if they are not designed for use in your country of operation. For example, an access point with part number AIR-AP1030-A-K9 (which is included in the Americas regulatory domain) cannot be used in Australia. Always be sure to purchase access points that match your country regulatory domain. For a complete list of country codes supported per product, see the following URL: http://www.cisco.com/warp/public/779/smbiz/wireless/approvals.html .

Step 5 Enter the time (in seconds) after which the authentication response times out.

Step 6 Click Save.

Related Topics

Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing), on page 557
Enable Band Selection to Reduce AP Channel Interference, on page 558
Ensure IP Multicast Delivery Using MediaStream, on page 560
Create RF Profiles That Can Be Used by AP Groups, on page 561

Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing)

Enabling aggressive load balancing on the controller allows lightweight access points to load balance the wireless clients across access points. Clients are load balanced between the access points on the same controller. Load balancing does not occur between access points on different controllers.

When a wireless client attempts to associate to a lightweight access point, association response packets are sent to the client with an 802.11 response packet including status code 17. This code indicates whether the access point can accept any more associations. If the access point is too busy, the client attempts to associate to a different access point in the area. The system determines if an access point is relatively more busy than its neighbor access points that are also accessible to the client.

For example, if the number of clients on AP1 is more than the number of clients on AP2 plus the load-balancing window, then AP1 is considered to be busier than AP2. When a client attempts to associate to AP1, it receives an 802.11 response packet with status code 17, indicating that the access point is busy, and the client attempts to associate to a different access point.

You can configure the controller to deny client associations up to 10 times (if a client attempted to associate 11 times, it is allowed to associate on the 11th try). You can also enable or disable load balancing on a particular WLAN, which is useful if you want to disable load balancing for a select group of clients (such as time-sensitive voice clients).

To configure aggressive load balancing, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller

Step 2 Click the device name of the applicable controller.

Step 3 Choose 802.11 > Load Balancing from the left sidebar menu. The Load Balancing page appears.

Step 4 Enter a value between 1 and 20 for the client window size. The page size becomes part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations:

load-balancing page + client associations on AP with lightest load = load-balancing threshold

In the group of access points accessible to a client device, each access point has a different number of client associations. The access point with the lowest number of clients has the lightest load. The client page size plus the number of clients on the access point with the lightest load forms the threshold. Access points with more client associations than this threshold is considered busy, and clients can associate only to access points with client counts lower than the threshold.

Step 5 Enter a value between 0 and 10 for the max denial count. The denial count sets the maximum number of association denials during load balancing.

Step 6 Click Save.

Step 7 To enable or disable aggressive load balancing on specific WLANs, browse to the WLAN Configuration page, and click the Advanced tab. For instructions on using the WLAN Configuration page, see Configuring Controller WLANs in Related Topics.

Related Topics

Set Multiple Country Codes on 802.11 Controllers, on page 556
Enable Band Selection to Reduce AP Channel Interference, on page 558
Ensure IP Multicast Delivery Using MediaStream, on page 560
Create RF Profiles That Can Be Used by AP Groups, on page 561
Create WLANs on a Controller, on page 499

Enable Band Selection to Reduce AP Channel Interference

Band selection enables client radios that are capable of dual-band (2.4- and 5-GHz) operation to move to a less congested 5-GHz access point. The 2.4-GHz band is often congested. Clients on this band typically experience interference from Bluetooth devices, microwave ovens, and cordless phones as well as co-channel interference from other access points because of the 802.11b/g limit of three non-overlapping channels. To combat these sources of interference and improve overall network performance, you can configure band selection on the controller.

Band selection works by regulating probe responses to clients. It makes 5-GHz channels more attractive to clients by delaying probe responses to clients on 2.4-GHz channels.

You can enable band selection globally on a controller, or you can enable or disable band selection for a particular WLAN, which is useful if you want to disable it for a select group of clients (such as time-sensitive voice clients).

Band-selection-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

Guidelines for Using Band Selection

Follow these guidelines when using band selection:

- Band selection can be used only with Cisco Aironet 1140 and 1250 series access points.
- Band selection operates only on access points that are connected to a controller. A FlexConnect access point without a controller connection does not perform band selection after a reboot.
- The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running.

- You can enable both band selection and aggressive load balancing on the controller. They run independently and do not impact one another.

To configure band selection:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose 802.11 > Band Select from the left sidebar menu. The Band Select page appears.

Step 4 Enter a value between 1 and 10 for the probe cycle count. The cycle count sets the number of suppression cycles for a new client. The default cycle count is 2.

Step 5 Enter a value between 1 and 1000 milliseconds for the scan cycle period threshold. This setting determines the time threshold during which new probe requests from a client come from a new scanning cycle. The default cycle threshold is 200 milliseconds.

Step 6 Enter a value between 10 and 200 seconds for the age out suppression field. Age-out suppression sets the expiration time for pruning previously known 802.11b/g clients. The default value is 20 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 7 Enter a value between 10 and 300 seconds for the age out dual band field. The age-out period sets the expiration time for pruning previously known dual-band clients. The default value is 60 seconds. After this time elapses, clients become new and are subject to probe response suppression.

Step 8 Enter a value between –20 and –90 dBm for the acceptable client RSSI field. This field sets the minimum RSSI for a client to respond to a probe. The default value is –80 dBm.

Step 9 Click Save.

Step 10 To enable or disable band selection on specific WLANs, browse to the WLAN Configuration page and click the Advanced tab. For instructions on using the WLAN Configuration page, see Configuring Controller WLANs in Related Topics.

Set Multiple Country Codes on 802.11 Controllers, on page 556
Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing), on page 557
Ensure IP Multicast Delivery Using MediaStream, on page 560
Create RF Profiles That Can Be Used by AP Groups, on page 561
Create WLANs on a Controller, on page 499

Control Priorities for SIP Calls

The Preferred Call feature enables you to specify highest priority to SIP calls made to some specific numbers. The high priority is achieved by allocating bandwidth to such preferred SIP Calls even when there is no available voice bandwidth in the configured Voice Pool. This feature is supported only for those clients that use SIP based CAC for bandwidth allocation in WCS or WLC.

You can configure up to 6 numbers per controller.

To configure the preferred call support, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose 802.11 > Preferred Call. The following fields appear if there is an existing preferred call:

- Description—Description for the preferred call.
- Number Id—Indicates the unique identifier for the controller and denotes one of the six preferred call numbers assigned to the controller.
- Preferred Number—Indicates the preferred call number.

Step 4 From the Select a command drop-down list, choose Add Number.

Step 5 Select a template to apply to this controller.

You need to select a template to apply to the selected controller. To create a New Template for Preferred Call Numbers, see Configuring Preferred Call Templates in Related Topics.

Step 6 Click Apply.

To delete a preferred call, select the check box for the applicable preferred call number and choose Delete from the Select a command drop-down list. Click Go and then click OK to confirm the deletion.

Related Topics

Set Multiple Country Codes on 802.11 Controllers, on page 556
Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing), on page 557
Enable Band Selection to Reduce AP Channel Interference, on page 558
Create RF Profiles That Can Be Used by AP Groups, on page 561

Ensure IP Multicast Delivery Using MediaStream

To configure media parameters for 802.11, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose 802.11 > Media Stream.

Step 4 In the Media Stream Configuration section, configure the following parameters

- Media Stream Name
- Multicast Destination Start IP—Start IP address of the media stream to be multicast
- Multicast Destination End IP—End IP address of the media stream to be multicast
- Maximum Expected Bandwidth—Maximum bandwidth that a media stream can use

Step 5 In the Resource Reservation Control (RRC) Parameters group box, configure the following parameters:

- Average Packet Size—Average packet size that a media stream can use.
- RRC Periodical Update—Resource Reservation Control calculations that are updated periodically; if disabled, RRC calculations are done only once when a client joins a media stream.
- RRC Priority—Priority of RRC with the highest at 1 and the lowest at 8.

- Traffic Profile Violation—Appears if the stream is dropped or put in the best effort queue if the stream violates the QoS video profile.
- Policy—Appears if the media stream is admitted or denied.

Step 6 Click Save.

Create RF Profiles That Can Be Used by AP Groups

The RF Profiles page enables you to create or modify RF profiles that get associated to AP Groups.

To configure a RF Profile for a controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Click RF Profiles or choose either 802.11 > RF Profiles from the left sidebar menu. The RF Profiles page appears. This page lists the existing RF Profile templates.

Step 4 If you want to add a RF profile, choose Add RF Profile from the Select a command drop-down list.

Step 5 Click Go. The New Controller Template page appears.

Step 6 Configure the following information:

- General
  - Template Name—User-defined name for the template. Profile Name—User-defined name for the current profile. Description—Description of the template.
  - Radio Type—The radio type of the access point. This is a drop-down list from which you can choose an RF profile for APs with 802.11a or 802.11b radios.
- TCP (Transmit Power Control)
  - Minimum Power Level Assignment (-10 to 30 dBm)—Indicates the minimum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Maximum Power Level Assignment (-10 to 30 dBm)—Indicates the maximum power assigned. The range is -10 to 30 dB, and the default value is 30 dB.
  - Power Threshold v1(-80 to -50 dBm)—Indicates the transmitted power threshold. Power Threshold v2(-80 to -50 dBm)—Indicates the transmitted power threshold.
- Data Rates—Use the Data Rates drop-down lists to specify the rates at which data can be transmitted between the access point and the client. These data rates are available:
  - 802.11a—6, 9, 12, 18, 24, 36, 48, and 54 Mbps.
  - 802.11b/g—1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, or 54 Mbps.

  For each data rate, choose one of these options:

  - Mandatory—Clients must support this data rate to associate to an access point on the controller.
  - Supported—Any associated clients that support this data rate might communicate with the access point using that rate. However, the clients are not required to be able to use this rate to associate.
  - Disabled—The clients specify the data rates used for communication.

Step 7 Click Save.

Related Topics

Set Multiple Country Codes on 802.11 Controllers, on page 556
Specify When Controllers Cannot Accept More Client Associations (AP Load Balancing), on page 557
Enable Band Selection to Reduce AP Channel Interference, on page 558

Configure a Device's 802.11a/n Parameters

To view 802.11a/n parameters for a specific controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose one of the following:

- 802.11a/n > Parameters to view or edit the parameters.
- 802.11a or n or ac > dot11a-RRM > RRM Thresholds to configure the 802.11a/n RRM threshold controller.
- 802.11a/n > RRM Intervals or 802.11b/g/n > RRM Intervals to configure the 802.11a/n or 802.11b/g/n RRM intervals for an individual controller.
- 802.11a/n-RRM > TPC to configure the 802.11a/n or 802.11b/g/n RRM Transmit Power Control.
- 802.11a or n or ac >dot11a-RRM > DCA to configure the RRM Dynamic Channel Allocation.
- 802.11a/n > RRM > RF Grouping to configure the 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller.
- 802.11a/n > Media Parameters to configure the media parameters for 802.11a/n.
- 802.11a/n > EDCA Parameters or 802.11b/g/n > EDCA to configure the 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller.
- 802.11a/n > Roaming Parameters to configure the 802.11a/n or 802.11b/g/n roaming parameters.
- 802.11a/n > 802.11h or 802.11b/g/n > 802.11h to configure the 802.11h parameters for an individual controller.
- 802.11a/n > High Throughput or 802.11b/g/n > High Throughput to configure the 802.11a/n or 802.11b/g/n high throughput parameters.
- 802.11a/n > CleanAir to configure 802.11a/n CleanAir parameters.

Step 4 Click Save.

Configure a Device's 802.11b/g/n Parameters

To view 802.11b/g/n parameters for a specific controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose one of the following:

- 802.11b/g/n Parameters to view or edit the parameters.
- 802.11b or g or n > dot11b-RRM > Thresholds to configure the 802.11b/g/n RRM Thresholds.
- 802.11a/n > RRM Intervals or 802.11b/g/n > RRM Intervals to configure the 802.11b/g/n RRM Intervals.
- 802.11b/g/n-RRM > TPC to configure the 802.11b/g/n RRM Transmit Power Control parameters.
- 802.11b or g or n > dot11b-RRM > DCA to configure the 802.11a/n or 802.11b/g/n RRM DCA channels for an individual controller
- 802.11b/g/n > RRM > RF Grouping to configure the 802.11a/n or 802.11b/g/n RRM Radio Grouping for an individual controller.
- 802.11b/g/n > Media Parameters to configure the media parameters for 802.11b/g/n.
- 802.11a/n > EDCA Parameters or 802.11b/g/n > EDCA to configure the 802.11a/n or 802.11b/g/n EDCA parameters for an individual controller.
- 802.11a/n > Roaming Parameters or 802.11b/g/n > Roaming Parameters to configure the 802.11a/n or 802.11b/g/n EDCA parameters.
- 802.11a/n > High Throughput or 802.11b/g/n > High Throughput to configure the 802.11a/n or 802.11b/g/n high throughput parameters.
- 802.11b/g/n > CleanAir to configure the 802.11b/g/n CleanAir parameters

Step 4 Click Save.

Configure a Device's Mesh Parameters

To configure Mesh parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Mesh > Mesh Settings.

Step 4 View or edit the following mesh parameters:

- RootAP to MeshAP Range —By default, this value is 12,000 feet. You can enter a value between 150 and 132,000 feet. Enter the optimum distance (in feet) that exists between the root access point and the mesh access point. This global field applies to all access points when they join the controller and all existing access points in the network.
- Client Access on Backhaul Link—Enabling this feature lets mesh access points associate with 802.11a wireless clients over the 802.11a backhaul. This is in addition to the existing communication on the 802.11a backhaul between

the root and mesh access points. This feature is applicable only to the access points with two radios. Changing Backhaul Client Access reboots all the mesh access points. See the “Client Access on 1524SB Dual Backhaul” in the Related Topics for more information.

The Mesh Background Scanning and Auto parent selection feature enables a mesh access point (MAP) to find and connect with a better potential parent across channels and maintain its uplink with the best parent all the time.

This feature eliminates the time consuming task of finding a parent across channels by scanning all the channels. The off-channel procedure transmits broadcast packets on selected channels (at a periodicity of 3 seconds, with a maximum of 50 milliseconds per off-channel) and receives packets from all 'reachable' neighbors. This keeps the child MAP updated with neighbor information across channels enabling it to 'switch' to a new neighbor and use it as a parent for the uplink. The 'switch' need not be triggered from parent loss detection, but on identifying a better parent while the child MAP still has its current parent uplink active.

- Background Scanning—Select the Background Scanning check box to enable mesh background scanning feature. The default value is disabled.
- Mesh DCA Channels— Enabling this option lets the backhaul channel to deselect on the controller using the DCA channel list. Any change to the channels in the Controller DCA list is pushed to the associated access points. This option is only applicable for 1524SB mesh access points. See “Backhaul Channel Deselection on Controllers” in the Related Topics for more information.
- Mesh RAP Downlink Backhaul—Changing backhaul downlink slot reboots all Mesh APs.
- Outdoor Access For UNII 1 Band Channels
- Global Public Safety— Enabling this option indicates that 4.9 Ghz can be used on backhaul link by selecting channel on the 802.11a backhaul radio. 4.9Ghz considered to be public safety band and is limited to some service providers. This setting applies at the controller level.
- Security Mode—Choose EAP (Extensible Authentication Protocol) or PSK (Pre-Shared Key) from the Security Mode drop-down list. Changing Security reboots all mesh access points.

Step 5 Click Save.

Related Topics

Enable Client Access to Backhaul Radios on 1524 SB APs, on page 564
Enable Backhaul Channel Deselection on Controllers, on page 565

Enable Client Access to Backhaul Radios on 1524 SB APs

The 1524 Serial Backhaul (SB) access point consists of three radio slots.

- Radio in slot-0 operates in 2.4 GHz frequency band and is used for client access.
- Radios in slot-1 and slot-2 operate in 5.8 GHz band and are primarily used for backhaul.

The two 802.11a backhaul radios use the same MAC address. There might be instances where the same WLAN maps to the same BSSID in more than one slot.

By default, client access is disabled over both the backhaul radios.

These guidelines must be followed to enable or disable a radio slot:

- You can enable client access on slot-1 even if client access on slot-2 is disabled.
- You can enable client access on slot-2 only when client access on slot-1 is enabled.
- If you disable client access on slot-1, then client access on slot-2 is automatically disabled.
- All the Mesh Access Points reboot whenever the client access is enabled or disabled.

The Universal Client Access feature allows client access over both the slot-1 and slot-2 radios. You can configure client access over backhaul radio from either one of the following:

- The Controller command-line interface (CLI)
- The Controller Graphical User Interface (GUI)
- GUI.

To configure client access on the two backhaul radios, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Mesh > Mesh Settings.

Step 4 Select the Client Access on Backhaul Link check box.

Step 5 Select the Extended Backhaul Client Access check box.

Step 6 Click Save.

A warning message is displayed:

Example:

```
Enabling client access on both backhaul slots will use same BSSIDs on both the slots. Changing Backhaul
 Client Access will reboot all Mesh APs.
```

Step 7 Click OK.

The Universal Client access is configured on both the radios.

Related Topics

Enable Backhaul Channel Deselection on Controllers, on page 565
Configure a Device's Mesh Parameters , on page 563

Enable Backhaul Channel Deselection on Controllers

To configure backhaul channel deselection, follow these steps:

Step 1 Configure the Mesh DCA channels flag on the controllers. See “Enable Client Access to Backhaul Radios on 1524 SB APs” in Related Topics.

Step 2 Change the channel list using configuration groups. See “Change the Controller Channel List Using Prime Infrastructure Configuration Groups” in Related Topics.

Related Topics

Enable Client Access to Backhaul Radios on 1524 SB APs, on page 564
Configure a Device's Mesh Parameters , on page 563
Change the Controller Channel List Using Configuration Groups, on page 566

Push Channel Changes from Controllers to 1524 SB APs

You can configure the Mesh DCA Channel flag to push each channel change on one or more controllers to all the associated 1524SB access points. To configure this feature, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Mesh > Mesh Settings.

Step 4 Select the Mesh DCA Channels check box to enable channel selection. This option is unselected by default.

The channel changes in the controllers are pushed to the associated 1524SB access points.

Change the Controller Channel List Using Configuration Groups

You can use controller configuration groups to configure backhaul channel deselection. You can create a configuration group and add the required controllers to the group and use the Country/DCA tab to select or deselect channels for the controllers in that group.

To configure backhaul channel deselection using configuration groups, follow these steps:

Step 1 Choose Configuration > Controller Configuration Groups.

Step 2 Select a configuration group to view its configuration group details.

Step 3 From the Configuration Group detail page, click the Country/DCA tab.

Step 4 Select or unselect the Update Country/DCA check box.

Related Topics

Enable Client Access to Backhaul Radios on 1524 SB APs, on page 564
Enable Backhaul Channel Deselection on Controllers, on page 565
Configure a Device's Mesh Parameters , on page 563
Push Channel Changes from Controllers to 1524 SB APs, on page 566

Configure a Device's Port Parameters

To configure Port parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then select Device Type > Wireless Controller.

Step 2 Click an applicable device.

Step 3 From the left sidebar menu, choose Ports > Port Settings.

Step 4 Click the applicable Port Number to open the Port Settings Details page. The following parameters are displayed:

- General Parameters:
  - Port Number—Read-only.
  - Admin Status—Choose Enabled or Disabled from the drop-down list.

- Physical Mode— Auto Negotiate (Read-only)
- Physical Status— Full Duplex 1000 Mbps (Read-only).
- STP Mode—Choose 802.1D, Fast, or Off.
- Link Traps—Choose Enabled or Disabled.
- Power Over Ethernet
- Multicast Application Mode—Select Enabled or Disabled.
- Port Mode SFP Type— Read-only

- Spanning Tree Protocol Parameters:
  - Priority—The numerical priority number of the ideal switch.
  - Path Cost—A value (typically based on hop count, media bandwidth, or other measures) assigned by the network administrator and used to determine the most favorable path through an internetwork environment (lower the cost, better the path).

Step 5 Click Save.

Related Topics

Configure a Device's Mesh Parameters , on page 563
Configure a Controller's Management Parameters , on page 567
Configure a Controller’s IPv6 Neighbor Binding and RA Parameters, on page 576
Configure a Controller’s Proxy Mobile IPv6 (PMIP) Parameters, on page 578
Configure a Controller’s Location Information, on page 574
Configure a Controller’s Multicast DNS (mDNS) Settings, on page 581
Configure a Controller’s Application Visibility and Control (AVC) Parameters, on page 583
Configure a Controller’s NetFlow Settings , on page 584

Configure a Controller's Management Parameters

The following management parameters of the controllers can be configured:

- Trap Receivers
- Trap Control
- Telnet and SSH
- Multiple Syslog servers
- Web Admin
- Local Management Users
- Authentication Priority

Related Topics

Configure Controller Traps, on page 568
Configure Syslog Servers on Controllers, on page 570
Configure Controller Telnet SSH Session Parameters, on page 570
Configure Web Admin Management on a Controller, on page 572
Configure Local Management Users on a Controller, on page 573
Configure Controller Management Authentication Server Priority, on page 573

Configure Trap Receivers for a Controller

The trap receiver parameter can be configured for individual wireless controllers. This parameter can be added / deleted from the wireless controller. A trap receiver can be added by creating a template under Configuration > Features & Technologies.

To configure trap receivers for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Management > Trap Receiver.

Step 4 The following parameters are displayed for current trap receivers:

- Community Name— Name of the trap receiver.
- IP Address—The IP address of the server.
- Admin Status—Status must be enabled for the SNMP traps to be sent to the receiver.

Step 5 Click a receiver Name to access its details.

Step 6 Select the Admin Status check box to enable the trap receiver. Unselect the check box to disable the trap receiver.

Step 7 Click Save.

Step 8 To delete a receiver / receivers, select the applicable receiver / receivers check-box.

Step 9 From the Select a command drop-down list, choose Delete Receivers.

Step 10 Click Go.

Step 11 Click OK in the confirmation message.

Configure Controller Traps

To configure trap control parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Management > Trap Control.

Step 4 The following traps can be enabled for this controller:

- Miscellaneous Traps:
  - SNMP Authentication—The SNMPv2 entity has received a protocol message that is not properly authenticated. When a user who is configured in SNMP V3 mode tries to access the controller with an incorrect password, the authentication fails and a failure message is displayed. However, no trap logs are generated for the authentication failure. Link (Port) Up/Down—Link changes status from up or down. Multiple Users—Two users login with the same login ID. Spanning Tree—Spanning Tree traps. See the STP specifications for descriptions of individual parameters. Rogue AP—Whenever a rogue AP is detected this trap is sent with its MAC address; For a rogue AP that was detected earlier and it no longer exists, this trap is sent. Config

Save—Notification sent when the controller configuration is modified. RFID Limit Reached Threshold— The maximum permissible value for RFID limit.

- Client Related Traps:
  - 802.11 Association—The associate notification is sent when the client sends an association frame. 802.11 Disassociation—The disassociate notification is sent when the client sends a disassociation frame. 802.11 Deauthentication—The deauthenticate notification is sent when the client sends a deauthentication frame. 802.11 Failed Authentication—The authenticate failure notification is sent when the client sends an authentication frame with a status code other than 'successful'. 802.11 Failed Association—The associate failure notification is sent when the client sends an association frame with a status code other than 'successful'. Excluded—The associate failure notification is sent when a client is excluded. 802.11 Authenticated— The authenticate notification is sent when the client sends an authentication frame with a status code 'successful'. MaxClients Limit Reached Threshold— The maximum permissible number of clients allowed.
- Cisco AP Traps:
  - AP Register—Notification sent when an access point associates or disassociates with the controller. AP Interface Up/Down—Notification sent when access point interface (802.11a or 802.11b/g) status goes up or down.
- Auto RF Profile Traps:
  - Load Profile—Notification sent when Load Profile state changes between PASS and FAIL. Noise Profile—Notification sent when Noise Profile state changes between PASS and FAIL. Interference Profile—Notification sent when Interference Profile state changes between PASS and FAIL. Coverage Profile—Notification sent when Coverage Profile state changes between PASS and FAIL.
- Auto RF Update Traps:
  - Channel Update—Notification sent when access point dynamic channel algorithm is updated. Tx Power Update—Notification sent when access point dynamic transmit power algorithm is updated.
- AAA Traps
  - User Auth Failure—This trap is to inform that a client RADIUS Authentication failure has occurred. RADIUS Server No Response—This trap is to indicate that no RADIUS server(s) are responding to authentication requests sent by the RADIUS client.
- 802.11 Security Traps:
  - WEP Decrypt Error—Notification sent when the controller detects a WEP decrypting error. Signature Attack—Notification sent when a signature attack is detected in the wireless controller that uses RADIUS Authentication.

Step 5 After selecting the applicable parameters, click Save.

Related Topics

Configure Trap Receivers for a Controller, on page 568
Configure Syslog Servers on Controllers, on page 570
Configure Controller Telnet SSH Session Parameters, on page 570
Configure Web Admin Management on a Controller, on page 572
Configure Local Management Users on a Controller, on page 573

Configure Controller Management Authentication Server Priority, on page 573

Configure Controller Telnet SSH Session Parameters

To configure Telnet SSH (Secure Shell) parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Management > Telnet SSH.

The following parameters can be configured:

- Session Timeout—Indicates the number of minutes a Telnet session is allowed to remain inactive before being logged off. A zero means there is no timeout. Might be specified as a number from 0 to 160. The factory default is 5.
- Maximum Sessions—From the drop-down list, choose a value from 0 to 5. This object indicates the number of simultaneous Telnet sessions allowed.
- Allow New Telnet Sessions—Indicates that new Telnet sessions are not allowed on the DS Port when set to no. The factory default value is no. New Telnet sessions can be allowed or disallowed on the DS (network) port. New Telnet sessions are always allowed on the Service port.
- Allow New SSH Sessions—Indicates that new Secure Shell Telnet sessions are not allowed when set to no. The factory default value is yes.

Step 4 After configuring the applicable parameters, click Save.

Related Topics

Configure Trap Receivers for a Controller, on page 568
Configure Syslog Servers on Controllers, on page 570
Configure Web Admin Management on a Controller, on page 572
Configure Local Management Users on a Controller, on page 573
Configure Controller Management Authentication Server Priority, on page 573

Configure Syslog Servers on Controllers

For Release 5.0.148.0 controllers or later, you can configure multiple (up to three) syslog servers on the WLAN controller. With each message logged, the controller sends a copy of the message to each configured syslog host, provided the message has severity greater than or equal to the configured syslog filter severity level.

To enable syslogs for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Management > Multiple Syslog.

The applied template is identified:

Syslog Server Address—Indicates the server address of the applicable syslog.

Step 4 Click Save.

Step 5 To delete syslog server(s), select the syslog server(s) check-box.

Step 6 From the Select a command drop-down list, choose Delete Syslog Servers.

Step 7 Click Go.

Step 8 Click OK in the confirmation message.

Related Topics

Configure Trap Receivers for a Controller, on page 568
Configure Controller Traps, on page 568
Configure Controller Telnet SSH Session Parameters, on page 570
Configure Web Admin Management on a Controller, on page 572
Configure Local Management Users on a Controller, on page 573
Configure Controller Management Authentication Server Priority, on page 573

Configure Network Assurance

To push client related data to a web server periodically, enable Network Assurance along with normal WLC functionality. This data is used as input for the newly introduces Assurance related dashboards. To configure Network Assurance for a controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Management > Network Assurance.

Step 4 You can view the applied template and configure the following parameters:

- Publish Data to Assurance Server - Global level field which controls network assurance feature.
- Data Externalization - A data model related setting on the controller. To enable Network Assurance, Data Externalization should be enabled first. A change in Data Externalization field value requires WLC reboot.
- NA Server URL - Server address to which WLC posts client data periodically. Server address can be host based or ip address based. If NA Server URL is host based, then NA Server CA Certificate should be generated on host name. Similarly, if URL is IP address based, then certificate should be generated with IP address.

Step 5 Click Save.

Related Topics

Download NA Server CA Certificate to Controllers
Generating Self Signed Certificates for Network Assurance
Configure Trap Receivers for a Controller, on page 568
Configure Syslog Servers on Controllers, on page 570
Configure Controller Telnet SSH Session Parameters, on page 570

Configure Web Admin Management on a Controller

This section provides instructions for enabling the distribution system port as a web port (using HTTP) or as a secure web port (using HTTPS). You can protect communication with the GUI by enabling HTTPS. HTTPS protects HTTP browser sessions by using the Secure Sockets Layer (SSL) protocol. When you enable HTTPS, the controller generates its own local web administration SSL certificate and automatically applies it to the GUI. You can download an externally generated certificate.

To enable WEB admin parameters for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Management > Web Admin.

The following parameters can be configured:

- WEB Mode—Choose Enable or Disable from the drop-down list. When enabled, users can access the controller GUI using http:ip-address. The default is Disabled. Web mode is not a secure connection.
- Secure Web Mode—Choose Enable or Disable from the drop-down list. When enabled, users can access the controller GUI using https://ip-address . The default is Enabled.
- Certificate Type— The Web Admin certificate must be downloaded.The controller must be rebooted for the new Web Admin certificate to take effect.
  - Download Web Admin Certificate—Click to access the Download Web Admin Certificate to Controller page. See “Download Web Auth or Web Admin Certificates to a Controller” for more information.

Download Web Auth or Web Admin Certificates to a Controller

To download a Web Auth or Web Admin Certificate to the controller, follow these steps:

Step 1 Click the Download Web Admin Certificate or Download Web Auth Certificate link.

Step 2 In the File is located on field, specify Local machine or TFTP server. If the certificate is located on the TFTP server, enter the server filename. If it is located on the local machine, click Browse and enter the local filename.

Step 3 Enter the TFTP server name in the Server Name text box. The default is the server.

Step 4 Enter the server IP address.

Step 5 In the Maximum Retries text box, enter the maximum number of times that the TFTP server attempts to download the certificate.

Step 6 In the Time Out text box, enter the amount of time (in seconds) that the TFTP server attempts to download the certificate.

Step 7 In the Local File Name text box, enter the directory path of the certificate.

Step 8 In the Server File Name text box, enter the name of the certificate.

Step 9 Enter the password in the Certificate Password text box.

Step 10 Re-enter the above password in the Confirm Password text box.

Step 11 Click OK.

Step 12 Click Regenerate Cert to regenerate the certificate.

Related Topics

Configure Trap Receivers for a Controller, on page 568
Configure Controller Traps, on page 568
Configure Controller Telnet SSH Session Parameters, on page 570
Configure Web Admin Management on a Controller, on page 572
Configure Local Management Users on a Controller, on page 573
Configure Controller Management Authentication Server Priority, on page 573

Configure Local Management Users on a Controller

This page lists the names and access privileges of the local management users. You can also delete the local management user.

To access the Local Management Users page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Management > Local Management Users.

Step 4 Click a username.

- User Name (read-only)—Name of the user.
- Access Level (read-only)—Read Write or Read Only.

Step 5 To delete the Local Management User, select the user(s) check-box.

Step 6 From the Select a command drop-list, choose Delete Local Management Users.

Step 7 Click Go.

Step 8 Click OK in the confirmation message.

Configure Trap Receivers for a Controller, on page 568
Configure Controller Traps, on page 568
Configure Controller Telnet SSH Session Parameters, on page 570
Configure Web Admin Management on a Controller, on page 572
Configure Controller Management Authentication Server Priority, on page 573

Configure Controller Management Authentication Server Priority

Authentication Priority is configured to control the order in which authentication servers are used to authenticate controller management users.

To access the Authentication Priority page, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Management > Authentication Priority.

Step 4 The local database is searched first. Choose either RADIUS or TACACS+ for the next search. If authentication using the local database fails, the controller uses the next type of server.

Step 5 Click Save.

Related Topics

Configure a Controller's Management Parameters , on page 567
Configure a Device's Mesh Parameters , on page 563
Configure a Device's Port Parameters , on page 566
Configure a Controller's Location Information, on page 574
Configure a Controller's IPv6 Neighbor Binding and RA Parameters, on page 576
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 578
Configure a Controller's Multicast DNS (mDNS) Settings, on page 581
Configure a Controller's Application Visibility and Control (AVC) Parameters, on page 583
Configure a Controller's NetFlow Settings , on page 584

Configure a Controller's Location Information

Currently WiFi clients are moving towards lesser probing to discover an AP. Smartphones do this to conserve battery power. The applications on a smartphone have difficulty generating probe request but can easily generate data packets and hence trigger enhanced location for the application. Hyperlocation is configured from WLC 8.1MR and . It is ultra-precise in locating beacons, inventory, and personal mobile devices. Some networks use multiple access points to get location coordinates within 5 to 7 meters of accuracy, but Hyperlocation can track locations to within a single meter.

To configure location configurations for an individual controller, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose Location > Location Configuration.

The Location Configuration page displays two tabs: General and Advanced.

Step 4 Add or modify the General parameters:

- RFID Tag Data Collection—Select the check box to enable the collection of data on tags.

Before the location server can collect asset tag data from controllers, you must enable the detection of active RFID tags using the CLI command config rfid status enable on the controllers.

- Location Path Loss Configuration
  - Calibrating Client—Select the check box to enable calibration for the client. Controllers send regular S36 or S60 requests (depending on the client capability) by way of the access point to calibrate clients. Packets are

transmitted on all channels. All access points gather RSSI data from the client at each location. These additional transmissions and channel changes might degrade contemporaneous voice or video traffic.

- Normal Client—Select the check box to have a non-calibrating client. No S36 requests are transmitted to the client. S36 is compatible with CCXv2 or later whereas S60 is compatible with CCXv4 or later.

- Measurement Notification Interval (in secs)
  - Tags, Clients, and Rogue APs/Clients—Allows you to set the NMSP measurement notification interval for clients, tags, and rogues. Specify how many seconds should elapse before notification of the found element (tags, clients, and rogue access points/clients).

Setting this value on the controller generates an out-of-sync notification which you can view in the Synchronize Servers page. When different measurement intervals exist between a controller and the mobility services engine, the largest interval setting of the two is adopted by the mobility services engine.

Once this controller is synchronized with the mobility services engine, the new value is set on the mobility services engine. Synchronization to the mobility services engine is required if changes are made to measurement notification interval.

- RSS Expiry Timeout (in secs)
  - For Clients—Enter the number of seconds after which RSSI measurements for normal (non-calibrating) clients must be discarded.
  - For Calibrating Clients—Enter the number of seconds after which RSSI measurements for calibrating clients must be discarded.
  - For Tags—Enter the number of seconds after which RSSI measurements for tags must be discarded.
  - For Rogue APs—Enter the number of seconds after which RSSI measurements for rogue access points must be discarded.

Step 5 Add or modify the Advanced parameters:

- RFID Tag Data Timeout (in secs)—Enter a value (in seconds) to set the RFID tag data timeout setting.
- Location Path Loss Configuration
  - Calibrating Client Multiband—Select the Enable check box to send S36 and S60 packets (where applicable) on all channels. Calibrating clients must be enabled in the general tab as well. To use all radios (802.11a/b/g/n) available, you must enable multiband.
- Hyperlocation Config Parameters
  - Hyperlocation— By enabling this option, all the APs associated to that controller which have the Hyperlocation module will be enabled.
  - Packet Detection RSSI Minimum—Adjust this value to filter out weak RSSI readings from location calculation.
  - Scan Count Threshold for Idle Client Detection—The maximum permissible count of the idle clients detected while scanning.
  - NTP Server IP Address—Enter the valid NTP server IP address.This IP address is used by all APs for time synchronization.
  - Azimuth angle — Refer below table for correct Azimuth values:

Table 48: Azimuth Values

Mount Position	Arrow Direction	Azimuth (in Degrees)	Elevation (in Degrees)
Ceiling Mount	South	90	0 (Up)

Mount Position	Arrow Direction	Azimuth (in Degrees)	Elevation (in Degrees)
East Wall Mount	East	0	90 (Down)
South Wall Mount	South	90	90 (Down)
West Wall Mount	West	180	90 (Down)
North Wall Mount	North	270	90 (Down)
Angled North Wall at 45degrees	North	270	45 (Down)

Tip Install the APs on the ceiling grid and if possible, try to align Hyperlocation arrow on AP so they all are pointing in the same direction. The recommendation is to mount APs in default orientation.

Step 6 Click Save.

Related Topics

Configure a Controller's Management Parameters , on page 567
Configure a Controller's IPv6 Neighbor Binding and RA Parameters, on page 576
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 578
Configure a Device's Mesh Parameters , on page 563
Configure a Device's Port Parameters , on page 566
Configure a Controller's Multicast DNS (mDNS) Settings, on page 581
Configure a Controller's Application Visibility and Control (AVC) Parameters, on page 583
Configure a Controller's NetFlow Settings , on page 584

Configure a Controller's IPv6 Neighbor Binding and RA Parameters

IPv6 can be configured with Neighbor Binding Timer and Router Advertisements (RA) parameters.

Related Topics

Configure Controller Neighbor Binding Timers, on page 576
Configure Router Advertisement Throttling on Controllers, on page 577
Configure RA Guard on Controllers, on page 577

Configure Controller Neighbor Binding Timers

To configure the Neighbor Binding Timers, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose IPv6 > Neighbor Binding Timers.

Step 4 The applied template will be displayed. Add or modify the following parameters:

- Down Lifetime Interval— This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

- Reachable Lifetime Interval—This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.
- Stale Lifetime Interval—This indicates the maximum time, in seconds. The range is 0 to 86,400 seconds, and the default value is 0.

Step 5 Click Save.

Configure Router Advertisement Throttling on Controllers

The RA Throttle Policy allows you to limit the amount of multicast Router Advertisements (RA) circulating on the wireless network.

To configure RA Throttle Policy, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose IPv6 > RA Throttle Policy.

Step 4 If you want to enable the RA Throttle Policy, select the Enable check box and configure the following parameters:

- Throttle Period—Duration of the throttle period in seconds. The range is 10 to 86,400 seconds.
- Max Through—The number of RA that passes through over a period or over an unlimited period. If the No Limit check-box is not enabled, the maximum pass-through number can be specified.
- Interval Option—Indicates the behavior in case of RA with an interval option.
  - Ignore
  - Passthrough
  - Throttle
- Allow At-least—Indicates the minimum number of RA not throttled per router.
- Allow At-most—Indicates the maximum or unlimited number of RA not throttled per router. If the No Limit check-box is not enabled, the maximum number of RA not throttled per router can be specified.

Step 5 Click Save.

Related Topics

Configure Controller Neighbor Binding Timers, on page 576
Configure RA Guard on Controllers, on page 577

Configure RA Guard on Controllers

RA Guard is a Unified Wireless solution to drop RA from wireless clients. It is configured globally, and by default it is enabled. You can configure IPv6 Router Advertisement parameters.

To configure RA Guard, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 From the left sidebar menu, choose IPv6 > RA Guard.

Step 4 If you want to enable the Router Advertisement Guard, select the Enable check box.

Step 5 Click Save.

Related Topics

Configure Controller Neighbor Binding Timers, on page 576
Configure Router Advertisement Throttling on Controllers, on page 577

Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters

Proxy Mobile IPv6 is a network-based mobility management protocol that supports a mobile node by acting as the proxy for the mobile node in any IP mobility-related signaling. The mobility entities in the network track the movements of the mobile node and initiate the mobility signaling and set up the required routing state.

The main functional entities are the Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). The LMA maintains the reachability state of the mobile node and is the topological anchor point for the IP address of the mobile node. The MAG performs the mobility management on behalf of a mobile node. The MAG resides on the access link where the mobile node is anchored. The controller implements the MAG functionality.

Related Topics

Configure PMIP Global Parameters on Controllers, on page 578
Configure PMIP Local Mobility Anchors on Controllers, on page 579
Configure PMIP Profiles on Controllers, on page 580

Configure PMIP Global Parameters on Controllers

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose PMIP > Global Configfrom the left sidebar menu.

Step 4 Configure the following fields:

- Domain Name—Read-only.
- MAG Name—Read-only.
- MAG Interface—Read-only.
- Maximum Bindings Allowed—Maximum number of binding updates that the controller can send to the MAG. The valid range is between 0 to 40000.
- Binding Lifetime—Lifetime of the binding entries in the controller. The valid range is between 10 to 65535 seconds. The default value is 65535. The binding lifetime should be a multiple of 4 seconds.

- Binding Refresh Time—Refresh time of the binding entries in the controller. The valid range is between 4 to 65535 seconds. The default value is 300 seconds. The binding refresh time should be a multiple of 4 seconds.
- Binding Initial Retry Timeout—Initial timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 1000 second.
- Binding Maximum Retry Timeout—Maximum timeout between the proxy binding updates (PBUs) when the controller does not receive the proxy binding acknowledgments (PBAs). The valid range is between 100 to 65535 seconds. The default value is 32000 seconds.
- Replay Protection Timestamp—Maximum amount of time difference between the timestamp in the received proxy binding acknowledgment and the current time of the day. The valid range is between 1 to 255 milliseconds. The default value is 7 milliseconds.
- Minimum BRI Retransmit Timeout—Minimum amount of time that the controller waits before retransmitting the BRI message. The valid range is between 500 to 65535 seconds.
- Maximum BRI Retransmit Timeout—Maximum amount of time that the controller waits before retransmitting the Binding Revocation Indication (BRI) message. The valid range is between 500 to 65535 seconds. The default value is 2000 seconds.
- BRI Retries—Number of BRI retries.
- MAG APN— Name of the Access Point Node of MAG.

Step 5 Click Save.

Related Topics

Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 578
Configure PMIP Local Mobility Anchors on Controllers, on page 579
Configure PMIP Profiles on Controllers, on page 580

Configure PMIP Local Mobility Anchors on Controllers

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose PMIP > LMA Configfrom the left sidebar menu.

Step 4 Configure the following fields:

- LMA Name—Name of the LMA connected to the controller.
- LMA IP Address—IP address of the LMA connected to the controller.

Step 5 Click Save.

Step 6 To delete the LMA configurations, select the applicable LMA config check-box.

Step 7 From the Select a command drop-list, choose Delete PMIP Local Configs.

Step 8 Click Go.

Step 9 Click OK in the confirmation message.

Related Topics

Configure PMIP Global Parameters on Controllers, on page 578
Configure PMIP Profiles on Controllers, on page 580
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 578

Configure PMIP Profiles on Controllers

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose PMIP PMIP Profile from the left sidebar menu.

Step 4 Enter the profile name.

Step 5 Click Add and then configure the following fields:

- Network Access Identifier—Name of the Network Access Identifier (NAI) associated with the profile.
- LMA Name—Name of the LMA to which the profile is associated.
- Access Point Node—Name of the access point node connected to the controller.

Step 6 Click Save.

Step 7 To delete the PMIP profiles, select the required PMIP profiles check-box.

Step 8 From the Select a command drop-list, choose Delete PMIP Local Configs.

Step 9 Click Go.

Step 10 Click OK in the confirmation message.

Related Topics

Configure PMIP Global Parameters on Controllers, on page 578
Configure PMIP Local Mobility Anchors on Controllers, on page 579
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 578

Configure a Controller's EoGRE Tunneling

Ethernet over GRE (EoGRE) is a solution for aggregating Wi-Fi traffic from hotspots. This solution enables customer-premises equipment (CPE) devices to bridge the Ethernet traffic coming from an end host, and encapsulate the traffic in Ethernet packets over an IP GRE tunnel. When the IP GRE tunnels are terminated on a service provider broadband network gateway, the end host's traffic is terminated and subscriber sessions are initiated for the end host.

To configure EoGRE tunneling, follow these steps:

Step 1 Choose Configuration > Network > Network Devices. then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose Tunneling > EoGRE from the left sidebar menu.

Step 4 From the Interface Name drop-down list, choose the source interface to tunnel.

Step 5 To create a tunnel gateway:

- Set the Heartbeat Interval. The default interval is 60 seconds.
- Set the Max Heartbeat Skip Count. The default value is set to 3. If the Tunnel Gateway (TGW) does not reply after three keepalive pings, Cisco WLC marks the TGW as nonoperational. The number of skip count decides how many times the TGW can skip consecutive replies, before the Cisco WLC knows that the TGW is nonoperational.
- Under Tunnel Gateway, click Add Row and configure tunnel gateway. You can create 10 such gateways.
  a. In the Tunnel Gateway Name field, enter the tunnel gateway name.
  b. In the Tunnel IP Addressfield, enter the tunnel IP address. Both IPv4 and IPv6 address formats are supported.
  c. Click Save.

     The default tunnel type is EoGRE.
  d. The Status can be UP or DOWN depending on the traps collected.
- Under Domain, click Add Row and configure the domain (domain is the grouping of two tunnel gateways).
  a. In theDomain Name text box, enter the domain name.
  b. From the Primary Gateway drop-down list, choose the primary tunnel gateway.
  c. From the Secondary Gateway drop-down list, choose the secondary tunnel gateway.

Step 6 Click Save.

Configure a Controller's Multicast DNS (mDNS) Settings

Multicast DNS (mDNS) service discovery provides a way to announce and discover services on the local network. mDNS perform DNS queries over IP multicast and supports zero configuration IP networking.

You can configure mDNS so that the controller can learn about the mDNS services and advertise these services to all clients.

There are two tabs in mDNS—Services and Profiles.

- Services tab—This tab enables you to configure the global mDNS parameters and update the Primary Services database.
- Profiles tab—This tab enables to view the mDNS profiles configured on the controller and create new mDNS profiles. After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority. By default, the controller has an mDNS profile, default-mdns-profile which cannot be deleted.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose mDNS > mDNS from the left sidebar menu.

Step 4 On the Services tab, configure the following parameters:

- Template Applied—The name of the template applied to this controller.
- Template Applied—The name of the template applied to this controller.
- Query Interval(10-120)—mDNS query interval, in minutes that you can set. This interval is used by WLC to send periodic mDNS query messages to services which do not send service advertisements automatically after they are started. The range is from 10 to 120 minutes. The default value is 15 minutes.
- rimary Services—Click Add Row and then configure the following fields:
  - Primary Service Name—Drop-down list from which you can choose the supported services that can be queried. To add a new service, enter or choose the service name, enter the service string, and then choose the service status. The following services are available

    :
  - AirTunes
  - AirPrint
  - AppleTV
  - HP Photosmart Printer1
  - HP Photosmart Printer2
  - Apple File Sharing Protocol (AFP)
  - Scanner
  - Printer
  - FTP
  - iTunes Music Sharing
  - iTunes Home Sharing
  - iTunes Wireless Device Syncing
  - Apple Remote Desktop
  - Apple CD/DVD Sharing
  - Time Capsule Backup

- Primary Services—Click Add Row and then configure the following fields:
- Primary Service Name—Name of the mDNS service.
- Service String—Unique string associated to an mDNS service. For example, _airplay._tcp.local. is the service string associated to AppleTV.
- Query Status—Check box that you select to enable an mDNS query for a service. Periodic mDNS query messages will be sent by WLC at configured Query Interval for services only when the query status is enabled; otherwise, service should automatically advertised for other services where the query status is disabled (for example AppleTV).

Step 5 On the Profiles tab, configure the following parameters:
'

- Profiles—Click Add Profile and then configure the following fields:
  - Profile Name—Name of the mDNS profile. You can create a maximum of 16 profiles.
  - Services—Select the services (using the check boxes) that you want to map to the mDNS profile.

Step 6 Click Save.

What to do next

By default, the controller creates an access policy, default-mdns-policy which cannot be deleted. This is displayed with the Group Name and Description. Select the policy to view its Service Group details.

Click Save after editing the fields.

Configure a Controller's Application Visibility and Control (AVC) Parameters

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1400 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, expensive network link usage, and infrastructure upgrades.

AVC is supported only on the Cisco 2500 and 5500 Series Controllers, and Cisco Flex 7500 and Cisco 8500 Series Controllers.

Set Up AVC Profiles on Controllers

To configure the AVC profile, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose Services > Application Visibility And Control > AVC Profilefrom the left sidebar menu.

Step 4 Click the AVC Profile Name that you want to configure.

Step 5 To create AVC rules, click Add.

Step 6 Configure the following parameters:.

- Application Name—Name of the application.
- Application Group Name—Name of the application group to which the application belongs.
- Action—Drop-down list from which you can choose the following:
  - Drop—Drops the upstream and downstream packets corresponding to the chosen application.
  - Mark— Marks the upstream and downstream packets corresponding to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.

- Rate Limit—If you select Rate Limit as an action, you can specify Average Rate Limit per client and Burst data rate limit. The number of rate limit applications is limited to 3. The default action is to permit all applications.

- DSCP—Packet header code that is used to define quality of service across the Internet. The DSCP values are mapped to the following QoS levels:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)— Provides lowest bandwidth for guest services.
  - Custom—Specify the DSCP value. The range is from 0 to 63.
- DSCP Value—This value can be entered only when Custom is chosen from the DSCP drop-down list.
- Avg. Rate Limit (in Kbps)—If you select Rate Limit as an action, you can specify Average Rate Limit per client which is the average bandwidth limit of that application.
- Burst Rate Limit (in Kbps)—If you select Rate Limit as an action, you can specify Burst Rate limit which is the peak limit of that application.

Step 7 Click Save.

Related Topics

Configure a Controller's Multicast DNS (mDNS) Settings, on page 581
Configure a Controller's NetFlow Settings , on page 584
Configure a Device's Mesh Parameters , on page 563
Configure a Device's Port Parameters , on page 566
Configure a Controller's Management Parameters , on page 567
Configure a Controller's Location Information, on page 574
Configure a Controller's IPv6 Neighbor Binding and RA Parameters, on page 576
Configure a Controller's Proxy Mobile IPv6 (PMIP) Parameters, on page 578

Configure a Controller's NetFlow Settings

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing by collecting IP traffic information from network devices. The NetFlow architecture consists of the following components:

- Collector—An entity that collects all the IP traffic information from various network elements.
- Exporter—A network entity that exports the template with the IP traffic information. The controller acts as an exporter.

Configure NetFlow Monitor on the Controller

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose NetFlow > Monitorfrom the left sidebar menu.

Step 4 Configure the following parameters:

- Monitor Name—Name of the NetFlow monitor. The monitor name can be up to 127 case-sensitive alphanumeric characters. You can configure only one monitor in the controller.
- Record Name—Name of the NetFlow record. A NetFlow record in the controller contains the following information about the traffic in a given flow:
  - Client MAC address
  - Client Source IP address
  - WLAN ID
  - Application ID
  - Incoming bytes of data
  - Outgoing bytes of data
  - Incoming Packets
  - Outgoing Packets
  - Incoming DSCP
  - Outgoing DSCP
  - Name of last AP

Step 5 Exporter Name—Name of the exporter. You can configure only one monitor in the controller.

Step 6 Exporter IP—IP address of the collector.

Step 7 Port Number—UDP port through which the NetFlow record is exported from the controller.

Step 8 Click Save.

Configure NetFlow Exporter on the Controller

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click the device name of the applicable controller.

Step 3 Choose NetFlow > Exporter from the left sidebar menu.

Step 4 Configure the following parameters:

- Exporter Name—Name of the exporter.
- Exporter IP —IP address of the exporter.
- Port Number—The UDP port through which the Netflow record is exported.

Related Topics

Configure a Controller’s Multicast DNS (mDNS) Settings, on page 581
Configure a Controller’s NetFlow Settings , on page 584
Configure a Device's Mesh Parameters , on page 563
Configure a Device's Port Parameters , on page 566
Configure a Controller's Management Parameters , on page 567
Configure a Controller’s Location Information, on page 574
Configure a Controller’s IPv6 Neighbor Binding and RA Parameters, on page 576
Configure a Controller’s Proxy Mobile IPv6 (PMIP) Parameters, on page 578

Configure a Third-Party Controller or Access Point

enables you to add third-party controllers and access points. As part of this feature you can perform the following functions:

- Add third-party controllers to the .
- Monitor the state of the third-party controllers.
- Get inventory information for the third-party controllers and their associated access points.
- Use the background tasks to view the operations status third-party controllers and access points.

Related Topics

Add a Third-Party Controller, on page 586
View a Third-Party Controller's Operational Status, on page 587
View a Third-Party Access Point's Settings, on page 588
Remove a Third-Party Access Point, on page 588
View a Third-Party Controller's Operational Status, on page 587

Add a Third-Party Controller

To add a third-party controller, follow these steps:

Step 1 Choose Configuration > Network Devices > Third Party Wireless Controller.

Step 2 Click Add Device.

Step 3 In the Add Device page, enter the required parameters in the following tabs:

- General
- SNMP
- Telnet/SSH
- HTTP/HTTPS
- IPSec

Step 4 Click Add.

Related Topics

View a Third-Party Controller's Operational Status, on page 587
View a Third-Party Access Point's Settings, on page 588

Remove a Third-Party Access Point, on page 588
View a Third-Party Controller's Operational Status, on page 587

View a Third-Party Controller's Operational Status

To view the Third Party Controller Operational Status page, follow these steps:

Step 1 Choose Administration > Settings > Background Tasks.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the Third Party Controller Operational Status check box. From the Select a command drop-down list, choose Execute Now, and click Go. You see the status change in the Enabled column.

- Enable the task.

  Select the Third Party Controller Operational Status check box. From the Select a command drop-down list, choose Enable Tasks, and click Go. The task converts from dimmed to available in the Enabled column.

- Disable the task.

  Select the Third Party Controller Operational Status check box. From the Select a command drop-down list, choose Disable Tasks, and click Go. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the Third Party Controller Operational Status link in the Background Tasks column.

The Third Party Controller Operational Status page displays the Last Execution Information:

- Start Time.
- End Time.
- Elapsed Time (in seconds) of the task.
- Result—Success or error.
- Message—Text message regarding this task.

Step 4 View or modify the following in the Task Details section:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task. The default is 3 hours.

Step 5 When finished, click Save to confirm task changes.

Related Topics

Add a Third-Party Controller, on page 586
View a Third-Party Access Point's Settings, on page 588
Remove a Third-Party Access Point, on page 588

View a Third-Party Access Point's Settings

The third-party access points are discovered when you add a third-party controller.

To view the configurations of a third-party access point, follow these steps:

Step 1 Choose Configuration > Network Devices > Third Party Access Points.

Step 2 Click the AP Name link to display the details. The General tab for that third-party access point appears.

Related Topics

Add a Third-Party Controller, on page 586
View a Third-Party Controller's Operational Status, on page 587
Remove a Third-Party Access Point, on page 588
View a Third-Party Controller's Operational Status, on page 587

Remove a Third-Party Access Point

To remove third-party access points, follow these steps:

Step 1 Choose Configuration > Network Devices > Third Party Access Points.

Step 2 Select the check boxes of the access points you want to remove.

Step 3 Click Delete.

Step 4 A confirmation message appears.

Step 5 Click Yes.

Related Topics

Add a Third-Party Controller, on page 586
View a Third-Party Controller's Operational Status, on page 587
View a Third-Party Access Point's Settings, on page 588
View a Third-Party Controller's Operational Status, on page 587

View a Third-Party Access Point's Operational Status

To view the Third Party Access Point Operational Status page, follow these steps:

Step 1 Choose Administration > Settings > Background Tasks.

Step 2 In this page, perform one of the following:

- Execute the task now.

  Select the Third Party Access Point Operational Status check box. From the Select a command drop-down list, choose Execute Now, and click Go. You see the status change in the Enabled column.

- Enable the task.

Select the Third Party Access Point Operational Status check box. From the Select a command drop-down list, choose Enable Tasks, and click Go. The task converts from dimmed to available in the Enabled column.

- Disable the task.

  Select the Third Party Access Point Operational Status check box. From the Select a command drop-down list, choose Disable Tasks, and click Go. The task is dimmed in the Enabled column after the disabling is complete.

Step 3 To modify the task, click the Third Party Access Point Operational Status link in the Background Tasks column.

The Third Party Controller Operational Status page displays the Last Execution Information:

- Start Time.
- End Time.
- Elapsed Time (in seconds) of the task.
- Result—Success or error.
- Message—Text message regarding this task.

Step 4 View or modify the following in the Edit Task group box:

- Description—Display only. Displays the name of the task.
- Enabled—Select the check box to enable this task.
- Interval—Indicates the frequency (in minutes) of the task. The default is 3 hours.

Step 5 When finished, click Save to confirm task changes.

Related Topics

Add a Third-Party Controller, on page 586
View a Third-Party Controller's Operational Status, on page 587
View a Third-Party Access Point's Settings, on page 588
Remove a Third-Party Access Point, on page 588

View Switch Settings

Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs to see a summary of all switches in the database. Click any column heading to sort the information by that column. You can switch between ascending and descending sort order by clicking the column heading more than once.

Related Topics

View Switch Details, on page 589

View Switch Details

Choose Configuration > Network > Network Devices > Device Type > Switches and Hubsto see a summary of all switches in the database. Click a Device Name to see detailed information about that switch.

Related Topics

Example: Configure SNMPv3 on Switches, on page 592

Change Switch SNMP Parameters

To modify SNMP parameters for a switch, follow these steps:

Step 1 Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs, then click the checkbox next to the switch for which you want to change SNMP credentials.

Step 2 Click Edit.

Step 3 Modify the necessary SNMP Parameters fields, then click one of the following:

- Reset to restore the previously saved parameters.
- Save to save and apply the changes you made.
- Cancel to exit without saving your changes and return to the previous screen.

Related Topics

View Switch Settings, on page 589
Example: Configure SNMPv3 on Switches, on page 592
Change Switch Telnet/SSH Credentials, on page 590

Change Switch Telnet/SSH Credentials

To modify Telnet or SSH parameters for a switch, follow these steps:

Step 1 Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs, then click the checkbox next to the switch for which you want to change Telnet or SSH credentials.

Step 2 Click Edit.

Step 3 Modify the necessary Telnet/SSH Parameters fields, then click one of the following:

- Reset to restore the previously saved parameters.
- Save to save and apply the changes you made.
- Cancel to exit without saving your changes and return to the previous screen.

Related Topics

View Switch Settings, on page 589
Example: Configure SNMPv3 on Switches, on page 592
Change Switch SNMP Parameters, on page 590

Add Switches

You can add switches to database to view overall switch health and endpoint monitoring and to perform switchport tracing. The following switches can be configured:

- 3750
- 3560
- 3750E
- 3560E
- 2960.

The switch functionality appears on the configuration menu in however you cannot configure switch features using . You can only configure system.

allows you to do the following:

- Add switches in the Configuration > Network > Network Devices > Device Type > Wireless Controller page and specify CLI and SNMP credentials.
- Add a location-capable switch for tracking wired clients by mobility services engine and in the Configuration > Network > Network Devices > Device Type > Wireless Controller page.
- Monitor Switches by choosing Monitor > Network Devices.
- Run switch-related reports using the Reports menu.

When you add a switch to the database, by default, verifies the SNMP credentials of the switch. If the device credentials are not correct, you receive an SNMP failure message but the switch is added to the database.

Features Available by Switch Type

When you add a switch to , you specify how the switch is to be managed, based on this, determines the features that are available:

- Monitored switches—You can add switches (choose Configuration > Network > Network Devices > Device Type > Wireless Controller) and monitor switch operation (choose Monitor > Network Devices). Each switch counts as a single device against the total device count for your license. If you have unused device counts available in your license engine, you can add a switch to . If you have no remaining device counts available, you cannot add additional switches to .
- Switch Port Tracing (SPT) only switches—Switches perform switch port tracing only. SPT-only switches appear in the Configuration > Network > Network Devices > Device Type > Switches and Hubs page and in inventory reports. Licensing does not apply to SPT switches.

To add a switch to , follow these steps:

Step 1 Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs, then click Add Device.

Step 2 Enter the appropriate information in the fields displayed.

See Cisco Pime Infrastrucutre Reference Guide, for more information.

Step 3 Click Add to add the switch or click Cancel to cancel the operation and return to the list of switches.

Related Topics

Import Switches From CSV Files, on page 592
Example: Configure SNMPv3 on Switches, on page 592

Example: Configure SNMPv3 on Switches

The following is an example for configuring SNMPv3 on the switch:

snmp-server view v3default iso includedsnmp-server group v3group v3 auth write v3default snmp-server user <username> <v3group> v3 auth <md5 or sha> <authentication password>

If the switch has VLANs, you must configure each VLAN, otherwise switch porting tracing fails. The following is an example if the switch has VLANs 1 and 20.

snmp-server group v3group v3 auth context vlan-1 write v3defaultsnmp-server group v3group v3 auth context vlan-20 write v3default

snmp-server group v3group v3 auth context vlan-20 write v3default

When you create SNMP v3 view, make sure you include all of the OIDs.

Related Topics

Import Switches From CSV Files, on page 592

Import Switches From CSV Files

You can import switches into the database using a CSV file. The first row of the CSV file is used to describe the columns included. The IP Address column is mandatory.

The following example shows a sample CSV file.

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type,
 snmpv3_auth_password, snmpv3_privacy_type, snmpv3_privacy_password, snmp_retries,
snmp_timeout,protocol,telnet_username,telnet_password,enable_password,telnet_timeout
16.1.1.3,255.255.255.0,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
16.1.1.4,255.255.255.0,v2,public,,,,,,3,10,ssh2,cisco,cisco,cisco,60
16.1.1.5,255.255.255.0,v2,public,,,,,,3,10,,cisco,cisco,cisco,60
16.1.1.6,255.255.255.0,v2,public,,,,,,3,10,telnet,cisco,cisco,cisco,60
3.3.3.3,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4
4.4.4.4,255.255.255.0,v3,,default,HMAC-MD5,default,DES,default,3,4,telnet,cisco,cisco,cisco,60
```

The fields in the Civic Location pane are populated after the civic information is imported.

See Cisco Prime Infrastructure Reference Guide, for more information.

Related Topics

Add Switches, on page 591
Example: Configure SNMPv3 on Switches, on page 592

Remove Switches

When you remove a switch from the database, the following functions are performed:

- Inventory information for that switch is removed from the database.
- Alarms for the switch remain in the database with a status of Clear. By default, cleared alarms are not displayed in the interface.
- Saved reports remain in the database even if the switch on which the report was run is removed.

To remove a switch from , follow these steps:

Step 1 Choose Configuration > Network > Network Devices > Device Type > Switches and Hubs, then click the checkbox next to the switch for which you want to remove.

Step 2 Click Delete.

Step 3 Click OK to confirm the deletion.

Related Topics

Add Switches, on page 591

Example: Configure Switch Traps and Syslogs for Wired Clients

The following Cisco IOS configuration example shows how this Cisco IOS switch feature forwards SNMP traps from the switch to server for MAC notifications (for on-802.1x clients):

```
snmp-server enable traps mac-notification change move threshold
snmp-server host<IP address of Prime Infrastructure server> version 2c <community-string>
mac-notification
mac address-table notification change interval 5
mac address-table notification change history-size 10
mac address-table notification change


interface <interface>
 description non-identity clients
 switchport access vlan <VLAN ID>
 switchport mode access
 snmp trap mac-notification change added  <- interface level config for MAC Notification
  snmp trap mac-notification change removed <- interface level config for MAC Notification
```

The debug command is:

```
debug snmp packets
```

The show command is:

```
show mac address-table notification change
```

See Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, for more information.

Example: Configure Syslog Forwarding for Catalyst Switches Using IOS

The syslog configuration forwards syslog messages from a Catalyst switch to the server. This feature is used for identity clients discovery.The following Cisco IOS configuration example shows how this Cisco IOS switch forwards syslog messages from a Catalyst switch to the Prime Infrastructure server:

```
archive
 log config
  notify syslog contenttype plaintext
logging facility auth
logging <IP address of Prime Infrastructure server>
```

See Catalyst 3750 Software Configuration Guide, for more information.

Using Cisco OfficeExtend APs With

An OfficeExtend access point provides secure communications from a controller to an access point at a remote location, seamlessly extending the corporate WLAN over the Internet to the residence of an employee. The experience of a teleworker at the home office is exactly the same as it is at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the access point and the controller ensures that all communications have the highest level of security.

Figure 25-1 205774.jpg illustrates a typical OfficeExtend access point setup.

OfficeExtend access points are designed to work behind a router or other gateway device that is using network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), thereby enabling an entire group of computers to be represented by a single IP address. In controller release 6.0, only one OfficeExtend access point can be deployed behind a single NAT device.

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 series controller with a WPlus license can be configured to operate as OfficeExtend access points.

Your firewall must be configured to allow traffic from access points using CAPWAP. Make sure that UDP ports 5246 and 5247 are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.

Before licensing for an OfficeExtend Access Point make sure that the WPlus license is installed on the 5500 series controller. After the license is installed, you can enable the OfficeExtend mode on an 1130 series or 1140 series access point.

The operating system software automatically detects and adds an access point to the database as it associates with existing controllers in the database.

Configure Link Latency to Measure the Link Between an AP and Controller

You can configure link latency on the controller to measure the link between an access point and the controller. This feature can be used with all access points joined to a controller but is especially useful for FlexConnect access points, for which the link could be a slow or unreliable WAN connection.

Link latency is supported for use only with FlexConnect access points in connected mode. FlexConnect access points in standalone mode are not supported.

Link latency monitors the round-trip time of the CAPWAP heartbeat packets (echo request and response) from the access point to the controller and back. This time can vary due to network link speed and controller processing loads. The access point timestamps the outgoing echo requests to the controller and the echo requests received from the controller. The access point sends this delta time to the controller as the system round-trip time. The access point sends heartbeat packets to the controller at a default interval of 30 seconds.

Link latency calculates the CAPWAP response time between the access point and the controller. It does not measure network latency or ping responses.

The controller displays the current round-trip time as well as a running minimum and maximum round-trip time. The minimum and maximum times continue to run as long as the controller is up or can be cleared and allowed to restart.

To configure link latency, follow these steps:

Step 1 Choose Configuration > Network > Network Devices > Device Type > Unified AP, then click on a Device Name.

Step 2 Select the Enable Link Latency check box to enable link latency for this access point or unselect it to prevent the access point from sending the round-trip time to the controller after every echo response is received. The default value is unselected.

Step 3 Click Save to save your changes.

The link latency results appear below the Enable Link Latency check box:

a. Current—The current round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

b. Minimum—Because link latency has been enabled or reset, the minimum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

c. Maximum—Because the link latency has been enabled or reset, the maximum round-trip time (in milliseconds) of CAPWAP heartbeat packets from the access point to the controller and back.

Step 4 To clear the current, minimum, and maximum link latency statistics on the controller for this access point, click Reset Link Latency. The updated statistics appear in the Minimum and Maximum fields.

Configure Unified APs

You can use theConfiguration > Network > Network Devices > Device Type > Unified AP page to view and configure unified access points.

Step 1 Choose Configuration > Network > Network Devices, then from the Device Groups menu on the left, select Device Type > Wireless Controller.

Step 2 Click an applicable IP address to view the following parameters:

- AP Name—Click an access point name to view or configure access point details.
- Base Radio MAC
- Admin Status
- AP Mode
- Software Version
- Primary Controller Name

Step 3 Click an access point name to view or configure the access point details. The displayed information might vary depending for the access point type.

Enable the Sniffer Feature on a Unified Access Point (AiroPeek)

When the sniffer feature is enabled on an access point, the access point functions as a sniffer and captures and forwards all the packets on a particular channel to a remote machine that runs AiroPeek. The packets contain information on timestamp, signal strength, packet size, and so on.

The sniffer feature can be enabled only if you are running AiroPeek, which is a third-party network analyzer software that supports decoding of data packets. For more information on AiroPeek, see the following URL: www.wildpackets.com/products/airopeek/overview

Before You Begin

Before using the sniffer feature, you must complete the following:

- Configure an access point in sniffer mode at the remote site. For information on how to configure an access point in sniffer mode, see Configuring an AP in Sniffer Mode Using the Web User Interface in Related Topics.
- Install AiroPeek Version 2.05 or later on a Windows XP machine.
  - You must be a WildPackets Maintenance Member to download the following dll files. See the following URL: https://wpdn.wildpackets.com/view_submission.php?id=30
- Copy the following dll files:
  - socket.dll file to the Plugins folder (Example: C:\ProgramFiles\WildPackets\AiroPeek\Plugins)
  - socketres.dll file to the PluginRes folder (Example:C:\ProgramFiles\WildPackets\AiroPeek\1033\PluginRes)

Related Topics

Configure a Device's 802.11 Parameters , on page 556

Configure the AiroPeek Sniffer on a Remote Machine

To configure AiroPeek on the remote machine, follow these steps:

Step 1 Start the AiroPeek application and click Options on the Tools tab.

Step 2 Click Analysis Module in the Options page.

Step 3 Right-click inside the page and select Disable All option.

Step 4 Find the Cisco remote module column and enable it. Click OK to save the changes.

Step 5 Click New capture to bring up the capture option page.

Step 6 Choose the remote Cisco adapter and from the list of adapter modules.

Step 7 Expand it to locate the new remote adapter option. Double-click it to open a new page, enter a name in the text box provided and enter the controller management interface IP in the IP address column.

Step 8 Click OK. The new adapter is added to the remote Cisco adapter.

Step 9 Select the new adapter for remote airopeek capture using the access point.

Step 10 Click start socket capture in the capture page to start the remote capture process.

Step 11 From the controller CLI, bring up an access point, and set it to sniffer mode by entering the config ap mode sniffer ap-name command.

The access point reboots and comes up in sniffer mode.

Configure an AP in Sniffer Mode Using

To configure an AP in Sniffer mode using the web user interface, follow these steps:

Step 1 Choose Configuration > Network > Network Devices, then click an item in the AP Name column to navigate to this page.

Step 2 In the General group box, set the AP mode to Sniffer using the drop-down list, and click Apply.

Step 3 Click a protocol (802.11a/802.11b/g) in the Protocol column in the Radio Interfaces group box. This opens the configuration page.

Step 4 Select the Sniff check box to bring up the Sniff parameters. Select the channel to be sniffed and enter the IP address of the server (The remote machine running AiroPeek).

Step 5 Click Save to save the changes.

Enable Flex+Bridge Mode on AP

To enable Flex+Bridge mode on your AP, follow these steps:

Step 1 Click Configuration > Templates > Lightweight Access Points.

Step 2 Click the relevant AP template or add a new template.

Step 3 Click AP Parameters tab and check the AP Mode checkbox.

Step 4 Select Flex+Bridge from the drop-down list and click Save.

- If you're switching the AP mode to or from Flex+Bridge, the AP goes for a reboot.
- Flex+Bridge mode does not support API encryption, AP Retransmit Interval, and only Critical AP Failover criteria is supported.
- Configurations made in FlexConnect and Mesh tabs does not provisioned when you change the AP mode. You first have to change the AP mode to Flex+Bridge and then configure parameters on FlexConnect and Mesh tabs.

Configure Controller Redundancy

"Controller Redundancy" refers to the High Availability (HA) framework embedded in controllers. Redundancy in wireless network controllers allows you to reduce network downtime. In a redundancy architecture, one controller is in the Active state and a second controller is in the Standby state. The Standby controller monitors the health of the Active controller continuously, using a redundant port. Both controllers share the same configurations including the IP address of the management interface.

The Standby or Active state of a controller is based on the redundancy stock keeping unit (SKU), which is a manufacturing-ordered unique device identifier (UDI). A controller with a redundancy SKU UDI is in the Standby state for the first time when it boots and pairs with a controller that runs a permanent count license. For controllers that have permanent count licenses, you can manually configure whether the controller is in the Active state or the Standby state.

supports stateful switchover of access points (also known as "AP SSO"). AP SSO ensures that AP sessions remain intact despite controller switchovers. For more details on controller redundancy, see "Configuring Wireless Redundancy" in Related Topics.

Controller redundancy is similar to, but separate from, the HA framework used to reduce server downtime. For more information on this, see “Configuring High Availability” in Related Topics.

See Cisco Prime Infrastructire Administrator Guide, for more infromation.

Note Chassis Priority option will be disabled after WLC HA is established. The peer timeout and keep alive retires can be changed with HA mode configuration and to change any other configurations, HA should be disabled and reconfigured.

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats

supports Cisco Adaptive Wireless Intrusion Prevention System (Cisco Adaptive wIPS, or wIPS), which uses profiles to quickly activate wireless threat protection features.

provides a list of pre-defined wIPS profiles based on customer types, building types, and industry types, such as “Education”, “Financial”, “Military”, “Tradeshow”, and so on. You can use these profiles “as is” or customize them to better meet your needs. You can then apply them to the Mobility Services Engines and controllers you select.

Cisco Adaptive wIPS does not support the partitioning feature.

See Cisco Wireless Intrusion Prevention System Configuration Guide for more information.

Related Topics

View wIPS Profiles, on page 598
Add wIPS Profiles, on page 599
Edit wIPS Profiles, on page 600
Apply wIPS Profiles, on page 601
Delete wIPS Profiles, on page 602

View wIPS Profiles

wIPS Profiles List page provides access to wIPS profiles. You can use it to view, edit, apply or delete current wIPS profiles, and to create new wIPS profiles.

Choose Services > Mobility Services > wIPS Profiles. The wIPS Profiles List displays the list of current wIPS profiles. It gives the following information for each existing profile:

- Profile Name—The user-defined name for the wIPS profile.

  To view or edit a wIPS profile, click the Profile Name. Then follow the steps in “Edit wIPS Profiles” in Related Topics.

- Profile ID—The profile’s unique identifier.
- Version— The version of the profile.
- MSE(s) Applied To—Indicates the number of Mobility Services Engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.

- Controller(s) Applied To—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

Related Topics

Add wIPS Profiles, on page 599
Edit wIPS Profiles, on page 600
Apply wIPS Profiles, on page 601
Delete wIPS Profiles, on page 602
Create SSID Groups, on page 602

Add wIPS Profiles

You can create new wIPS profiles using the default profile or any of the currently pre-configured profile.

Step 1 Select Services > Mobility Services > wIPS Profiles.

Step 2 Choose Select a command > Add Profile > Go.

Step 3 Type a profile name in the Profile Name text box of the Profile Parameters page.

Step 4 Select the applicable pre-defined profile, or choose Default from the drop-down list. Pre-defined profiles include the following:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

Step 5 Click:

- Save to save the wIPS profile with no changes and no assignments. The profile appears in the profile list. You can access the profile for edits and assignment later, as explained in “Accessing wIPS Profiles” in Related Topics.
- Save and Edit to save the profile, edit its settings, and assign it to Mobility Services Engines and Controllers. For details, see “Editing wIPS Profiles” in Related Topics.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 598
View wIPS Profiles, on page 598
Edit wIPS Profiles, on page 600

Edit wIPS Profiles

The wIPS profile editor allows you to configure profile details, including the following:

- SSID groups—Select the SSID groups to which the wIPS profile will be applied.
- Policy inclusion—Determine which policies are included in the profile.
- Policy level settings—Configure settings for each policy included in the profile, such as threshold, severity, notification type, and ACL/SSID groups.
- MSE/controller applications—Select the MSEs and controllers to which you want to apply the profile.

Step 1 Access the wIPS profile editor by:

- Create a new wIPS profile and then click Save and Edit.
- Choose Services > Mobility Services > wIPS Profilesand then click the Profile Name of the wIPS profile you want to edit.

  displays the SSID Group List page. Using this page, you can edit and delete current SSID groups or add a new group. You can also select from the global list of SSID groups. For details, see “Associating SSID Groups With wIPS Profiles” in Related Topics.

Step 2 Select the SSID groups you want to associate with the wIPS profile, then click Save.

Step 3 Click Next. The Profile Configuration page displays.

Step 4 In the Select Policy pane’s policy tree, select the check boxes of the policies you want to enable or disable in the current profile.

You can enable or disable an entire branch or an individual policy by selecting the check box for the applicable branch or policy.

By default, all policies are selected.

Step 5 In the Profile Configuration page, click an individual policy to display the policy description and to view or modify current policy rule settings. The following options are available for each policy:

- Add—Click Add to access the Policy Rule Configuration page to create a new rule for this policy.
- Edit—Select the check box of the applicable rule, and click Edit to access the Policy Rule Configuration page to edit the settings for this rule.
- Delete—Select the check box of the rule you want to delete, and click Delete. Click OK to confirm the deletion.

  There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.
- Move Up—Select the check box of the rule you want to move up in the list. Click Move Up.
- Move Down—Select the check box of the rule you want to move down in the list. Click Move Down.

  The following settings can be configured at the policy level:

- Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. When the threshold is reached for a policy, an alarm is triggered.

  Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues.

  Threshold options vary based on the selected policy.

  Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page. Choose Monitor > Security to access this page. The wIPS attacks are located in the Threats and Attacks section.

- Severity—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.
- Notification—Indicates the type of notification associated with the threshold.
- ACL/SSID Group—Indicates the ACL or SSID Group(s) to which this threshold is be applied.

  Only selected groups trigger the policy.

Step 6 When the profile configuration is complete, click Save to save your changes to the profile.

Step 7 Click Next to display the MSE/Controller(s) page.

Step 8 In the Apply Profile page, select the check boxes of the MSEs and controllers to which you want to apply the current profile.

Step 9 When you are finished, click Apply to apply the current profile to the selected MSEs and controllers.

You can also apply a newly created profile directly from the Profile List page. See “Applying wIPS Profiles” in Related Topics.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 598
View wIPS Profiles, on page 598
Apply wIPS Profiles, on page 601
Delete wIPS Profiles, on page 602
Create SSID Groups, on page 602

Apply wIPS Profiles

Step 1 Choose Services > Mobility Services > wIPS Profiles.

Step 2 Select the check boxes of the wIPS profiles you want to apply.

Step 3 Choose Select a command > Apply Profile > Go.

Step 4 Select the mobility services engines and controllers to which you want the profile applied.

If the new profile assignment is different from the current assignment, you are prompted to save the profile with a different name.

Step 5 Click Apply.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 598
Create SSID Groups, on page 602

Delete wIPS Profiles

Profiles currently applied to MSEs and controllers cannot be deleted.

Step 1 Choose Services > Mobility Services > wIPS Profiles.
Step 2 Select the check boxes of the wIPS profiles you want to delete.
Step 3 Choose Select a command > Delete Profile > Go.
Step 4 Click OK to confirm the deletion.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 598
Add wIPS Profiles, on page 599
Edit wIPS Profiles, on page 600
Apply wIPS Profiles, on page 601

Associate SSID Groups With wIPS Profiles

The SSID (Service Set IDentifier) is a token or key which identifies an 802.11 (Wi-Fi) network. Users must either know or be able to discover the SSID to join an 802.11 network.

You can associate SSIDs with a wIPS profile by adding the SSIDs to an SSID group, then associating the SSID group with the wIPS profile.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 598
Delete wIPS Profiles, on page 602
Create SSID Groups, on page 602
Edit SSID Groups, on page 603

Create SSID Groups

Step 1 Choose Services > Mobility Services > wIPS Profiles.
Step 2 Click the Profile Name of any wIPS profile. displays the SSID Group List page.
Step 3 Choose Select a command > Add Group > Go.
Step 4 Enter the SSID Group Name in the text box.
Step 5 Enter the SSIDs in the SSID List text box. Enter multiple SSIDs with a carriage return after each SSID.
Step 6 Click Save.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 598

Associate SSID Groups With wIPS Profiles, on page 602

Edit SSID Groups

Step 1 Choose Services > Mobility Services > wIPS Profiles.
Step 2 Click the Profile Name of any wIPS profile. displays the SSID Group List page.
Step 3 Select the check box of the SSID group that you want to edit.
Step 4 Choose Select a command > Edit Group > Go.
Step 5 Make the necessary changes to the SSID Group Name or the SSID List.
Step 6 Click Save.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 598
View wIPS Profiles, on page 598

Delete SSID Groups

Step 1 Choose Services > Mobility Services > wIPS Profiles.
Step 2 Click the Profile Name of any wIPS profile. displays the SSID Group List page.
Step 3 Select the check boxes of the SSID groups that you want to delete.
Step 4 Choose Select a command > Delete Group > Go.
Step 5 Click OK to confirm the deletion.

Related Topics

Configure Cisco Adaptive wIPS to Protect Controllers Against Threats , on page 598
View wIPS Profiles, on page 598
Edit wIPS Profiles, on page 600

Configure High Availability for MSE Servers

You can use to pair and manage Cisco Mobility Services Engine (MSE) devices that have been configured for MSE High Availability (HA). The following related topics explain how to perform these and related tasks.

Related Topics

MSE HA Server Failover and Failback, on page 604
Configure the MSE HA Servers, on page 604
View Details About the Primary and Secondary MSE HA Server, on page 605
View MSE Server HA Status, on page 606
Trigger MSE HA Manual Failover or Failback, on page 606
Configure Automatic HA Failover and Failback on MSE Servers, on page 607

MSE HA Server Failover and Failback

The MSE HA feature is intended to permits continued access to MSE services even when the primary MSE fails. The secondary MSE maintains a complete copy of the primary MSE's data, serving as its backup. Health Monitor and "heartbeat" processes running on both the primary and secondary keep each server informed about the state of the other.

Whenever the primary MSE fails, a "failover" to the secondary MSE is triggered. Prime Infrastructure will then use the secondary's mobility services instead of the primary until the problems with the primary are fixed.

When the primary is back in service, a "failback" is triggered, returning control to the primary MSE, and replicating data about the intervening state of the network back to the primary from the secondary MSE.

When configuring MSE HA, you can choose to have failovers triggered either automatically or manually. You have the same options for failbacks.

Configuring MSE HA for manual failover or failback means these operations must be triggered by a user, in response to critical alarms sent when the primary fails or is restored to service.

Configuring MSE HA for automatic failover reduces the need for network administrators to manage MSE HA. It also reduces the time taken to respond to the conditions that provoked the failover, since it brings up the secondary server automatically, within approximately 10 seconds (the default) of detection of failure on the primary. If MSE HA is configured for automatic failback, the system will trigger the failback only after successful receipt of 30 ping messages sent once per minute.

Related Topics

Configure the MSE HA Servers, on page 604
Configure Automatic HA Failover and Failback on MSE Servers, on page 607
Configure High Availability for MSE Servers, on page 603

Configure the MSE HA Servers

In order to activate High Availability for MSE devices, you must create a pairing, where one MSE serves as the primary MSE device, and another acts as the secondary MSE.

Note that you can only pair MSE devices that are:

- Properly configured for use with MSE High Availability, as explained in the related topic "Configuring MSE High Availability".
- Added to , as explained in the related topic "Adding MSEs to ".

Before You Begin

To create the pairing, you will need to know:

- The device name of the primary MSE server.
- The device name of the secondary MSE server. This can be a previously assigned device name, or a new name you assign at the moment you pair the servers.
- The secondary MSE HA server's IP address. This is the IP address of the HA Health Monitor, which was assigned when configuring the MSE server for HA use.
- The secondary MSE HA server's password. This is the communication password, which was assigned when configuring the MSE server for HA use.

You must also decide if you want to configure the MSE HA servers for manual or automatic failback. For guidelines, see the related topic "MSE HA Automatic vs Manual Failover and Failback".

Step 1 Choose Services > Mobility Services > Mobility Services Engines. A list of the existing MSEs is displayed.

Step 2 In the list, find the MSE you want to act as the primary MSE HA server.

Step 3 The "Secondary Server" column for the MSE listing displays the message "N/A (Click here to configure)". Click on the link to display the HA configuration page for the primary MSE.

Step 4 Enter the secondary MSE's device name, Health Monitor IP address, and communication password in the appropriate fields.

Step 5 Specify the failover and failback types. You can choose either Manual or Automatic

Step 6 Specify the Long Failover Wait. This is the maximum time the system will wait to trigger automatic failover after detection of primary MSE failure. The default is 10 seconds; the maximum is 120 seconds.

Step 7 Click Save. prompts you to confirm that you want to pair these MSEs. Click OK to confirm.

conducts the pairing and synchronization automatically. These processes can take up to 20 minutes to complete, depending on network bandwidth and many other factors. To check on the progress of these processes, select Services > Mobility Services Engine > System > Services High Availability > HA Status.

Related Topics

MSE HA Server Failover and Failback, on page 604
Configure Automatic HA Failover and Failback on MSE Servers, on page 607
Configure High Availability for MSE Servers, on page 603

View Details About the Primary and Secondary MSE HA Server

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 To see the HA parameters for the:

- Primary MSE HA server: Click the name of the server in the Device Name column.
- Secondary MSE HA server: Click the name of the server in the Secondary Server column.

displays the Mobility Services Engines configuration page for the server you selected.

Step 3 In the left sidebar menu, choose HA Configuration. The HA Configuration page provides the following information:

- Primary Health Monitor IP
- Secondary Device Name
- Secondary IP Address
- Secondary Password
- Secondary Platform UDI
- Secondary Activation Status
- Failover Type
- Failback Type

- Long Failover Wait

Related Topics

Configure the MSE HA Servers, on page 604
Trigger MSE HA Manual Failover or Failback, on page 606
View MSE Server HA Status, on page 606
Configure Automatic HA Failover and Failback on MSE Servers, on page 607
Configure High Availability for MSE Servers, on page 603

View MSE Server HA Status

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 To see the HA status of the:

- Primary MSE HA server: Click the name of the server in the Device Name column.
- Secondary MSE HA server: Click the name of the server in the Secondary Server column.

displays the Mobility Services Engines configuration page for the server you selected.

Step 3 In the left sidebar menu, choose HA Status. The Current High Availability Status page shows the following information:

- Status—Shows whether the MSE HA server is active and correctly synchronized.
- Heartbeats—Shows whether the MSE HA server is exchanging heartbeat signals with its partner.
- Data Replication—Shows whether MSE HA server is replicating data with its partner.
- Mean Heartbeat Response Time—Shows the mean heartbeat response time between servers.
- Events Log—Shows the last 20 events that the MSE server has generated.

Step 4 Click Refresh Status to update the MSA server's HA status information and Events Log.

Related Topics

Configure the MSE HA Servers, on page 604
View Details About the Primary and Secondary MSE HA Server, on page 605
Configure Automatic HA Failover and Failback on MSE Servers, on page 607
Configure High Availability for MSE Servers, on page 603

Trigger MSE HA Manual Failover or Failback

Manual failover and failback are enabled by default. Manual configuration requires that the administrator trigger failovers and failbacks manually, in response to system alarms.

You can also configure paired MSE HA servers for automatic failover and failback (see Related Topics).

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 To trigger a:

- Failover from the primary to the secondary: Click the name of the primary MSE HA server in the Device Name column.
- Failback from the secondary to the primary: Click the name of the secondary MSE HA server in the Secondary Server column.

displays the Mobility Services Engines configuration page for the server you selected.

Step 3 In the left sidebar menu, choose HA Configuration. The HA Configuration page displays the HA configuration information for the server you chose.

Step 4 Click Switchover to initiate the failover or failback.

Step 5 Click OK to confirm that you want to initiate the switchover.

Related Topics

MSE HA Server Failover and Failback, on page 604
Configure Automatic HA Failover and Failback on MSE Servers, on page 607
Configure High Availability for MSE Servers, on page 603

Configure Automatic HA Failover and Failback on MSE Servers

Manual failover and failback are enabled by default. If you configure paired MSE HA servers for automatic failover and failback, the change will occur automatically, as follows:

- Failover from primary to secondary: Triggered immediately, as soon as the secondary detects a failure on the primary.
- Failback from secondary to primary: Triggered after 30 successful ping messages from the secondary to the primary. Ping requests are sent once per minute.

Step 1 Choose Services > Mobility Services > MSE High Availability.

Step 2 Click the name of the primary MSE HA server in the Device Name column.

displays the HA Configuration page for the primary MSE HA server.

Step 3 In the Failover Type and Failback Type list boxes, select Automatic.

Step 4 If needed: Change the value in Long Failover Wait to control the maximum delay between detection of a failure on the primary and automatic failover. The default is 10 seconds.

Step 5 Click Save to save your changes.

Related Topics

MSE HA Server Failover and Failback, on page 604
Trigger MSE HA Manual Failover or Failback, on page 606
Configure High Availability for MSE Servers, on page 603

Unpair MSE HA Servers

Step 1 Choose Services > Mobility Services > MSE High Availability.

Step 2 Click the name of the primary MSE HA server in the Device Name column.

displays the HA Configuration page for the Primary MSE HA server.

Step 3 Click Delete to unpair the MSE servers.

Step 4 Click OK to confirm that you want to unpair the MSE HA servers.

Related Topics

Configure the MSE HA Servers, on page 604
Configure High Availability for MSE Servers, on page 603

Configure Controllers Using Plug and Play

Auto provisioning allows to automatically configure a new or replace a current wireless LAN controller (WLC). auto provisioning feature can simplify deployments for customers with a large number of controllers.

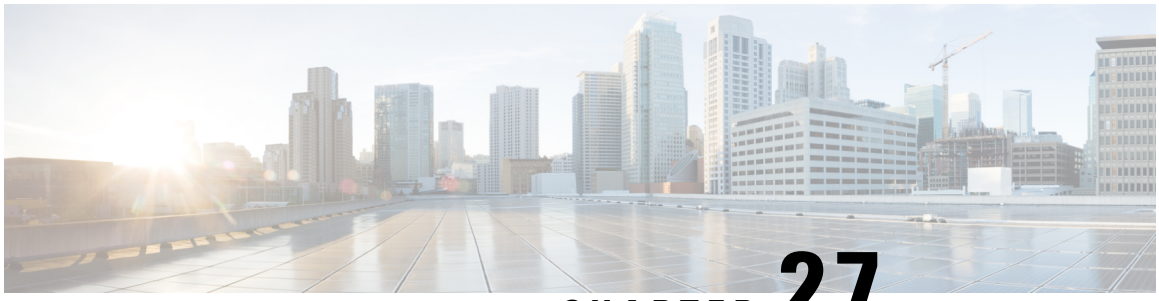
For Auto Provisioning privileges, you must have Admin, Root, or SuperUser status.

To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using Administration Settings > Users, Roles, and AAA > User Groups > group name > List of Tasks Permitted in . Select or unselect the check box to allow or disallow these privileges.

A controller radio and b/g networks are initially disabled by the downloaded startup configuration file. If desired, you might turn on those radio networks by using a template, which should be included as one of the automated templates.

To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To access the Auto Provisioning feature, choose Configuration > Plug and Play > WLC Auto Provisioning.



CHAPTER 27

Configure Wireless Technologies

Track Tagged Assets Using Optimized Monitor Mode on APs

To optimize monitoring and location calculation of tags, you can enable Tracking Optimized Monitor Mode (TOMM) on up to four channels within the 2.4-GHz band (802.11b/g radio) of an access point. This allows you to focus channel scans only on those channels on which tags are usually programmed to operate (such as channels 1, 6, and 11).

After enabling Monitor mode at the access point level, you must then enable TOMM and assign monitoring channels on the 802.11b/g radio of the access point.

To set enable TOMM and assign monitoring channels on the access point radio, follow these steps:

Step 1 After enabling Monitor mode at the access point level, choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 In the Access Points page, click the 802.11 b/g Radio link for the appropriate access point.

Step 3 In the General group box, disable Admin Status by unselecting the check box. This disables the radio.

Step 4 Select the TOMM check box. This check box only appears for Monitor Mode APs. The drop-down lists for each of the four configurable channels are displayed.

Step 5 Choose the four channels on which you want the access point to monitor tags.

Note You can configure fewer than four channels for monitoring. To eliminate a monitoring channel, choose None from the channel drop-down list.

Step 6 Click Save. Channel selection is saved.

Step 7 In the Radio parameters page, reenable the radio by selecting the Admin Status check box.

Step 8 Click Save. The access point is now configured as a TOMM access point.

The AP Mode displays as Monitor/TOMM in the Monitor > Access Points page.

Configure Wireless Chokepoints

Creating a Wireless Chokepoint

To add a chokepoint, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Chokepoints.

Step 2 From the Select a command drop-down list, choose Add Chokepoints, and then click Go.

Step 3 Enter the MAC address and name for the chokepoint.

Step 4 Select the check box to indicate that it is an Entry/Exit Chokepoint.

Step 5 Enter the coverage range for the chokepoint.

Chokepoint range is a visual representation only. It is product-specific. The actual range must be configured separately using the applicable chokepoint vendor software.

Step 6 Click ok.

After the chokepoint is added to the database, it can be placed on the appropriate the Prime Infrastructure floor map.

Removing a Wireless Chokepoint from the Network

To remove a chokepoint, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Chokepoints.

Step 2 Select the check box of the chokepoint that you want to delete.

Step 3 From the Select a command drop-down list, choose Remove Chokepoints, then click Go.

Step 4 Click OK to confirm the deletion.

Manage Unified APs

Configuration

Put APs in Maintenance State

To move an access point to the maintenance state, follow these steps:

Step 1 Click Configuration > Access Points Radio.

The Unified Access Points page appears.

Step 2 In Unified AP Radio tab, select the desired AP(s), and then click Configure > Place in Maintenance State.

The access point is moved to maintenance state.

Once the access point is moved to maintenance state, the access point down alarms are processed with lower severity instead of critical.

Note Reducing the severity of access point down alarms that are in the Maintenance State will not prevent Prime Infrastructure from sending out alarm notification emails, even though the state of the alarm notification policy is "Critical events".

Remove APs from Maintenance State

To remove an access point from the maintenance state, follow these steps:

Step 1 Click Configuration > Access Points Radios.

The Unified AP Radio page appears.

Step 2 In Unified AP Radio tab, select the desired AP(s), and then click Configure > Remove from Maintenance State.

The access points are removed from the maintenance state.

Scheduling

Schedule AP Radio Status Changes

To schedule a radio status change (enable or disable), follow these steps:

Step 1 Click Configuration > Access Points Radios.

Step 2 In Unified AP Radio tab, select the desired APs, and then click Schedule > Schedule Radio Status.

Step 3 Choose Enable or Disable from the Admin Status drop-down list.

Step 4 Use the Hours and Minutes drop-down lists to determine the scheduled time.

Step 5 Click the calendar icon to select the scheduled date for the status change.

Step 6 If the scheduled task is recurring, choose Daily or Weekly as applicable. If the scheduled task is a one-time event, choose No Recurrence.

Step 7 Choose Save to confirm the scheduled task.

View Scheduled AP Radio Status Changes

To view currently scheduled radio status tasks, follow these steps:

Step 1 Click Configuration > Access Points Radios.

Step 2 In Unified AP Radio tab, select the desired APs, and then click Schedule > View Schedule Radio Task(s).

The Scheduled Task(s) information includes:

a. Scheduled Task(s)—Choose the task to view its access points and access point radios.

b. Scheduled Radio admin Status—Indicates the status change (Enable or Disable).

c. Schedule Time—Indicates the time the schedule task occurs.

d. Execution status—Indicates whether or not the task is scheduled.

e. Recurrence—Indicates Daily or Weekly if the scheduled task is recurring.

f. Next Execution—Indicates the time and date of the next task occurrence.

g. Last Execution—Indicates the time and date of the last task occurrence.

h. Unschedule—Click Unschedule to cancel the scheduled task. Click OK to confirm the cancellation.

View Alarms for APs in the Maintenance State

uses critical alarms to track if the managed access points are down. The controller sends three different alarms when the following occurs:

- The Access point is down
- Radio A of the access point is down

- Radio B/G of the access point is down

In Release 7.0.172.0 and later, these 3 alarms are grouped into a single alarm.

When an access point is under technical maintenance, the critical alarms need to be deprioritized. You can deprioritize the severity of an alarm of an access point using the Configure > Access Points page. When you move an access point to maintenance state, the alarm status for that access point appears in black color.

Configure AP Ethernet Interfaces

To configure an Ethernet interface, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 Click the link under AP Name to see detailed information about that access point name. The Access Point Detail page appears.

Note The Access Point Details page displays the list of Ethernet interfaces.

Step 3 Click the link under Interface to see detailed information about that interface. The Ethernet Interface page appears.

This page displays the following parameters:

- AP Name—The name of the access point.
- Slot Id—Indicates the slot number.
- Admin Status—Indicates the administration state of the access point.
- CDP State—Select theCDP State check box to enable the CDP state.

Step 4 Click Save.

Configure APs by Importing CSV Files

To import a current access point configuration file, follow these steps:

Note You can use this to configure AP Names, Primary, Secondary, and Tertiary controller details, AP location in bulk.

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 In Unified AP Radio page, select the applicable AP(s), click Import / Export > Import AP Config.

Step 3 Enter the CSV file path in the text box or click Browse to navigate to the CSV file on your computer.

The first row of the CSV file is used to describe the columns included. The AP Ethernet Mac Address column is mandatory. The parameters on this page are used for columns not defined in the CSV file.

Sample File Header:

Example:

```
AP Name,Ethernet MAC,Location,Primary Controller,Secondary Controller,Tertiary Controller
ap-1, 00:1c:58:74:8c:22, sjc-14-a, controller-4404-1, controller-4404-2, controller-4404-3
```

The CSV file can contain following fields.

- AP Ethernet MAC Address—Mandatory
- AP Name—Optional
- Location—Optional
- Primary Controller—Optional
- Secondary Controller—Optional
- Tertiary Controller—Optional

Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primaryMwar and secondaryMwar entries are empty then a unified access point update is not complete.

- Ethernet MAC—AP Ethernet MAC Address
- AP Name—AP Name
- Location—AP Location
- Primary Controller—Primary Controller Name
- Secondary Controller—Secondary Controller Name
- Tertiary Controller—Tertiary Controller Name

Note Optional fields can remain empty. The AP Config Import ignores empty optional field values. However, if primary controller and secondary controller entries are empty then a unified access point update is not complete.

Step 4 When the appropriate CSV file path appears in the Select CSV File text box, click OK.

Configure CDP on Access Points

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices.

Note CDP is enabled on the Ethernet and radio ports of the bridge by default.

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 Choose an access point associated with software release 5.0 or later.

Step 3 Click the slots of radio or an Ethernet interface for which you want to enable CDP.

Step 4 Select the CDP State check box to enable CDP on the interface.

Step 5 Click Save.

Manage Autonomous APs

From Prime Infrastructure, the following methods are available for adding autonomous access points

Add Autonomous APs Using Device Information

Autonomous access points can be added to Prime Infrastructure by device information using comma-separated IP addresses and credentials.

Cisco autonomous access points are shipped from the factory with Cisco as the default enable password. This password allows users to log into the non-privileged mode and execute show and debug commands, posing a security threat. The default enable password must be changed to prevent unauthorized access and to enable users to execute configuration commands from the console port of an access point.

To add autonomous access points using device information, follow these steps:

Step 1 Click Configuration > Network > Network Devices.

Step 2 Click the Plus icon and select Add Devices from the drop-down menu.

Step 3 In the General tab, enter the IP address of the Cisco Access Point. If you are adding by the DNS name, add the DNS name.

Step 4 On the SNMP tab, choose the SNMP version that you created on Cisco Access Point.

Step 5 If you are using SNMP v1 or v2c, then you must provide the read and write community string that was configured on AP. If you are using SNMP v3, then you must configure:

- Username
- Mode
- Auth.Type
- Auth.Password
- Privacy Type
- Privacy Password

Step 6 On the Telent/SSH tab, configure the Telnet/SSH Parameters.

Step 7 On the HTTP/HTTPs tab, provide HTTPs credentials so that Cisco Prime Infrastructure can collect data from them.

- From the Protocol drop-down list, choose HTTP or HTTPs. The TCP Port will change automatically to the default port for the protocol that you have selected.
- In the TCP Port text box, enter a different TCP Port if you want to override the default.
- Enter the name of a user.
- Enter the password and confirm the same.
- Enter the Monitor username, password, and confirm the password.

Step 8 Click Add.

After the AP is added and its inventory collection is completed, it appears in the Autonomous APs list page (Configuration > Network > Network Devices > Device Type > Autonomous AP. If it is not found in the Autonomous APs list, choose Configuration > Network > Network Devices > Device Type > Unknown Devices page to check the status.

Note Autonomous access points are not counted towards the total device count for your license.

Add Autonomous APs Using CSV Files

Autonomous access points can be added to Prime Infrastructure using a CSV file exported from WLSE.

To add autonomous access points using a CSV file, follow these steps:

Step 1 Choose Configuration > Network > Network Devices.
Step 2 Click Plus icon and Select Bulk Import option.
Step 3 Click browse to select the applicable CSV file from your system.
Step 4 Click Import.

Bulk Update of Autonomous APs Using CSV Files

You can update multiple autonomous access points credentials by importing a CSV file.

To update autonomous access point(s) information in a bulk, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.
Step 2 In Autonomous AP Radio page, select the checkbox(es) of the desired AP(s).
Step 3 Click Bulk Update APs.
The Bulk Update Autonomous Access Points page appears.
Step 4 Click Choose File to select a CSV file, and then navigate to the CSV file you want to import.
Step 5 Click Update and Sync.

Sample CSV File for Bulk Update of Autonomous APs

The sample CSV files for V2 devices are as follows:

```
ip_address, network_mask, snmp_version, snmp_community, snmpv3_user_name, snmpv3_auth_type,
 snmpv3_auth_password, snmpv3_privacy_type,
 snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,telnet_timeout
209.165.200.224,255.255.255.224,v2,public,,,,,,3,4209.165.201.0,255.255.255.0,v2,public,,,,,,3,4,Cisco,Cisco,2,10
```

Note The SNMP, telnet, or SSH credentials are mandatory.

The sample CSV files for V3 devices are as follows:

```
ip_address, network_mask, snmp_version, snmpv3_user_name, snmpv3_auth_type,
snmpv3_auth_password, snmpv3_privacy_type,
snmpv3_privacy_password, snmp_retries,
snmp_timeout,telnet_username,telnet_password,telnet_retries,
telnet_timeout209.165.200.224,255.255.255.224,v3,default,HMAC-MD5,default,None,,3,4209.165.201.0,255.255.255.224,v3,
default1,HMAC-MD5,default1,DES,default1,3,4,Cisco,Cisco,2,10
```

The CSV files can contain the following fields:

- ip_address
- network_mask
- snmp_version
- snmp_community
- snmpv3_user_name
- snmpv3_auth_type
- snmpv3_auth_password
- snmpv3_privacy_type
- snmpv3_privacy_password
- snmp_retries
- snmp_timeout
- telnet_username
- telnet_password
- enable_password
- telnet_retries
- telnet_timeout

Deleting Autonomous APs from Prime Infrastructure

Note If you replace Autonomous Access Points because of some reason, remove the Autonomous Access Points from Prime Infrastructure before you install the replacement access points on the network.

To remove an autonomous access point from Prime Infrastructure, follow these steps:

Step 1 Select the check boxes of the access points you want to remove. Select the APs that are not associated.

Step 2 Choose Remove APs from the Select a command drop-down list.

View Autonomous APs

Once added, the autonomous access points can be viewed on the Monitor > Access Points page.

Click the autonomous access point to view more detailed information such as the following:

- Operational status of the access points
- Key attributes including radio information, channel, power, and number of clients on the radio
- CDP neighbored information

The autonomous access points can also be viewed in Monitor > Maps.

They can be added to a floor area by choosing Monitor > Maps floor area and choosing Add Access Points from the Select a command drop-down list.

Download Images to Autonomous APs via TFTP

Lightweight access point images are bundled with controller images and managed by the controller. Autonomous access point images must be handled by a NMS system such as WLSE, CiscoWorks, or Prime Infrastructure.

To download images to autonomous access points using TFTP, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 In Autonomous AP Radio tab, select the check box of the autonomous access point to which you want to download an image.

The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 Click Download > Download Autonomous AP Image (TFTP).
The Download images to Autonomous APs page appears.

Step 4 Configure the following parameters:

- File is located on—Choose Local machine or TFTP server.
- Server Name—Choose the default server or add a new server from the Server Name drop-down list.
- IP address—Specify the TFTP server IP address. This is automatically populated if the default server is selected.
- Prime Infrastructure Server Files In—Specify where Prime Infrastructure server files are located. This is automatically populated if the default server is selected.
- Server File Name—Specify the server filename.

Step 5 Click Download.

Tip Some TFTP servers might not support files larger than 32 MB.

Download Images to Autonomous APs via FTP

To download images to autonomous access points (using FTP), follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 In Autonomous AP Radio tab, select the check box of the autonomous access point to which you want to download an image. The AP Type column displays whether the access point is autonomous or lightweight.

Step 3 Click Download > Download Autonomous AP Image (FTP).
The Download images to Autonomous APs page appears.

Step 4 Enter the FTP credentials including username and password.

Step 5 Click Download.

View Autonomous APs in Workgroup Bridge (WGB) Mode

Workgroup Bridge (WGB) mode is a special mode where an autonomous access point functions as a wireless client and connects to a lightweight access point. The WGB and its wired clients are listed as clients in Prime Infrastructure if the AP mode is set to Bridge, and the access point is bridge capable.

To view a list of all Prime Infrastructure clients that are WGBs, choose Monitor > Clients. From the Show drop-down list, choose WGB Clients, and click Go. The Clients (detected as WGBs) page appears. Click a user to view detailed information regarding a specific WGB and its wired clients.

Note Prime Infrastructure provides WGB client information for the autonomous access point whether or not it is managed by Prime Infrastructure. If the WGB access point is also managed by Prime Infrastructure, Prime Infrastructure provides basic monitoring functions for the access point similar to other autonomous access points.

Export Autonomous AP Details

To export current access point configuration files, follow these steps:

Step 1 Choose Configuration > Wireless Technologies > Access Point Radios.

Step 2 From the Select a command drop-down list, choose Export AP Config.

A pop-up alert box appears stating All Unified AP(s) are exported to CSV/EXCEL/XML file.

Step 3 Click OK to close the pop-up alert box.

Step 4 Click Go to view the current AP configurations including:

a) AP Name
b) Ethernet MAC
c) Location
d) Primary Controller
e) Secondary Controller
f) Tertiary Controller

Step 5 Select the file option (CSV, Excel, XML) to export the access point configurations.

Step 6 In the File Download window, click Save to save the file.

Configure Access Points XOR Antenna

provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

If you choose Configuration > Wireless echnologies > Access Point Radios, and select an XOR (2.4GHz) or XOR (5GHZ) from the Radio column, the following page appears.

This page contains the following fields:

Note Changing any of the fields causes the radio to be temporarily disabled and thus might result in loss of connectivity for some clients.

General

- AP Name—The operator-defined name of the access point.
- AP Base Radio MAC—MAC address of the base radio of the access point.
- Slot ID—Slot ID.
- Admin Status—Select the box to enable the administration state of the access point.
- CDP State—Select the CDP State check box to enable CDP.
- Controller—IP address of the controller. Click the IP address of the controller for more details.
- Site Config ID—Site identification number.
- CleanAir Capable—Displays if the access point is CleanAir capable.
- CleanAir—From the drop-down choose any of the options: Both Disabled, 5GHz Enabled, 2.4 GHz Enabled, and Both Enabled.

Radio Assignment

- Assignment Method—The assignment methods are: Auto, Serving, or Monitor.

Note Band Selection, RF Channel Assignment, and Tx Power Level Assignment appears only for Serving assignment method.

- Band Selection— You can either choose 2.4 GHz or 5 GHz radio.

Antenna

Depending on the Radio Assignment selection, the following parameters appear:

- Antenna Type—Indicates the antenna type: External or Internal.
- XOR A Antenna—(Displayed only for Auto assignment method). Choose the external antenna or Other from the drop-down list.

- XOR B Antenna—(Displayed only for Auto assignment method). Choose the external antenna or Other from the drop-down list.
- External Antenna—(Displayed for Serving and Monitor assignment method). Choose the external antenna or Other from the drop-down list. The values in the drop-down varies for 2.4 GHz and 5GHz radio.
- Antenna Gain—(Displayed for Serving and Monitor assignment method). Enter the desired antenna gain in the text box. To configure the custom antenna gain, select Others for the External Antenna option.

Note The peak gain of the dBi of the antenna for directional antennas and the average gain in dBi for omni-directional antennas connected to the wireless network adapter. The gain is in multiples of 0.5 dBm. An integer value 4 means 4 x 0.5 = 2 dBm of gain.

RF Channel Assignment

The following 802.11a RF Channel Assignment parameters appear only if you have selected Radio Assignment method as Serving.

- Current Channel—Channel number of the access point.
- Channel Width—Only radios with 20 MHz is supported for a 2.4 GHz radio. For a 5 GHZ radio, from the Channel Width drop-down list, choose 20 MHz, 40 MHz, 80 MHz or 160 MHZ.
- Assignment Method—Select one of the following:
  - Global—Use this setting if the channel of the access point is set globally by the controller.
  - Custom—Use this setting if the channel of the access point is set locally. Select a channel from the Custom drop-down list. The values in the drop-down varies for 2.4 GHz and 5 GHz radios.

11n and 11ac Parameters

- 11n Supported—Indicates whether or not 11n radio is supported.
- 11ac Supported—Indicates whether or not 11ac radio is supported.

Performance Profile

Click the URL to view or edit performance profile parameters for this access point interface.

- ClientLink—Enable or disable client link for the access point radios per interface. This feature is only supported for legacy (orthogonal frequency-division multiplexing) OFDM rates. The interface must support ClientLink, and OFDM rates must be enabled. Also, two or more antennas must be enabled for transmission, and all three antennas must be enabled for reception.

Note The maximum number of clients supported is 15. If the antenna configuration restricts operation to a single transmit antenna or OFDM rates are disabled, ClientLink cannot be used.

Tx Power Level Assignment

- Current Tx Power Level—Indicates the current transmit power level.
- Assignment Method—Select one of the following:
  - Global—Use this setting if the power level is set globally by the controller.
  - Custom—Use this setting if the power level of the access point is set locally. Choose a power level from the drop-down list.

11n Antenna Selection

Prime Infrastructure provides the ability to enable or disable the use of specific antennas. All antennas are enabled by default.

Note At least one transmitting and one receiving antenna must be enabled. You cannot disable all transmitting or all receiving antennas at once.

Select any of the 11n Antenna Selection parameters:

- Antenna A
- Antenna B
- Antenna C
- Antenna D

11n Parameters

The following 11n fields appear:

- 11n Supported—Indicates whether or not 802.11n radios are supported.
- Client Link—Use this option to enable or disable client links. Choose Enable, Disable, or Not Applicable from the drop-down list.

Find Access Points

Use the search options in the uppermost right corner of the page to create and save custom searches:

- New Search: Enter an IP address, name, SSID, or MAC, and click Search.
- Saved Searches: Click Saved Search to choose a category, a saved custom search, or choose other criteria for a search from the drop-down lists.
- Advanced Search: An advanced search allows you to search for a device based on a variety of categories and filters.

After you click Go, the access point search results appear (see Table 49: Access Point Search Results , on page 623).

Table 49: Access Point Search Results

Field	Options
IP Address	IP address of the access point.
Ethernet MAC	MAC address of the access point.
AP Name	Name assigned to the access point. Click the access point name item to display details.
Radio	Protocol of the access point is either 802.11a/n or 802.11b/g/n.
Map Location	Campus, building, and floor location.
Controller	IP address of the controller.
AP Type	Access point radio frequency type.
Operational Status	Displays the operational status of the Cisco radios (Up or Down).
Alarm Status	Alarms are color coded as follows: • Clear = No Alarm • Red = Critical Alarm • Orange = Major Alarm • Yellow = Minor Alarm
Audit Status	The audit status of the access point.
Serial Number	The serial number of the access point.
AP Mode	Describes the role of the access point modes such as Local, FlexConnect, Monitor, Rogue Detector, Sniffer, Bridge, or SE-Connect.

Wireless Configuration Groups

Wireless Configuration Groups workflow is the improved workflow of WLAN Controller Configuration Groups feature, which is available in Cisco Prime Infrastructure. With the improved Wireless Configuration workflow, you can:

- Select device specific templates.
- Deploy multiple templates on multiple devices.
- Audit multiple wireless templates from PI.

Note CLI templates and Guest users cannot be deployed from Wireless Configuration Groups.

Create a New Configuration Group

Step 1 Choose Configuration > Wireless Technologies > Wireless Configuration Groups.

Step 2 Click Create to create a new configuration group.
The Configuration Group Workflow wizard appears.

Step 3 In the General Configuration tab, enter the configuration group name, and click Next.
The Select Template tab appears.

Step 4 In the Select Template tab, select the Device Type: CUWN or CUWN-IOS and UA.

Step 5 Drag and drop a template or a group from Templates tree view > My Templates to the Selected Template(s) group box.

The Selected Template(s) group box lists templates or groups, which were added from the Templates tree view.

Step 6 Click Save and Quit to save the configuration group and quit the work flow.

Step 7 Click Next to save the configuration group and to deploy the templates selected.
The Select Devices tab appears.

Step 8 The Select Devices tab lists Controllers based on the device type selected.

Step 9 Select the Device Name check box and click Deploy.
Once the deploy is successful, the Wireless Configuration Groups list page appears.

The Wireless Configuration Groups page contains the following details for the deployed device:

- Group Name
- Last Deployed Devices Count
- Templates Count
- Last Deploy Status
  - Not Initiated —Indicates if the device is deployed on any of the devices or not.
  - Success—Indicates the number of successful templates associated with the applicable IP address.
  - Partial Success / Failure—Indicates the number of failures with provisioning of templates to the applicable controller. Click on Partial Success / Failure link to know the reason for failure.
- Last Undeploy status
- Last Audit Status
- Background Audit—Turn the On/Off toggles to enable the background audit. If this is turned on, then all the templates that are part of this group are audited against the controller during network and controller audits.
- Enforcement—Turn the On/Off toggles to enable the enforcement. If enforcement is turned on, then the templates are automatically applied during the audit if any discrepancies are found.
- Last Modified On
- Last Applied On

Add or Remove Templates from Wireless Configuration Group

The Config Groups Audit page allows you to verify if the controllers configuration complies with the group template. During the audit, you can leave this screen or logout of Cisco Prime Infrastructure. The process continues, and you can return to this page later to view the report.

Note Do not perform any other configuration group functions during the audit verification.

Step 1 Choose Configuration > Wireless Technologies > Wireless Configuration Groups.

Note In Controller List Page, you can click the information icon in Controller List column and then click the export icon to download a CSV file containing details of controllers on which that Configuration Group is configured.

Step 2 Select the Group Name check box, and click Edit.

Step 3 In the Configuration Group Workflow wizard, click Select Templates tab.

Step 4 Choose CUWN or CUWN-IOS.

- Drag and drop a template or a group from the Templates tree view to the Selected Template(s) group box.
- The Selected Template(s) group box will list the selected template or groups which were added from the Templates Tree view.

Step 5 Click Next.

Step 6 In the Device List page, select the devices on which you want to configure the configuration group.

Step 7 Click Deploy to deploy the configuration group on the selected controllers. Or click Save and Quit to configure.

Last Deployed Time column displays timestamp for controllers on which the group is deployed; and displays Not Deployed for the controllers on which the group is only configured.

Audit Wireless Config Groups

The Config Groups Audit page allows you to verify if the controllers configuration complies with the group template. During the audit, you can leave this screen or logout of Cisco Prime Infrastructure. The process continues, and you can return to this page later to view the report.

Note Do not perform any other configuration group functions during the audit verification.

Step 1 Choose Configuration > Wireless Technologies > Wireless Configuration Groups.

Step 2 Select theGroup Name check box, and click Audit.
The Select Devices page appears.

Step 3 Select a Device Name check box and click Audit.

A report is generated and the current configuration on each controller is compared with that in the configuration group template. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

- Audit Status
  - Not Initiated
  - Success—Indicates whether the number of templates associated with the applicable IP address are in sync or not.
  - Not In Sync—Indicates the number of failures with provisioning of templates to the applicable controller. Click Not In Sync to know more details.

View Links in Mesh Networks

You can access mesh link details in several ways:

- Click the Mesh dashboard in home page.
- Choose Monitor > Access Points, click the Mesh Links tab, and click the Details link.
- After you import a KML file from Google Earth, click the AP Mesh link.

The current statistics are displayed at the top of the page followed by diagrams for certain statistics.

- SNR Graph—SNR Up and Down graphs are combined into one graph. Each set of data is represented by different colors.
- Link Metrics Graph—The Adjusted Link Metric and Unadjusted Link Metric is combined into one graph. Each set of data is represented by different colors.
- Packet Error Rate Graph—Displays the packet error rates in a graph.
- Link Events—The last five events for the link are displayed.
- Mesh Worst SNR Links—Displays the worst signal-to-noise ratio (SNR) links.
- AP Uptime—These statistics help determine if an access point is rebooting frequently.
- LWAPP Join Taken Time—These statistics determine how long it takes an access point to join.
- Location Links—Allows you to navigate to Prime Infrastructure map or the Google Earth location.

Define Controller Rogue AP Classification Rules

You can view or edit current rogue access point rules on a single WLC.

To access the rogue access point rules, follow these steps:

Step 1 Choose Configure > Controllers.

Step 2 Click an IP address in the IP Address column.

Step 3 From the left sidebar menu, choose Security > Rogue AP Rules. The Rogue AP Rules displays the rogue access point rules, the rule types (malicious or friendly), and the rule sequence.

Step 4 Choose a Rogue AP Rule to view or edit its details.

Use Controller Auto-Provisioning to Add and Replace WLCs

simplifies WLAN deployments with support for auto-provisioning. Auto provisioning allows Prime Infrastructure to automatically configure a new or replace a current Cisco Wireless LAN Controller (WLC). auto provisioning feature can simplify deployments for customers with a large number of controllers.

Note The controller radio and b/g networks are initially disabled by the startup configuration file. You can turn on those radio networks by using a template, which should be included as one of the automated templates.

View the Controller Auto Provisioning List

The Auto Provision Filters page allows you to create and edit auto provisioning filters that define the list of allowable devices to be auto provisioned or auto monitored by Prime Infrastructure.

For Auto Provisioning privileges, you must have Admin, Root, or Super User status. To allow or disallow a user Auto Provisioning privileges, edit the permitted tasks using Administration > User Roles & AAA User Groups > group name > List of Tasks Permitted in Prime Infrastructure. Select or unselect the check box to allow or disallow these privileges.

Filter parameters include:

Parameter	Description
Filter Name	Identifies the name of the filter.
Filter Enable	Indicates whether or not the filter is enabled. Only enabled filters can participate in the Auto Provisioning process.
Monitor Only	If selected, the Cisco WLC defined in this filter is managed by Prime Infrastructure but not configured by Prime Infrastructure if the Cisco WLC contacts Prime Infrastructure during the auto provisioning process.
Filter Mode	Indicates the search mode for this filter (Host Name, MAC Address, or Serial Number).
Config Group Name	Indicates the Configuration Group name. All Config-Groups used by auto provision filters should not have any controller defined in them.

Create Controller Auto Provisioning Filter

To specify the Auto Provision filter contents, you can directly enter the details in the application or import the details from a CSV file. The auto provisioning feature supports the 5500 and non-5500 series controllers. The non-5500 series controllers have AP manager interface configuration information defined, whereas 5500 series controllers do not have this information.

To add an Auto Provisioning Filter:

Step 1 Choose Configuration > Wireless Technologies > WLAN Controller Auto Provisioning.

Step 2 Choose Add Filterfrom the Select a command drop-down list, then click Go.

Step 3 Enter the required parameters.

You can specify the Dynamic Interface configuration and Device Specific configuration details only when you input a CSV file. These two configurations cannot be performed using the graphical user interface.

Step 4 Click Save.

To change the default username and password, you need to delete and then recreate the admin user and explained in Steps 5 through Step 8.

Step 5 To change the default username and password, you need to create a new read/write user on the controller using the Local Management User Template. You must create this new user so that you can delete the default admin user as shown in Step 6.

Step 6 Choose Inventory > Device Manangement > Network Devices, click on the controller name, click the Configuration tab, then select Management > Local Management User, select the admin user, then from the Select a command drop-down list, select Delete Local Management User and click Go.

Step 7 Create a new admin user on the controller using the Local Management User Template.

Step 8 Delete the user you created in Step 5.

Control the Order of Search for Primary Keys Used in Controller Auto Provisioning

Use the Primary Search Key Setting to set the matching criteria search order.

Step 1 Choose Configuration > Plug and Play > Controller Auto Provisioning, then from the left sidebar menu, choose Setting.

Step 2 Click to highlight the applicable search key, then use the Move Up or Move Down buttons to move the search key to a higher or lower priority.

Step 3 Click Save to confirm the changes.

Information About 9800 Series Configuration Model

Cisco Catalyst 9800 Series Wireless Controller simplifies the configuration of the wireless controller using different tags, namely rf-tag, policy-tag, and site-tag. The access points would derive their configuration from the profiles that are contained within the tags.

Profiles are a collection of feature-specific attributes and parameters applied to a specific target. The configuration targets are AP, radio, and WLAN. The rf-tag contains the radio profiles, the policy-tag contains flex-profile and ap-join-profile, and the wireless-tag contains the WLAN profile and policy profile.

The new configuration model (flexconnect mode) helps the central controller to manage sites that are geo-distributed, for example, retail, campus, and so on, where the WLANs are the same. Only, the network and radio profiles have some changes based on the local deployment or topology.

Table 50: Catalyst 9800 Series Configuration Workflow

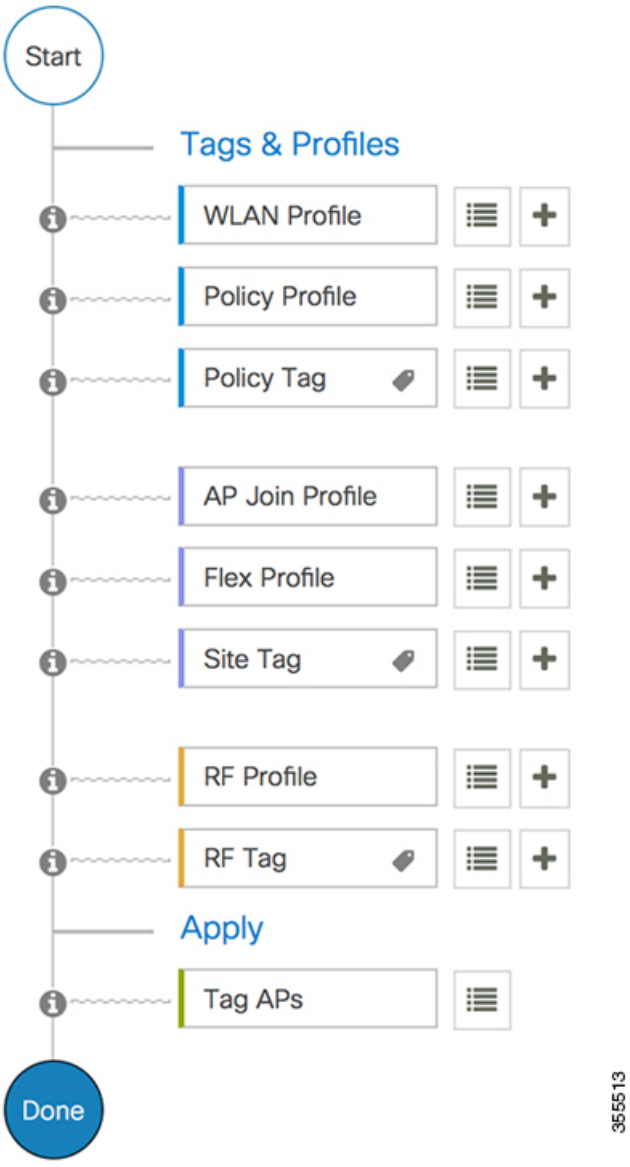
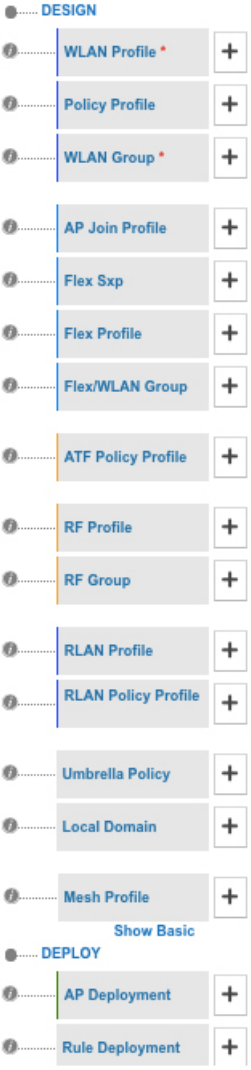
IOS-XE Polaris	Prime Infrastructure
	

Table 51: Mapping of UI constructs between IOS-XE Polaris and Prime Infrastructure

IOS-XE Polaris	Prime Infrastructure
Policy Tag	• WLAN Group • Flex WLAN Group (Prime Infrastructure only) Saves mapping of Flex profile and WLAN profile, which is useful in Flex based deployments
RF Tag	RF Profile
Site Tag	AP Deployment and AP Join Profile AP Deployment name is used to create Site tag on device using: • AP Join Profile and Flex-WLAN Group for Flex based deployment • AP Join Profile and WLAN Group for Non-Flex based deployment

Policy Tag

The policy tag constitutes mapping of the WLAN profile to the policy profile. The WLAN profile defines the wireless characteristics of the WLAN. The policy profile defines the network policies and the switching policies for the client (Quality of Service [QoS] is an exception which constitutes AP policies as well).

The policy tag contains the map of WLAN policy profile. There are 16 such entries per policy tag. Changes to the map entries are effected based on the status of the WLAN profile and policy profile. For example, if a map (WLAN1 and Policy1) is added to the policy tag, and both the WLAN profile and the policy profile are enabled, the definitions are pushed to the APs using the policy tag. However, if one of them is in disabled state, the definition is not pushed to the AP. Similarly, if a WLAN profile is already being broadcast by an AP, it can be deleted using the no form of the command in the policy tag.

Site Tag

The site tag defines the properties of a site and contains the flex profile and the AP join profile. The attributes that are specific to the corresponding flex or remote site are part of the flex profile. Apart from the flex profile, the site tag also comprises attributes that are specific to the physical site (and hence cannot be a part of the profile that is a reusable entity). For example, the list of primary APs for efficient upgrade is a part of a site tag rather than that of a flex profile.

If a flex profile name or an AP profile name is changed in the site tag, the AP is forced to rejoin the controller by disconnecting the Datagram Transport Layer Security (DTLS) session. When a site tag is created, the AP and flex profiles are set to default values (default-ap-profile and default-flex-profile).

RF Tag

The RF tag contains the IEEE 802.11a and IEEE 802.11b RF profiles. The default RF tag contains the global configuration. Both these profiles contain the same default values for global RF profiles for the respective radios.

Profiles

Profiles are a collection of feature-specific attributes and parameters applied to a specific target. The configuration targets are AP, radio, and WLAN. Profiles are reusable entities that can be used across tags. Profiles (used by tags) define the properties of the APs or its associated clients.

WLAN Profile

WLAN profiles are configured with same or different service set identifiers (SSIDs). An SSID identifies the specific wireless network for the controller to access. Creating WLANs with the same SSID allows to assign different Layer 2 security policies within the same wireless LAN.

To distinguish WLANs having the same SSID, create a unique profile name for each WLAN. WLANs with the same SSID must have unique Layer 2 security policies so that clients can select a WLAN based on the information advertised in the beacon and probe responses. The switching and network policies are not part of the WLAN definition.

Policy Profile

Policy profile broadly consists of network and switching policies. Policy profile is a reusable entity across tags. Anything that is a policy for a client that is applied on an AP or controller is moved to the policy profile, for example, VLAN, ACL, QoS, session timeout, idle timeout, AVC profile, bonjour profile, local profiling, device classification, BSSID QoS, and so on. However, all the wireless-related security attributes and features on the WLAN are grouped under the WLAN profile.

Flex Profile

Flex profile contains the attributes that are a part of the flex group. However, policy attributes are grouped with the policy profile. The flex profile also contains remote site-specific parameters. For example, the EAP profiles that can be used when the AP acts as an authentication server for local RADIUS server information, VLAN-ACL mapping, VLAN name-to-ID mapping, and so on.

AP Join Profile

The default AP join profile values will have the global AP parameters and the AP group parameters. The AP join profile contains the following parameters – CAPWAP, IPv4 and IPv6, UDP Lite, High Availability, Retransmit config parameters, Global AP failover, Hyperlocation config parameters, Telnet and SSH, 11u parameters, and so on.

RF Profile

RF profile contains the common radio configuration for the APs. RF profiles are applied to all the APs that belong to an AP group, where all the APs in that group have the same profile settings.

Static Association of APs

APs can only be configured statically using the policy-tag, site tag, and RF tag. The APs are identified by the Ethernet MAC address and the association to AP and tag is stored on the controller as a configuration.

Modifying AP Tags

Modifying an AP tag results in DTLS connection reset, forcing the AP to rejoin the controller. If only one tag is specified in the configuration, default tags are used for other types, for example, if only policy tag is specified, the default-site-tag and default-rf-tag will be used for site tag and RF tag.

Configure Local Domain for Cisco Umbrella Policy for Cisco Catalyst 9800 Series Wireless Controllers

OpenDNS supports splitting of DNS traffic so that administrator can directly send some desired DNS traffic to intended DNS server (For example, a DNS server located within the Enterprise) thereby, bypassing OpenDNS cloud.

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Local Domain to view available profiles, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 In Regex Pattern area, click the Plus icon to create a new local domain.

Step 4 Enter the URL and Save it.

You need to add this local domain to an Umbrella policy.

Configuring Cisco Umbrella Policy for Cisco Catalyst 9800 Series Wireless Controllers

Cisco Umbrella is a Cloud delivered network security service, which protects devices from malware and breach protection in real time.

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Umbrella Policy to view available profiles, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 Enter or edit the requisite details and select a local domain from the Local Domain dropdown menu.

You need to obtain the token for device from OpenDNS dashboard and ensure it is applied on WLC.

Note Prime Infrastructure 3.5 supports only global policy.

Configure a Flex Sxp Profile for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Flex Sxp to view available profiles, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 Enter or edit the requisite details and Save it.

You need to map this Flex Sxp profile to a Flex profile.

Configure a Flex Profile for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Flex Profile to view available profiles, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 Enter or edit the requisite details.

Step 4 To map a Flex Sxp profile or change it, go to Advanced > General and select the profile from Flex Sxp Profile dropdown menu.

Step 5 Click Save.

Configure Airtime Fairness for Catalyst 9800 Series Wireless Controller

Create Airtime Fairness Policy for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click ATF Policy Profile to view available policies or click the Plus icon to create new. Click an existing ATF policy to edit it.

Step 3 Enter or edit the requisite details.

Step 4 Click Save.

Note You need to map this policy to a Policy Profile.

Add Airtime Fairness Policy to a Policy Profile

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click Policy Profile to view available policies or click the Plus icon to create new. Click an existing policy to edit it.

Step 3 Click Access Policies.

Step 4 Under Air Time Fairness Policies, select policy profiles for 2.4 GHz and 5 GHz bands.

You can select separate policies or the same policy for both bands.

Step 5 Click Save.

Enable ATF Policy on an RF profile

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click RF Profile to view available profiles or click the Plus icon to create new. Click an existing profile to edit it.

Step 3 Click Advanced > Air Time Fairness.

Step 4 Select the mode of operation as applicable:

- Disable: To disable ATF on the WLC.
- Enforced: To apply ATF policy on WLC.
- Monitor: To monitor air time usage on your network.

Note You can choose to override the weightage set for WLANs in case of Mesh APs by enabling Override Airtime Allocation. You can enter a weightage for such scenarios when you enable overriding.

Step 5 Click Save.

Configure Remote LAN (RLAN) for Catalyst 9800 Series Wireless Controller

Create RLAN Profile for Cisco Catalyst 9800 Series Wireless Controllers

Remote Lan (RLAN) feature in Prime Infrastructure provides support for wired clients to join the network as wireless clients. WLC authenticates the wired clients. Once a wired client successfully joins, the LAN ports can switch the traffic in Central switching mode or local switching mode depending on the configuration.

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click RLAN Profile to view available policies or click the Plus icon to create new. Click an existing policy to edit it.

Step 3 Enter or edit the requisite details and click Save.

Note You need to map this profile to a WLAN Group.

Create RLAN Policy Profile for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Show Advanced, then click RLAN Policy Profile to view available policies or click the Plus icon to create new. Click an existing policy to edit it.

Step 3 Enter or edit the requisite details and click Save.

You can also configure Access Policies, QoS and AVC, and Advanced parameters.

Note You need to map this profile to a WLAN Group.

Configure WLAN Group for Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click WLAN Group to view available groups, and click the one you want to edit. Alternatively, click the Plus icon to create a new.

Step 3 In WLAN Mapping tab, select the WLAN profile(s) and the policy profile you want to map them to.

Step 4 Click Map To Policy.

Step 5 In RLAN Mapping tab, select the ports on which you want to activate the profile.

Note Ensure these ports are enabled on the AP.

Lightweight Access Points > AP Parameters > AP LAN Port configuration.

Deploy a Rule On Cisco Catalyst 9800 Series Wireless Controllers

Step 1 Click Configuration > Wireless Technologies > Cisco Catalyst 9800 Configuration.

Step 2 Click Rule Deployment to view available policies or click the Plus icon to create a new. Click an existing rule to edit it.

Step 3 Enter the requisite details for the following fields:

- Rule Name – Enter he name of the deployment rule

- AP Name Contains – Enter a regular expression (regex) on the basis of which you want to select the APs on which this rule is deployed.
- Deployment Mode – Select the deployment mode (Flex based or Non-Flex based.

Step 4 Select the Flex Profile, WLAN Group, AP Join Profile, and RF Group from their respective drop-down menus.

Step 5 Click Save.

Step 6 Cick Rule Deployment again to view the list of available rules.

Step 7 Select the rule(s) you want to deploy and then click Deploy.

Step 8 Choose from the available deployment options and then click Deploy.

To see the rule(s) deployed on your Catalyst 9800 Series Wireless Controller, click Configuration > Network > Network Devices > Device Groups > Device Type > Cisco Catalyst 9800 Series Wireless Controller for Cloud > . Click on your Catalyst 9800 Series device and then click Configuration > System > Rule Deployment.

Translate Cisco AireOS Controller Configurations to Cisco Catalyst 9800 Series Controller

AireOS Config Translator provides you with a seamless migration from a legacy Cisco WLC to a Cisco Catalyst 9800 Series Wireless Controller.

Note

- This feature works with Cisco WLCs running AireOS versions 8.8 and above.
- The conversion process may take longer if the WLC configuration is greater than 5000CLIs.
- When you translate an AireOS configuration using AireOS Config Translator, if there are WLANs which have the same IDs as the ones already on the Catalyst 9800 Controller, they are not created.

Before you begin

Please ensure the following criteria are met:

- Both the legacy (AireOS) WLC and the Catalyst 9800 Series controller should already be managed in Prime Infrastructure.
- Both the devices (AireOS and Catalyst 9800 Series) should be added to Prime Infrastructure with valid SNMP and CLI credentials.

Step 1 Click Configuration > Wireless Technologies > AireOS Config Translator.

Step 2 Select the AireOS device from the Select a source AireOS Device list on the Choose Source page.

Step 3 Select the appropriate Catalyst 9800 Series Controller from Select a Target 9800 Device list.

Step 4 Click Fetch Config.

This obtains the Running Config from the source WLC.

Step 5 Click Translate on the Verify and Update Config page.

This translates the fetched AireOS configurations to their Catalyst 9800 Series counterparts. The translated configurations get categorized as follows:

a. Supported – CLIs which were successfully translated

b. Unsupported – CLIs which are either not supported or did not get translated

c. Not Applicable – CLIs for which no translation is required

Step 6 Modify the hostname, passwords, and pre-shared keys in the Supported configurations (highlighted).

Step 7 Check the Accept to deploy checkbox.

Step 8 Click Deploy.

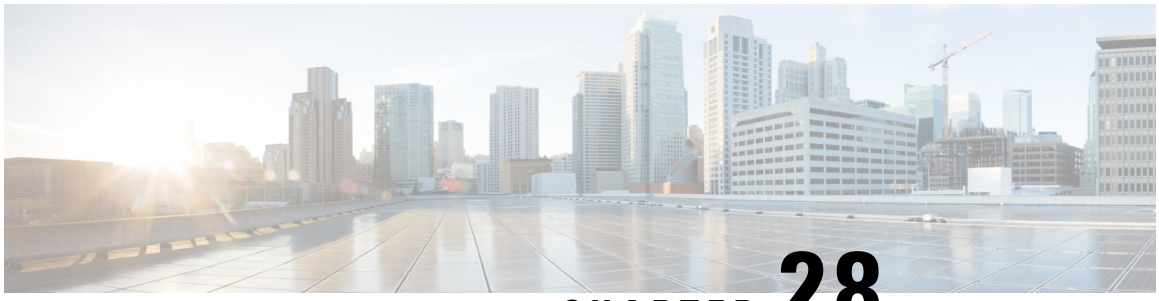
Step 9 Select the APs that you want to migrate and then click Migrate.

Results:

- The primary controller's name and IP address are configured.
- Sync is automatically triggered on Prime Infrastructure.

Related Topics

Add Devices to , on page 29



CHAPTER 28

Schedule Wireless/Data Center Configuration Tasks

View Scheduled Configuration Changes

The Scheduled Configuration Tasks page allows you to navigate to any templates, configuration tasks, or software download tasks that have been scheduled earlier and provides a filtered view of these tasks. This page displays the summary information about a task. The information includes the template name, last time the task was run, next time the task is scheduled to run, and a link to view the results of previous runs. You can also edit the template, modify the schedule, enable, disable, or delete a scheduled task.

After you create and schedule a configuration template, configuration group, or a software download task, the scheduled task or template is listed in the Scheduled Configuration Tasks page.

You cannot create any new scheduled task or template in this page. You can only edit the scheduled task or template that is already created.

You can modify, enable, disable, or delete the following scheduled configuration tasks:

- AP Template
- Configuration Group
- WLAN Configuration
- Download Software

Related Topics

View Scheduled Configuration Changes - Access Point Radio, on page 639
View Schedule Configuration Changes - WLANs, on page 640

View Scheduled Configuration Changes - Access Point Radio

The AP Template Tasks page allows you to manage current access point template tasks. Ensure that at least one lightweight access point task exists (see Configure a Lightweight AP Using Template, on page 432).

Task	Description
Modify a current access point template task	• Choose Configuration > Templates > Scheduled Configuration Task. • Click the template name of the applicable task. • In the AP Radio/Template page, click the Apply/Schedule tab. • Make any necessary changes to the current schedule or access point template, and click Schedule.
Enable a current access point template task	• Choose Configuration > Templates > Scheduled Configuration Task. • Select the check box of the scheduled task to be enabled. • Choose Enable Schedule from the Select a command drop-down list, then click Go.

Related Topics

View Scheduled Configuration Changes, on page 639
View Schedule Configuration Changes - WLANs, on page 640

View Schedule Configuration Changes - WLANs

To view and manage all scheduled WLAN tasks in :

Step 1 Choose Configuration > Template > Scheduled Configuration Task.

Step 2 From the left sidebar menu, choose WLAN Configuration.

Step 3 Select the Task Name link to open the WLAN Schedule Detail page. In this page, you can modify the date and time of the scheduled task.

Step 4 Select the check box of the scheduled task and use the Select a command drop-down list to enable, disable, or delete selected tasks.

Related Topics

View Scheduled Configuration Changes, on page 639
View Scheduled Configuration Changes - Access Point Radio, on page 639

Download Software to Controllers and APs

Use this feature to manage the software download tasks.

• Schedule Software Downloads to Controllers and APs, on page 640
• Change Scheduled Software Downloads, on page 642
• Schedule Controllers for Software Downloads, on page 642

Schedule Software Downloads to Controllers and APs

To add a download software task:

Step 1 Choose Configuration > Template > Scheduled Configuration Task, then from the left sidebar menu, choose Download Software.

Step 2 Choose Add Download Software Task from the Select a command drop-down list, then click Go.

Step 3 Configure the following information:

- General
  - Task Name—Enter a Scheduled Task Name to identify this scheduled software download task.
- Schedule Details
  - Download Type—Select the download type. Select the Download software to controller check box to schedule download software to controller or select the Pre-download software APs check box to schedule the pre-download software APs. If you select Download software to controller, specify the image details.

Note The pre-download option is displayed only when all selected controllers are using the Release 7.0.x.x or later.

To see Image Predownload status per AP, enable the task in the Administration > Dashboards > Job Dashboard > System Jobs > Wireless Poller AP Pre-Download Image Status, and run an AP Image Predownload report from the Report Launch Pad.

- Reboot Type—Indicates whether the reboot type is manual, automatic, or scheduled.

Note Reboot Type Automatic can be set only when the Download software to controller option is selected.

- Download date/time—Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date. Select the time from the hours and minutes drop-down lists.
- Reboot date/time—This option appears only if select the reboot type “Scheduled”. Enter a date in the provided text box or click the calendar icon to open a calendar from which you can choose a date to reboot the controller. Choose the time from the hours and minutes drop-down lists.

Schedule enough time (at least 30 minutes) between Download and Reboot so that all APs can complete the software pre-download.

If any one of the AP is in pre-download progress state at the time of scheduled reboot, the controller does not reboot. In such a case, wait for the pre-download to finish for all of the APs and reboot the controller manually.

- Notification (Optional)—Enter the email address of recipient to send notifications via email.

To receive email notifications, configure Prime Infrastructure mail server in theAdministration > Settings > Mail Server Configuration page.

- Image Details—Specify the TFTP or FTP Server Information:

Complete these details if you selected the Download software to controller option in Schedule Details area.

TFTP—Specify the TFTP Server Information:

- From the File is Located on drop-down list, choose Local machine or TFTP server.

If you choose TFTP server, choose Default Server or add a New server from the Server Name drop-down list.

- Specify the IP address of the TFTP server. This is automatically populated if the default server is selected.
- Specify the local filename or click Browse to navigate to the appropriate file.
- If you selected TFTP server previously, specify the filename.

FTP—Specify the FTP Server Information:

- FTP Credentials Information—Enter the FTP username, password, and port if you selected the FTP radio button.
- From the File is Located on drop-down list, choose Local machine or FTP server.
- If you choose FTP server, choose Default Server or add a New server from the Server Name drop-down list.
- Specify the IP address of the FTP server. This is automatically populated if the default server is selected.

- Specify the local filename, or click Browse to navigate to the appropriate file.
- If you selected FTP server previously, specify the filename.

Step 4 Click Save.

Related Topics

Change Scheduled Software Downloads, on page 642
Schedule Controllers for Software Downloads, on page 642

Change Scheduled Software Downloads

Before You Begin

At least one download software task must exist (see Schedule Software Downloads to Controllers and APs, on page 640).

To modify a download software task:

Step 1 Choose Configuration > Template > Scheduled Configuration Task.

Step 2 From the left sidebar menu, choose Download Software.

Step 3 Click the Task Name link to open the Download Software Task page, make any changes, then click Save.

Any changes in Download Type (Download/Pre-download) or Server Type (FTP/TFTP) for the task in Enabled state sets the task to Disabled state, and all existing controllers are disassociated from the task.

Related Topics

Schedule Software Downloads to Controllers and APs, on page 640
Schedule Controllers for Software Downloads, on page 642

Schedule Controllers for Software Downloads

This page lists all the supported controllers that can be selected for the scheduled image download/pre-download task.

To select a controller for scheduled image download:

Step 1 Choose Configuration > Template > Scheduled Configuration Task.

Step 2 From the left sidebar menu, choose Download Software.

Step 3 Click the Controller to open the Download Software Task details page, then click Select Controller to view the controller list.

Note If the pre-download option is chosen for the task, then only the controllers with software Release 7.0.x.x or later are listed.

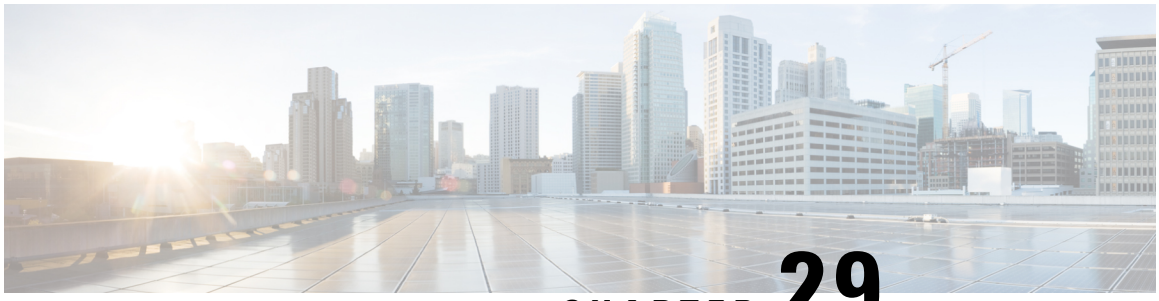
The Select Controllers page can also be accessed by choosing Configuration > Template > Scheduled Configuration Task > Download Software, then clicking the hyperlink in the Select Controller column for any download task that is in the Enabled, Disabled or Expired state.

You cannot download software to any controllers with the Reachability Status of Unreachable.

Step 4 Make any necessary changes, then click Save.

Related Topics

Change Scheduled Software Downloads, on page 642
Schedule Software Downloads to Controllers and APs, on page 640



CHAPTER 29

Use Plug and Play to Deploy New Devices

About Plug and Play

helps automate the deployment of new devices on the network by obtaining and applying the necessary software image and configuration on a new network device. The uses APIC-EM (Application Policy Infrastructure Controller) call-home and Cisco IOS auto-install (which uses DHCP and TFTP) features thus reducing the time a new device takes to join the network and become functional.

The Plug and Play feature of uses the templates defined in Configuration > Templates > Features and Technologies that you can reuse and apply to new devices. You can streamline new device deployment by creating bootstrap templates, which define the necessary initial configurations to enable the device to communicate with . You can specify (and predeploy) software images and configurations that will be added to the devices in the future.

Related Topics

Prerequisites for Using Plug and Play, on page 645

Plug and Play Workflow, on page 646

Prerequisites for Using Plug and Play

You must complete the following prerequisites.

- Configure DHCP with the appropriate settings in the network as described in Sample DHCP Server Settings, on page 666.
- You must have an existing network connection (distribution/core) available in the branch or campus to where the new device is connecting.
- The branch must have direct connectivity to the server, or you must use the Plug and Play external server to connect to .

Related Topics

Create Plug and Play Profiles That Define Device Deployments, on page 651

Plug and Play Workflow

allows you to perform an initial provisioning of a software image and configuration on a new device. To automate the deployment of a new device on your network, follow this workflow:

1. Specify that uses APIC-EM server for Plug and Play. See Integrate Map View With the Plug and Play Dashboard, on page 668 for information about setting up APIC-EM.
2. Create a Plug and Play profile for your devices.The profiles are categorized as Routers, Switches, Wireless AP and Nexus Profiles. See Create Plug and Play Profiles That Define Device Deployments, on page 651.
3. Power on the device.
4. Apply a bootstrap configuration to the device. The bootstrap configuration is a minimal configuration that is required for devices to establish a connection to the gateway (APIC-EM). See Create a Bootstrap Configuration for Plug and Play, on page 661.

In the case of Wireless AP profiles, the Primary, Secondary and Tertiary WLC details are required. See Create Wireless AP Plug and Play Profiles, on page 654.

Note In the case of Nexus devices, the Plug and Play workflow differs as these devices do not support bootstrap configuration. See Create Nexus Device Plug and Play Profiles , on page 654 for more details.

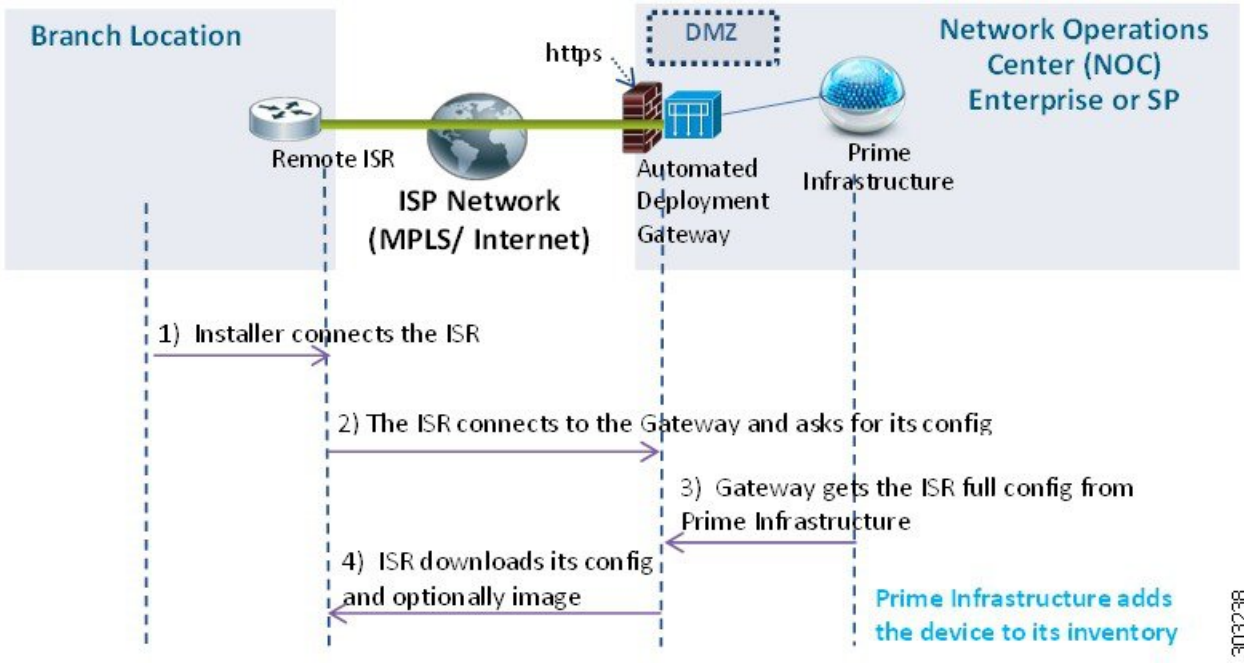
After you apply the initial configuration:

1. The device communicates with the server.
2. Based on the Device Plug and Play ID / serial number, verifies if this matches with the device ID in any of the Plug and Play preprovisioning definitions.
3. If there is a match, applies the upgraded software image and the configuration specified in the matched Plug and Play profile on the device.

   If there is no match for the device ID, matches the device type with any of the existing type-based Plug and Play preprovisioning definitions.
4. The device is added to its inventory and is managed by .
5. Plug and Play does not affect the inventory workflow. applies the post Plug and Play configurations, if specified in the Plug and Play profile, on the device, only after the inventory is collected. See the chapter Add and Organize Devices, on page 29.

After the bootstrap configuration is applied to the device, the installer connects the device to a WAN at the remote site. The device connects to the Plug and Play gateway using its serial number, and downloads the full configuration and (optional) Cisco IOS image (see the following image).

Figure 20: Plug and Play Branch Deployment



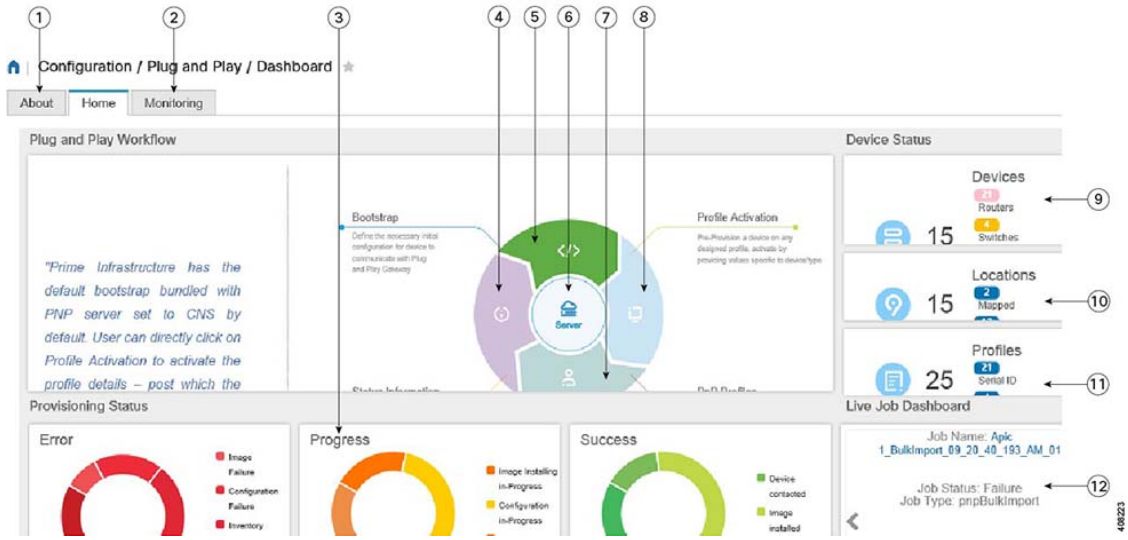
Note The Automated Deployment Gateway is APIC-EM controller.

Related Topics

Create a Bootstrap Configuration for Plug and Play, on page 661
Create Plug and Play Profiles That Define Device Deployments, on page 651

Use the Plug and Play Dashboard to Monitor New Device Deployments

Choose Configuration > Plug and Play > Dashboard and select the Home tab to view the dashboard of the Plug and Play application.



1	Click About to know about Plug and Play feature. See About Plug and Play, on page 645.
2	Click Monitoring to view the details of devices in a map view. See Integrate Map View With the Plug and Play Dashboard, on page 668.
3	Click Errors / Progress / Success to navigate to Device Status page. The details will be filtered and displayed accordingly.
4	Click to navigate to Device Status page to monitor the devices and its status.
5	Click to navigate to Bootstrap page to create bootstrap templates for profiles.
6	Click to navigate to Administration > Servers > APIC-EM Controller page.
7	Click to navigate to Plug and Play Profiles page to create profile for a device type.
8	Click to navigate to Profile Activation page to activate by providing values specific to device/type.
9	Click to navigate to Device Status page.
10	Click to navigate to Map View page to view the devices and their site locations.
11	Click to navigate to Plug and Play Profiles page.
12	Click to navigate to Administration > Dashboard > Jobs Dashboard page to view the job status.

Related Topics

Integrate Map View With the Plug and Play Dashboard, on page 668
Integrate APIC-EM Policy Information into Plug and Play, on page 650
Create Plug and Play Profiles That Define Device Deployments, on page 651
Associate Devices with Plug and Play Profiles, on page 655
Create a Bootstrap Configuration for Plug and Play, on page 661
Verify Devices After They Have Been Deployed Using Plug and Play, on page 667

Prerequisites for Using Plug and Play with APIC-EM

supports APIC-EM GA Release 1.0, APIC-EM GA Release 1.1, APIC-EM GA Release 1.2, APIC-EM GA Release 1.3, APIC-EM GA Release 1.4 amd APIC-EM GA Release 2.0.

Note Any APIC-EM configuration or settings must be done only in the Prime Infrastructure GUI and not in the APIC-EM.

You must preconfigure a profile which determines what is deployed on the devices (configurations, images, etc.). When the device calls home, based on the device's serial number, the profile is matched and the device is provisioned with the same pre-configured image and configuration from using APIC-EM's Plug and Play.

With APIC-EM Plug and Play integration, devices can be provisioned with http/https. If applicable, when the profile is created, you can also choose to install PKI (Public Key Infrastructure) and SUDI (Secure Unique Device Identifier) certificates on the device to use PKI and SUDI based authentication.

Related Topics

Integrate APIC-EM Policy Information into Plug and Play, on page 650
Plug and Play Workflow, on page 646

Prerequisites for Using Plug and Play with Nexus Devices

The following prerequisites should be met before connecting the Nexus device to the network:

- A DHCP server to bootstrap the interface IP address, gateway address, script server (3.2) and script file (Plug and Play). See Configure DHCP Server, on page 649.
- A TFTP or HTTP server containing the configuration script used to automate the software image installation and configuration process. See Configure HTTP Server, on page 650.
- 3. 2 server with created Plug and Play Nexus profile containing the software images and configuration files. See Create Nexus Device Plug and Play Profiles , on page 654.
- The Nexus device version must be higher than 6.2(12) or later to manage all the Nexus features in .

Configure DHCP Server

The Nexus device sends out DHCP discover messages on all of the active interfaces (including the management interface) soliciting DHCP offers from the DHCP server or servers. The DHCP client on the Nexus device uses the device serial number or its MAC address in the client-identifier option to identify itself to the DHCP server. The DHCP server uses this identifier to send information, such as the IP address and script file name, back to the DHCP client.

The DHCP discover message also mandates the following options:

- Option 66 (TFTP server name) or Option 150 (TFTP server address)—The DHCP server relays the TFTP server name or TFTP server address to the DHCP client. The DHCP client uses this information to contact the TFTP server to obtain the script file.
- IP address
- Default Gateway
- Option 67 (Bootfile name)—The DHCP server relays the bootfile name to the DHCP client. The bootfile name includes the complete path to the bootfile on the TFTP server which is used by the DHCP client to download the script file.

Related Topics

Configure HTTP Server, on page 650
Create Nexus Device Plug and Play Profiles , on page 654
Prerequisites for Using Plug and Play with Nexus Devices, on page 649
Add Device Profiles into Nexus Plug and Play Profiles, on page 660

Configure HTTP Server

Choose Administration > Settings > System Settings > General and select Server from the left navigation menu.

In the HTTP Forward section, select Enable to enable the device to contact the Plug and Play Gateway for downloading initial configuration and image. The default port is 80 but you can still change the port configuration on the device.

Note Restart for the changes to reflect.

Related Topics

Configure DHCP Server, on page 649
Create Nexus Device Plug and Play Profiles , on page 654
Prerequisites for Using Plug and Play with Nexus Devices, on page 649
Add Device Profiles into Nexus Plug and Play Profiles, on page 660

Integrate APIC-EM Policy Information into Plug and Play

communicates with APIC-EM via HTTPs and REST API's exposed by APIC-EM.

Note Prime Infrastructure requires a dedicated APIC-EM server. Hence you must not integrate the APIC-EM server with more than one Prime Infrastructure server to prevent data corruption and out of sync condition.

To integrate APIC-EM controller to , follow these steps:

Step 1 Choose Configuration > Plug and Play > Dashboard.

Step 2 In the Home tab, click on Server to view the Administration > Servers > APIC-EM Controller page.

Step 3 Click Add.

Step 4 Enter the APIC-EM controller IPv4 address.

Step 5 Enter the HTTPS port number to connect with APIC-EM.

Step 6 Enter your user name.

Step 7 Enter your password and confirm it.

The polling interval is not editable. The APIC-EM controller is polled periodically (every 5 minutes) to check the status of its connection / integration with . The device status is also updated form the APIC-EM for every 5 minutes.

After the APIC-EM controller is added to , you can view the reachability status of the APIC controller in same page. You can select a specific APIC-EM controller to view the history of the connection polling status. Make sure the APIC-EM connection is successful before using the service.

To navigate to Configuration > Plug and Play > Dashboard, click the link Please Click here to create Plug and Play Profiles.

The global option in Administration > Servers > APIC-EM Controller Global PnP/ZTD Settings is automatically set to APIC-EM when you add a valid APIC-EM controller into .

The APIC-EM integration is not bi-directional, hence you should not make any changes in the APIC-EM for integration.

Related Topics

Create Plug and Play Profiles That Define Device Deployments, on page 651
Create a Bootstrap Configuration for Plug and Play, on page 661
Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647

APIC-EM Site Sync

Prime Infrastructure can integrate and synchronize its inventory with APIC-EM. You need to have a dedicated instance of Prime Infrastructure that integrates with APIC-EM. The dedicated Prime Infrastructure instance can be used for monitoring the network only, not for provisioning.

From the dedicated instance of Prime Infrastructure, specify the APIC-EM instance from the Administration > Servers > APIC-EM Controller page. This Prime Infrastructure instance periodically syncs the sites, devices, device and location groups, WAN interface port groups, and endpoint associations with the APIC-EM instance. Prime Infrastructure collects inventory and other monitoring information for the synced devices and creates a new folder under All Devices > Location and adds the devices to the corresponding sites. Prime Infrastructure monitors the devices by collecting assurance and syslog information.

By default, Prime Infrastructure runs an APIC-EM integration sync job every six hours. If you remove sites and devices from APIC-EM, they are also deleted from Prime Infrastructure. If devices are added or updated in APIC-EM, Prime Infrastructure will also add and update them.

Create Plug and Play Profiles That Define Device Deployments

Choose Configuration > Plug and Play > Dashboardand in the Home tab, click PnP Profiles. The detailed summary of the list of plug and play profiles are displayed.

helps you create a Plug and Play Profile that allows any newly connected device to “call home” to the server so that the device can be discovered, added to the inventory, and configured. This profile, also known as a Bootstrap Profile, places credentials on the device, eliminating the need to “console” into every device to setup before the device can be managed by .

You can create any of the following Plug and Play profiles under the specific folders:

- Router profiles - See Add Device Profiles into Router and Switches Plug and Play Profiles, on page 657
- Switch profiles - See Add Device Profiles into Router and Switches Plug and Play Profiles, on page 657
- Wireless AP profiles - See Create Wireless AP Plug and Play Profiles, on page 654
- Nexus profiles - See Create Nexus Device Plug and Play Profiles , on page 654

Depending on the type, you can create Plug and Play profiles that contain:

- Software images only.
- Configurations only.
- Both software images and configurations.
- PKI certificates and SUDI certificates.
- Primary and Secondary Controllers, AP and Flexconnect groups (For Wireless AP only).

The profile can include additional post Plug and Play configurations (optional), that can be applied on the device only after the device is managed by .

Note You cannot create a profile under the root Plug and Play folder. Depending on the profile-type, you can create profiles only under the specific folders - Nexus Profiles, Switch Profiles, Router Profiles and Wireless AP Profiles.

Note

- PnP scale supports any number of devices distributed across profiles, but a profile can support maximum of 500 devices per profile instance. If you want to increase this scale, create additional profile and add devices to the new profile.
- A maximum of 50 devices will be provisioned simultaneously irrespective of the profile. The PnP agent will pick next set of devices after provisioning of the current 50 devices.
- stores details of the virtual domains under which profiles and profile instances are created and updated. The provisioned devices will be added to the inventory under the respective virtual domains and ROOT-DOMAIN.
- Ensure that the management IP address is unique for each profile instance.
- Adding location groups to profile instances while bulk importing or exporting of device profiles, is not supported. You can create rules under corresponding location groups to dynamically add the managed devices.

Related Topics

Prerequisites for Using Plug and Play with Nexus Devices, on page 649
Associate Devices with Plug and Play Profiles, on page 655
Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647
Verify Devices After They Have Been Deployed Using Plug and Play, on page 667
Delete Plug and Play Profiles, on page 669

Create Router and Switch Plug and Play Profiles

A Plug and Play profile must have at least one of the following:

- A bootstrap configuration— provides a standard bootstrap configuration, or you can create your own. See Create a Bootstrap Configuration for Plug and Play, on page 661.

- Software image—See How to Control Images that are Saved to the Image Repository During Inventory Collection, on page 86.
- Configuration CLI template (PnP and Post PnP configuration)—See Create a New CLI Configuration Template Using a Blank Template, on page 386.

Step 1 Choose Configuration > Plug and Play > Dashboardand in the Home tab, click PnP Profiles.

Step 2 Select the required profile (Router Profiles or Switch Profiles) from the left navigation pane, then click Add to view the details in Profile Summary tab.

Step 3 Provide the required information in the Profile Basic section.

You can select the required credential profile from theCredential Profile drop-down list to associate the credentials common to the device.

Step 4 (Optional) In the Profile Detail section, check the Enable Terminal Server check box to provision devices with terminal server IP and port.

Step 5 (Optional) In the Profile Detail section, check the Enable PKI check box to provision devices with PKI certificates. PKI certificates are installed on the device after the Image provision and configuration are complete. See Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E for more information.

If the Enable PKII check box is unchecked, the device is not provisioned with PKI certificates.

Note Enable PKI check box will be disabled for Switch Profiles.

Step 6 (Optional) In the Profile Detail section, check the Enable SUDI check box to provision devices with SUDI certificates. By enabling this option, you can specify that the APIC-EM controller must validate the SUDI certificate to authenticate the device.

Note If you select Enable SUDI, ensure that the device supports SUDI and add the device using the SUDI serial number.una

Step 7 From the Bootstrap Template drop-down list, select the bootstrap templates. You can also create a customized bootstrap template which will be saved in PnP Bootstrap Templates (User Defined). See Create a Bootstrap Configuration for Plug and Play, on page 661.

Step 8 (Optional) From the Software Image drop-down list, select the required software images. This step is required only if you want to provision the device with images. See Import Software Images for Plug and Play Profiles, on page 654.

Step 9 (Optional) From the Configuration Template drop-down list, select a previously created configuration template.

Step 10 (Optional) From the Post PnP Configuration Template drop-down list, select the required configuration template. This configuration is applied on the device once it is managed by .

Step 11 Click Save as New Plug and Play Profile.

Step 12 The profile is created and the details in Profile Summary tab is displayed. You can edit the details and click Save to save the details in the same profile and click Save as New to create a new profile.

Step 13 Click Profile Instances tab.

Step 14 Click Add to add details for the devices for which you want to pre-provision the Plug and Play Profile. See Add Device Profiles into Router and Switches Plug and Play Profiles, on page 657.

Related Topics

Add Device Profiles into Router and Switches Plug and Play Profiles, on page 657
Import Device Profiles into Plug and Play Profiles, on page 658
Associate Devices with Plug and Play Profiles, on page 655

Create a Bootstrap Configuration for Plug and Play, on page 661

Import Software Images for Plug and Play Profiles

You can import a software image to include it as part of a Plug and Play profile.

Step 1 Choose Inventory > Device Management Software > Software Images.

Step 2 Click Import, then specify the source from which the software image is to be imported.

Step 3 Specify the collection options and when to import the image file. You can run the job immediately or schedule it to run at a later time.

The image import job will run only once.

Step 4 Click Submit.

Step 5 To view the details of image management job, choose Administration > Dashboard > Jobs Dashboard.

Related Topics

Create Router and Switch Plug and Play Profiles, on page 652

Create Wireless AP Plug and Play Profiles

You can create a plug and play profile for a wireless AP to provision thousands of devices at a time.

Step 1 Choose Configuration > Plug and Play > Dashboard, and in the Home tab, click PnP Profiles.

Step 2 Select Wireless AP Profiles from the left navigation pane and click Add to view the details in the Profile Summary tab.

Step 3 Provide the required information in the Profile Basic section.

In the Device Type field, Autonomous AP is auto-populated and is non-editable. It is mandatory to provide the PID value for Wireless AP profiles.

Step 4 Provide the required information in the Profile Detail section.

Step 5 Click Save as New Plug and Play Profile.

Step 6 The profile is created and the details in Profile Summary tab is displayed. You can edit the details and click Save to save the details in the same profile and click Save as New to create a new profile.

Step 7 Click Profile Instances tab.

Step 8 Click Add to add details for the devices for which you want to pre-provision the Plug and Play Profile. See Add Device Profiles into Wireless AP Plug and Play Profiles, on page 659.

Related Topics

Add Device Profiles into Wireless AP Plug and Play Profiles, on page 659
Create a Bootstrap Configuration for Plug and Play, on page 661
Verify Devices After They Have Been Deployed Using Plug and Play, on page 667

Create Nexus Device Plug and Play Profiles

To create a Plug and Play profile for Nexus devices, follow these steps:

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.

Step 2 Select Nexus Profiles from the left navigation pane and click Add to view the details in the Profile Summary tab.

Step 3 Provide the required information in the Profile Basic section.

Select the required credential profile from the Credential Profile drop-down list to associate the credentials common to the device. See Apply Device Credentials Consistently Using Credential Profiles, on page 44.

Step 4 From the System Image and Kick Start Image drop-down lists, select the required software images. See Import Software Images for Plug and Play Profiles, on page 654.

Note While downloading from Cisco.com, ensure that both system and kick start images have the same image version.

Step 5 From the Configuration Template drop-down list, select either the system-defined Nexus POAP Configuration Template or a previously created configuration template and make additional changes.

Step 6 Click Save as New Plug and Play Profile.

Step 7 The profile is created and the details in Profile Summary tab is displayed. You can edit the details and click Save to save the details in the same profile and click Save as New to create a new profile.

Step 8 Click Profile Instances tab.

Step 9 Click Add to add details for the devices for which you want to pre-provision the Plug and Play Profile. See Add Device Profiles into Nexus Plug and Play Profiles, on page 660.

Related Topics

Prerequisites for Using Plug and Play with Nexus Devices, on page 649
Import Software Images for Plug and Play Profiles, on page 654
Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647
Add Device Profiles into Nexus Plug and Play Profiles, on page 660

Associate Devices with Plug and Play Profiles

You can pre-provision a device on any defined profile, and activate by providing values specific to device/type. To add devices in bulk, see Import Device Profiles into Plug and Play Profiles, on page 658.

You can perform either one of the following:

- Create a new plug and play profile and add device profiles to the created plug and play profile. See Create New Plug and Play Profiles and Add Device Profiles, on page 656.
- Add device profiles to an existing plug and play profile. See Add Device Profiles to an Existing Plug and Play Profile, on page 656.

Alternatively, you can choose Configuration > Plun and Play > Dashboard, in the Home tab, click PnP Profiles to create a new Plug and Play profile. After creating the required Plug and Play profile, click Add in the Profile Instances tab to add device profiles.

Related Topics

Add Device Profiles into Router and Switches Plug and Play Profiles, on page 657
Add Device Profiles into Wireless AP Plug and Play Profiles, on page 659
Add Device Profiles into Nexus Plug and Play Profiles, on page 660

Create New Plug and Play Profiles and Add Device Profiles

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Profile Activation.

Step 2 In the Select PnP Profile page, select Add device by creating new Profile.

Step 3 Select the type of profile you want to create from the Profile Type drop-down list.

Step 4 Enter the required information in the Profile Basic and Profile Detail sections. See Create Plug and Play Profiles That Define Device Deployments, on page 651 for information on profile creation.

Step 5 (Optional) Enter the Terminal Server IP and Port if the Enable Terminal Server check box has been selected while creating a Plug and Play profile.

Step 6 Click the arrow icon in the right to navigate to the Plug and Play Profile page to add device profiles to the created plug and play profile.

Step 7 (Optional) If the Enable Terminal Server check box is checked, import the raw configuration on the device by:

a. Import the zip files or tar files which contains multiple text files. Each text file will contain raw configuration that needs to be applied to the device. You can also import a single text file if required.

   The name of the text file should be DeviceSerialID.txt or DeviceName.txt. For example if the device ID is FGLABCD443f, the text file containing the configuration details must be FGLABCD443f.txt or if the device name is XaaaXX, the text file containing the configuration details must be XaaaXX.txt.

b. A job will be triggered for processing these files and uploading to APIC when the files are uploaded successfully.

c. Verify the configuration has been successfully applied to the corresponding devices in that profiles by going to that particular profile in APIC.

Related Topics

Add Device Profiles to an Existing Plug and Play Profile, on page 656
Add Device Profiles into Router and Switches Plug and Play Profiles, on page 657
Add Device Profiles into Wireless AP Plug and Play Profiles, on page 659
Add Device Profiles into Nexus Plug and Play Profiles, on page 660

Add Device Profiles to an Existing Plug and Play Profile

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Profile Activation.

Step 2 In the Select PnP Profile page, select Add device to an existing profile.

Step 3 Select the required profile from the Select Profile drop-down list, for which you need to add device profiles. See Create Plug and Play Profiles That Define Device Deployments, on page 651for information on profile creation.

Step 4 The details of the profile you selected gets auto-populated and are non-editable.

Step 5 Click the arrow icon in the right to navigate to the Plug and Play Profile page to add device profiles to the created plug and play profile.

Related Topics

Create New Plug and Play Profiles and Add Device Profiles, on page 656
Add Device Profiles into Router and Switches Plug and Play Profiles, on page 657
Add Device Profiles into Wireless AP Plug and Play Profiles, on page 659

Add Device Profiles into Nexus Plug and Play Profiles, on page 660

Add Device Profiles into Router and Switches Plug and Play Profiles

To add a device profile to the required Plug and Play profile, follow these steps:

Step 1 In the Plug and Play Device Provisioning Profile page, provide the required information.

- Select the site location to which the device will be mapped from the Location drop-down list. This detail will be displayed in the Map View.

Note Before you add a device to a specific location, create a location group in Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups. See Create Location Groups, on page 50.

Step 2 Click the arrow icon in the right to navigate to the Bootstrap Selection page.

Step 3 In the Bootstrap Selection page, the bootstrap template you selected in the profile creation phase will get auto-populated. You can edit the values as required.

- Plug and Play Gateway Location—By default, the server acts as the Plug and Play gateway server. You can modify the server by providing the external Plug and Play gateway IP address.

Click CLI to view the CLI summary of the bootstrap configured.

Step 4 Click the arrow icon in the right to navigate to the next pages.

Note If you had selected Software Image and Configuration Template in the profile creation phase, the Software Image, Configurationu and Post PnP Configuration tabs will be displayed in the Profile Activation page.

Step 5 (Optional) In the Software Image page, provide the required information.

Step 6 (Optional) In the Configurationu page, the configuration template you selected in the profile creation phase will be auto-populated. Provide the required information and navigate to the next page.

Click CLIto view the CLI summary.

Step 7 (Optional) In the Post PnP Configuration page, the configuration template you selected in the profile creation phase will be auto-populated. Provide the required information and navigate to the next page.

Click CLI to view the CLI summary.

Step 8 In the Management Credentials page, provide the required information. These device parameters ill be applied on the devices on provisioning.

Note If the device type is a router or switch, then in the Management Credentials page, the credential profile you selected in the profile creation phase will be auto-populated and the values cannot be edited.

Step 9 In the Profile Activation Summary page, the device details with their configurations is displayed.

Step 10 Click Finish to provision the device profile.

On successful provisioning, the device profile will be displayed in the Profile Instances page of the specific profile. Alternatively, the provisioning status of the device can be viewed at the Device Status page.

After the device is provisioned successfully, the device is added to the inventory so that the device can be managed. The device is added to the inventory based on the management parameters provided in the Plug and Play Profile. After

the device is added successfully to the inventory, additional post Plug and Play configurations (if applicable) are applied on the device.

If there is a mismatch in credentials, the device is added to the inventory, but it will not have “Managed” status.

Related Topics

Import Device Profiles into Plug and Play Profiles, on page 658
Create Plug and Play Profiles That Define Device Deployments, on page 651
Create Router and Switch Plug and Play Profiles, on page 652
Add Device Profiles into Nexus Plug and Play Profiles, on page 660
Add Device Profiles into Wireless AP Plug and Play Profiles, on page 659

Import Device Profiles into Plug and Play Profiles

You can perform import and export operations on device profiles in bulk. Instead of adding devices and specifying their attributes one at a time, you can import a CSV file that includes all the devices and their attributes. By performing bulk import, you can update the existing profiles and add new profiles. To update more than one device profile at a time, you can perform bulk export.

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.

Step 2 Select the required Plug and Play profile from the left navigation menu. The details in Profile Summary tab is displayed.

Step 3 Click Profile Instances tab.

Step 4 Select the device profiles check-boxes you need to edit and click Export.

The CSV file with the device properties will be exported.. You can add devices or edit the properties of the existing devices in the spreadsheet. Do not change the attribute names while editing the spreadsheet.

Note If you want to export a blank CSV file, click Export without selecting any device profiles. A blank csv file will be exported even if there are no device profiles in the Profile Instances page.

Step 5 Click Import and choose the CSV file in which you entered the device details. Click Upload.

The CSV file is uploaded and a link to Administration > Dashboard > Jobs Dashboard is displayed.

Step 6 In the Jobs Dashboard page, click PnP Bulk Import from the left navigation menu to view the job status of the bulk imported file.

Related Topics

Create Router and Switch Plug and Play Profiles, on page 652
Add Device Profiles into Nexus Plug and Play Profiles, on page 660
Add Device Profiles into Wireless AP Plug and Play Profiles, on page 659
Deployment Based on Device Type, on page 658

Deployment Based on Device Type

To deploy a Plug and Play profile based on the device type, you do not have to associate the device ID with the deployment profile. Device type-based deployment is useful primarily for switches that use the same set of images and configurations. Matching profiles are identified by the device type (PID) of the incoming device that is specified in the profile during the design phase.

During device type-based deployment:

1. The device type is matched hierarchically; searches for a profile with the same device type as that of the incoming device. If the profile does not match the device type, searches for a profile that is defined for a higher level of the device type in the hierarchy. For example:
   - If the 'switch_profile' in is defined for 'Switches and Hubs' and the incoming device is of type Switches and Hubs > Catalyst 2928 Series Switches > Catalyst 2928-24TC-C switch, and
   - If there is no profile defined specifically for this switch (Catalyst 2928-24TC-C or Catalyst 2928 Series Switches), then the 'switch_profile' is considered for deployment
2. If has multiple matching deployment profiles for a given device type, then chooses the deployment profile that is created or has been recently updated.

Related Topics

Import Device Profiles into Plug and Play Profiles, on page 658

Add Device Profiles into Wireless AP Plug and Play Profiles

supports only APIC-EM for Wireless AP profiles. You must preconfigure a plug and play profile which determines the primary, secondary and tertiary WLC details that is required to be provisioned on the devices. See Create Wireless AP Plug and Play Profiles, on page 654.

When the AP (Access Point) is connected to a network, the AP contacts the DHCP of the network to know the APIC-EM details. The AP then contacts the APIC-EM and based on the device's serial number and PID, the profile is matched. AP contacts WLC which then pushes the image and configurations to the device.

To add a device profile to the required Plug and Play profile, follow these steps:

Step 1 In the Plug and Play Device Provisioning Profile page, provide the required information.

Select the site location to which the device will be mapped from the Location drop-down list. This detail will be displayed in the Map View.

Note Before you add a device to a specific location, create a location group in Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups. See Create Location Groups.

Step 2 In the Profile Activation Summary page, the device details with their configurations is displayed.

Step 3 Click Finish to provision the device profile.

On successful provisioning, the device profile will be displayed in the Profile Instances page of the specific profile. Alternatively, the provisioning status of the device can be viewed at the Device Status page.

Related Topics

Associate Devices with Plug and Play Profiles, on page 655
Create Plug and Play Profiles That Define Device Deployments, on page 651
Create Wireless AP Plug and Play Profiles, on page 654
Add Device Profiles into Router and Switches Plug and Play Profiles, on page 657
Add Device Profiles into Nexus Plug and Play Profiles, on page 660

Add Device Profiles into Nexus Plug and Play Profiles

Before you begin, there is a set of prerequisites to be met. See Prerequisites for Using Plug and Play with Nexus Devices, on page 649.

When a Nexus device is connected to the network, it follows the below workflow:

1. Locates the configured DHCP server and establishes communication to get the IP Address, gateway, script server (3.2) and the script file (Nexus Plug and Play profile).
2. The device then communicates with the and downloads the created Plug and Play profile for Nexus device. See Create Nexus Device Plug and Play Profiles , on page 654.
3. The device then obtains the IP address of a TFTP server or URL of an HTTP server from which it downloads the image and the necessary configuration files.

To add a device profile to the required Plug and Play profile, follow these steps:

Step 1 In the Plug and Play Device Provisioning Profile page, provide the required information.

Select the site location to which the device will be mapped from the Location drop-down list. This detail will be displayed in the Map View.

Note Before you add a device to a specific location, create a location group in Inventory > Device Management > Network Devices or Inventory > Group Management > Network Device Groups. See Create Location Groups, on page 50.

Step 2 Click the arrow icon in the right to navigate to the Image Selection page.

The selected system and kick start images are auto-populated and cannot be edited.

Step 3 Click the arrow icon in the right to navigate to the Configuration page.

The configuration template you selected in the profile creation phase will be auto-populated. You should provide the Management Interface IP Address, Management Route IP Address and the other required information. This management IP address is configured to enable d to reach the Nexus device.

Click CLI to view the CLI summary.

Step 4 Click the arrow icon in the right to navigate to the Management Credentials page.

For Nexus devices, it is mandatory to specify the Management IP Address so that the device can be managed. Provide the other required information and navigate to the next page. These device parameters will be applied on the devices on provisioning.

Step 5 In the Profile Activation Summary page, the device details with their configurations is displayed.

Step 6 Click Finish to provision the device profile.

On successful provisioning, the device profile will be displayed in the Profile Instances page of the specific profile. Alternatively, the provisioning status of the device can be viewed at the Device Status page. The device is added to the inventory so that the device can be managed.

Related Topics

Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647
Create Plug and Play Profiles That Define Device Deployments, on page 651
Prerequisites for Using Plug and Play with Nexus Devices, on page 649

Create Nexus Device Plug and Play Profiles , on page 654
Add Device Profiles into Router and Switches Plug and Play Profiles, on page 657
Add Device Profiles into Wireless AP Plug and Play Profiles, on page 659

Supported Devices and Software Images for Plug and Play

If you are using APIC-EM, the Prime Infrastructure Plug and Play will support only the devices supported by APIC-EM.

Refer Release Notes for Cisco Network Plug and Play to know the devices and the corresponding software images supported for APIC-EM.

For more Details on all the supported devices and the corresponding sysObjectIDs, see Cisco Prime Infrastructure Supported Devices.

Related Topics

Create Plug and Play Profiles That Define Device Deployments, on page 651
Plug and Play Workflow, on page 646

Prerequisites for Deploying Bootstrap Configuration into a Device

To deploy bootstrap configuration into a device in a Server:

- Enable Cipher in Admin mode of the server by entering the following command.

ncs run pnp-ciphers enable

- Click Enable in the HTTP Forward section of the Administration > Settings > System Settings page.
- If you are going to use email to deliver either the bootstrap configuration or the PIN, you must have previously configured the mail server settings under Administration > Settings > System Settings > Mail Server Configuration.
- Ensure TFTP is enabled on the server by choosing Administration > Settings > System Settings > Server, then clicking Enable under TFTP. TFTP is enabled by default.

Related Topics

Create a Bootstrap Configuration for Plug and Play, on page 661

Create a Bootstrap Configuration for Plug and Play

A bootstrap configuration is a minimal configuration that is required for devices to establish a connection to the gateway (APIC-EM). provides a standard bootstrap configuration that you can use.

If you are using the DHCP option, you do not need to create a bootstrap configuration. See Export Bootstrap Configurations Using DHCP, on page 666.

To create a user-defined bootstrap template, follow these steps:

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Bootstrap.

By default, an APIC Bootstrap and Plug and Play Bootstrap template will be displayed. These templates cannot be deleted.

Step 2 Select the specific Bootstrap check-box and click Clone to clone a similar template. This new template will be displayed as APIC Bootstrap_1, APIC Bootstrap_1_1, and so on or Plug and Play Bootstrap_1, Plug and Play Bootstrap_1_1 and so on, depending on the bootstrap you cloned.

Note
- You can rename the cloned template. Once renamed, you cannot change the template name again.
- Make sure that you do not use the Configuration > Templates > Features & Technologies > CLI Templates > System Templates-CLI > Plug And Play Bootstrap to create a customized bootstrap template.

Step 3 Click Save.

Step 4 Click the pointer beside the Bootstrap template to view or edit the details.

Step 5 Click Update to save the changes. Click CLI to view the CLI summary.

Step 6 To delete any bootstrap template, select the specific bootstrap template check-box and click Delete.

These templates that you create will be saved in PnP Bootstrap Templates (User Defined).

You can choose this newly created bootstrap template when adding a profile instance by selecting the specific bootstrap template from PnP Bootstrap Templates (User Defined). The details will automatically be displayed and will be editable.

The bootstrap configurations that provides the following content:

- APIC-EM HTTP Bootstrap

```
pnp profile network-pnp
transport http ipv4 <APIC-EM server IP>
```

- APIC-EM HTTPS Bootstrap

```
crypto ca trustpoint <APIC-EM Server IP>.cisco.com
enrollment mode ra
enrollment terminal
usage ssl-client
exit
crypto ca authenticate <APIC-EM Server IP>.cisco.com
-----BEGIN CERTIFICATE-----
Certificate detail
-----END CERTIFICATE-----
pnp profile network-pnp
transport https ipv4 <APIC-EM Server IP> port 443
!
```

Related Topics

How to Install Bootstrap Configurations?, on page 663
Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647
Create Plug and Play Profiles That Define Device Deployments, on page 651
Associate Devices with Plug and Play Profiles, on page 655
Prerequisites for Deploying Bootstrap Configuration into a Device, on page 661

How to Install Bootstrap Configurations?

A bootstrap configuration is a minimal configuration that is required for devices to establish a connection to the gateway (APIC-EM). The bootstrap configuration can be installed on the devices using any of the bootstrap delivery methods that supports:

- Export and download the bootstrap—If you have access to the device console, you can export the bootstrap, and then copy and paste the bootstrap configuration to the device. See Export .
- Deploying bootstrap configuration through terminal server. See Deploy the Bootstrap Configurations Using Terrminal Server in related topics.
- Export and save the bootstrap to a USB flash drive—You can save the bootstrap configuration to a USB drive with the file name ciscortr.cfg. Connect the USB drive to the device, and then boot the device. The device will retrieve the bootstrap configuration from the USB drive. See Export Boostrap Configurations Using TFTP in related topics.
- Email the bootstrap. See Email Bootstrap Configuration in related topics..
- DHCP options based on the server you specified. See Export Bootstrap Configurations Using DHCP in related topics..
    - You can configure DHCP option 43 on the APIC-EM server IP under DHCP Configuration. When a device gets its IP address from DHCP, it will get the bootstrap configuration also.
- Mobile application—You can use the Cisco Network Plug and Play mobile application.

Related Topics

Prerequisites for Deploying Bootstrap Configuration into a Device, on page 661
Create a Bootstrap Configuration for Plug and Play, on page 661
Deploy the Bootstrap Configuration Using Terminal Server, on page 664
Export the Bootstrap Configuration, on page 663
Export Bootstrap Configurations Using DHCP, on page 666
Export the Bootstrap Configuration Using TFTP, on page 664
Email Bootstrap Configuration, on page 665

Export the Bootstrap Configuration

You can export a bootstrap configuration and then manually apply the bootstrap on the device. After the bootstrap configuration is applied, the Plug and Play deployment is initiated and the administrator can view the configuration status on .

Step 1 Choose Configuration > Plug and Play > Dashboard, and in the Home tab, click PnP Profiles.

Step 2 From the Plug and Play Profiles page, select a profile from the list.

Step 3 Click Profile Instances.

Step 4 Click Export Bootstrap > Download Bootstrap, then click OKs.

Step 5 After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated.

Related Topics

Export the Bootstrap Configuration Using TFTP, on page 664

Email Bootstrap Configuration, on page 665
Export Bootstrap Configurations Using DHCP, on page 666
Create a Bootstrap Configuration for Plug and Play, on page 661

Deploy the Bootstrap Configuration Using Terminal Server

If you have enabled the check box Enable Terminal Server while creating a Plug and Play profile you can deploy bootstrap config:

Step 1 Select the devices from the Plug and Play profile.

Step 2 Click Deploy button.

Step 3 Click OK in the pop up dialogue box to trigger a job to execute the bootstrap on to the device directly by using Terminal Server.

You can check the status of the PnP Terminal Server job on the Job Dashboard.

The APIC will provision the device when the job is executed successfully. The device will be added to the inventory once the device is provisioned.

Related Topics

Create Plug and Play Profiles That Define Device Deployments, on page 651

Export the Bootstrap Configuration Using TFTP

You can use the TFTP protocol to deliver the bootstrap configuration to the TFTP server. You can specify the file name that should be created on the TFTP server; this file is used by the auto-install enabled devices to get the IP address and other details through the DHCP. In the DHCP server, the TFTP server must be configured as the TFTP server. For more information, see Cisco Open Plug-n-Play Agent Configuration Guide, Cisco IOS XE Release 3E.

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.

Step 2 From the Plug and Play Profiles page, select a profile from the list.

Step 3 Click Profile Instances.

Step 4 Click Export Bootstrap > TFTP.

Step 5 After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated.

Related Topics

Email Bootstrap Configuration, on page 665
Create a Bootstrap Configuration for Plug and Play, on page 661
Export Bootstrap Configurations Using DHCP, on page 666

Email Bootstrap Configuration

You can email the bootstrap configuration and then manually apply the bootstrap on the device. After the bootstrap configuration is applied, the automated deployment is initiated. The administrator can view the configuration status on .

Note Before you can email the bootstrap configuration, you must set the email settings under Administration > Settings > System Settings > Mail and Notification > Mail Server Configuration.

To email the bootstrap configuration to the operator:

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click PnP Profiles.
Step 2 From the Plug and Play Profiles page, select a profile from the list.
Step 3 Click Profile Instances.
Step 4 Click Export Bootstrap > Download Bootstrap.
Step 5 Enter the email address to which the bootstrap configuration is be sent, then click OK.
Step 6 After the bootstrap configuration is downloaded and applied, the Plug and Play deployment is initiated.

Related Topics

Create a Bootstrap Configuration for Plug and Play, on page 661
Export Bootstrap Configurations Using DHCP, on page 666
Export the Bootstrap Configuration, on page 663
Export the Bootstrap Configuration Using TFTP, on page 664

Email PIN for the Bootstrap Configuration

generates a random Personal Identification Number (PIN) per device. This PIN can be used to identify the device and the Plug and Play profile (bootstrap configuration) associated with it. After the pre-provisioning tasks are complete, the administrator must use the Email PIN option (available in the pre-provisioning task of the) to email the unique PIN to the deployment engineer. During installation, the deployment engineer uses this PIN to download the bootstrap configuration from the server.

To deliver the PIN for the bootstrap configuration:

Step 1 Choose Configuration > Plug and Play > Dashboardand in the Home tab, click PnP Profiles.
Step 2 From the Plug and Play Profiles page, select a profile from the list.
Step 3 Click Profile Instances tab.
Step 4 Click the Email PIN.
Step 5 Enter the email address to which the PIN should be sent and click OK.
Step 6 Use one of the following methods to apply the bootstrap configuration:

- If you are applying the bootstrap configuration using the deployment application , the Plug and Play deployment application communicates to the and applies the bootstrap configuration on the device.

- If you are manually applying the bootstrap configuration using the PIN:
  - Use the PIN to download the bootstrap configuration from the Plug and Play gateway. You can also register the ISR's serial number during this process.
  - Apply the bootstrap configuration on the device manually, using a console or USB flash.

For detailed information about Plug and Play deployment, see the Cisco Plug and Play Application User Guide.

Step 7 After the bootstrap configuration is applied, the Plug and Play deployment is initiated.

Related Topics

Email Bootstrap Configuration, on page 665
Create a Bootstrap Configuration for Plug and Play, on page 661
Export Bootstrap Configurations Using DHCP, on page 666
Export the Bootstrap Configuration, on page 663
Export the Bootstrap Configuration Using TFTP, on page 664

Export Bootstrap Configurations Using DHCP

To use the DHCP option to export a bootstrap configuration, you must have the following configuration on your devices:

- For APIC-EM—DHCP option 43

```
ip dhcp pool <DHCP pool name>
network <subnet> <subnet mask>
default-router <default gateway>
option 43 ascii "5A1D;B2;K4;I<APIC-EM_server_IP>;J80"
```

Related Topics

Export the Bootstrap Configuration, on page 663
Sample DHCP Server Settings, on page 666
Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647
Create Plug and Play Profiles That Define Device Deployments, on page 651
Create a Bootstrap Configuration for Plug and Play, on page 661
How to Install Bootstrap Configurations?, on page 663

Sample DHCP Server Settings

If you select the DHCP-based method to deliver the Plug and Play Profile, you must configure the DHCP server to redirect the switch to the TFTP server by entering the commands described in the following table.

The DHCP-based method follows these steps:

1. The new switch contacts the DHCP server. You must configure the DHCP server to redirect the switch to the TFTP server. See the following table for more information.
2. The DCHP server points the switch to the new TFTP server where the Plug and Play bootstrap profile resides.
3. The switch loads the bootstrap configuration file, boots up, and then contacts the Plug and Play Gateway.

Table 52: DHCP Server Settings

Command to Enter	Description
`ip dhcp pool PNP`	Creates a DHCP pool named PNP.
`network 10.106.190.0 255.255.255.224`	Defines the network 10.106.190.0 and subnet mask 255.255.255.224. DHCP uses this pool of IP addresses to assign an IP address to the new device.
`default-router 10.106.190.17`	Configures the default route 10.106.190.17 on the new device.
`option 150 ip 10.77.240.224`	Specifies that the TFTP server IP address 10.77.240.224 is the server IP address.

Related Topics

Export the Bootstrap Configuration, on page 663
Export Bootstrap Configurations Using DHCP, on page 666
Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647
Create Plug and Play Profiles That Define Device Deployments, on page 651
Create a Bootstrap Configuration for Plug and Play, on page 661
How to Install Bootstrap Configurations?, on page 663

Verify Devices After They Have Been Deployed Using Plug and Play

Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Status Information.

The device details (Serial ID, hostname, IP address, type, profile name, location), current and post Plug and Play statuses, and the graphical representation of the provisioning status are displayed in a List view.

Click Map in the upper right corner to view the device details and their statuses in map view. See Related topics.

You can choose Administration > Dashboard > Jobs Dashboard > User Jobs > Post PnP Status to view the status of post Plug and Play configuration job on a device.

You can provision the device profiles again by selecting a device from the list and clicking the Reset button. Choose Configuration > Plug and Play > Dashboard > Device Status. The Reset button is enabled only for devices that have been successfully provisioned or when the provisioning has failed. It is not enabled for devices that show the provisioning status as pending.

You can also reset the device profiles in the profile instance page by choosing Configuration > Plug and Play > Dashboard > Profiles > Router Policies.

On resetting a device, provisioning status will be reset to pending.

If is integrated with APIC-EM GA Release 1.2.0.x or higher versions of APIC-EM, on resetting the device, it will first be reloaded if the provisioning had failed earlier.

Related Topics

Integrate Map View With the Plug and Play Dashboard, on page 668
Delete Plug and Play Profiles, on page 669
Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647

Create Plug and Play Profiles That Define Device Deployments, on page 651
Associate Devices with Plug and Play Profiles, on page 655
Create a Bootstrap Configuration for Plug and Play, on page 661

Integrate Map View With the Plug and Play Dashboard

You can view the details in a map view in any of the following ways:

- Choose Configuration > Plug and Play > Dashboard and click Monitoring tab.
- Choose Configuration > Plug and Play > Dashboard and clickHome tab. Click Status Information and click Map from the upper right corner of the Device Status page.
- Choose Configuration > Plug and Play > Dashboard and click Home tab. ClickLocations.

1	Click to view the map in full screen.
2	You can perform zooming operations using mouse or keyboard. With keyboard, click the + or - signs to zoom in or zoom out. With mouse, use the mouse scroll wheel to zoom in or zoom out or double-click to zoom in.
3	Click to view the provisioning status of the device in detail.
4	Click to view the sites that do not have geographical coordinates specified.
5	Click to view the devices that are not mapped to any location. Drag and drop the devices to a location in the map. The device automatically gets mapped to that location group.
6	Toggle the button to enable edit mode. Once enabled, you can drag and drop the unmapped devices to a location in the map. Before you map a device to a location, create location groups. See Create Location Groups, on page 50.
7	Select a location from the list.
8	Click to view the cluster details. A cluster represents two or more locations in a geographical area. Hover the mouse over the site to view the number of devices mapped to it. Click the number hyperlink to view the device details.

9	Click List to view the Device Status page.

Related Topics

Verify Devices After They Have Been Deployed Using Plug and Play, on page 667
Delete Plug and Play Profiles, on page 669
Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647
Create Plug and Play Profiles That Define Device Deployments, on page 651
Associate Devices with Plug and Play Profiles, on page 655
Create a Bootstrap Configuration for Plug and Play, on page 661

Delete Plug and Play Profiles

If you are using APIC-EM for Plug and Play, you might need to delete a plug and play profile that is incorrect or outdated.

Note

- If you delete a device from Prime Infrastructure Plug and Play, it gets deleted from APIC-EM, whereas if you delete a device from APIC-EM, it will remain in Prime Infrastructure.
- You must not create a profile in APIC-EM, when APIC-EM is integrated with Prime Infrastructure.
- If you delete a device from Plug and Play, you can immediately add the device back to Plug and Play.

Step 1 Execute the following command from the router CLI to remove the Plug and Play profile from the router:

no pnp profileplug_and_play_profile_name.

Step 2 Delete the provisioning profile by choosing Configuration > Plug and Play > Dashboardand clickPnP Profiles. Select a Plug and Play profile, click Profile Instances, then delete the required provisioning profile.

Step 3 Choose Configuration > Plug and Play > Dashboardand click PnP Profiles. Select the Plug and Play profile you want to delete, then click Delete.

Note When you delete a PnP profile with integrated APIC-EM, from the Plug and Play Dashboard, Prime Infrastructure sends a wipe command to APIC-EM to reset the device associated with the PnP profile and deletes it from the list of provisioned devices.

Related Topics

Verify Devices After They Have Been Deployed Using Plug and Play, on page 667
Use the Plug and Play Dashboard to Monitor New Device Deployments, on page 647
Create Plug and Play Profiles That Define Device Deployments, on page 651
Associate Devices with Plug and Play Profiles, on page 655
Create a Bootstrap Configuration for Plug and Play, on page 661

How to Retrieve Devices and Profiles Deleted in APIC-EM Server

allows you to retrieve the devices and profiles that were accidentally deleted or erased from the system when the APIC-EM server goes down.

To retrieve the deleted devices and profiles in Prime Infrastructure, follow these steps:

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Plug and Play Profiles.
The list of detailed summary of all plug and play profiles are displayed.

Step 2 Click the PNP APIC EM Sync button in the Plug and Play Profiles tab.
You will be prompted for a confirmation, click OK to start the sync.

Step 3 Click the Job Dashboard link in the PNP APIC-EM Sync pop-up window to view the status of the newly scheduled APIC-EM sync job.
Your job will be triggered and available in PNP APIC-EM SYNC JOB page.

Step 4 Click the i icon next to the Profile Name to view more details about the job.
Incase of the sync being successful, the status next to the Profile Instance Name will show as SUCCESS in the Synced Devices for new_apic_profile window.

If the sync is unsuccessful, the status will show as failure and the error details will be displayed in the job summary. If the device is not deleted already the status will be shown as Already Synced.

Note Only devices in PENDING status under Profiles Instances tab will be created/synced with APIC EM. The device in success or failure state, we will not be created/synchronized in APIC EM as they are already provisioned to success and PnP will not be required again.

How to Convert CNS Profile to APIC-EM Profile

CNS support for plug and play is deprecated from 3.2. You can convert all the existing CNS profiles to APIC-EM profiles.

Note You must be a Root-Domain user to perform the following operations otherwise these operations will fail:

- Convert CNS to APIC-EM
- PnP CNS to APIC-EM sync

To convert a CNS profile to an APIC-EM profile, follow these steps:

Step 1 Choose Configuration > Plug and Play > Dashboard and in the Home tab, click Plug and Play Profiles.
The list of detailed summary of all plug and play profiles are displayed.

Step 2 Click Convert CNS to APIC-EM button in the Plug and Play Profiles page.

You will be prompted for a confirmation, click OK to start the conversion.

Step 3 Click the Job Dashboard link in the Convert CNS to APIC-EM pop-up window to view the status of the newly scheduled APIC-EM conversion job.
Your job will be triggered and available in the PNP CNS TO APIC-EM SYNC JOB page.

Step 4 Click the i icon next to the Profile Name to view more details about the job.

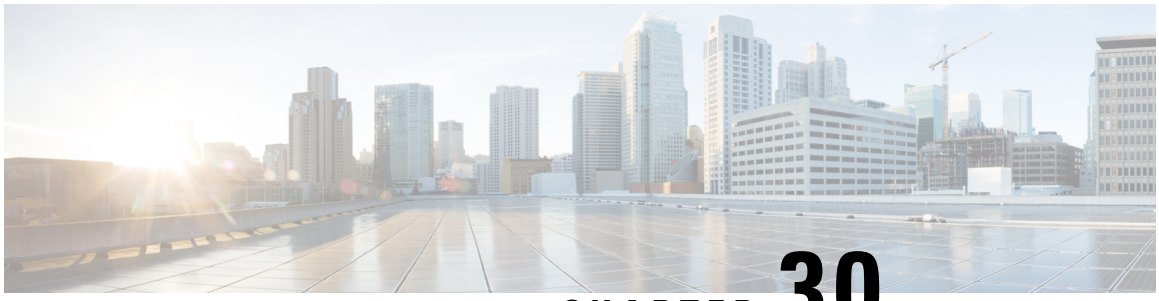
If the conversion is unsuccessful, the status will show as failure and the error details will be displayed in the job summary.

Note Only devices in PENDING status under Profiles Instances tab will be converted to APIC EM and created in APIC-EM. The device in success or failure state will not be created/synchronized in APIC EM as they are already provisioned to success state.

The CNS profiles created based on the device type will not be converted to APIC-EM profiles as APIC-EM does not support the profiles created based on the device type.

PART VI

Ensure Network Services



CHAPTER 30

Secure Network Services Using Trustsec

Overview of Cisco TrustSec

Cisco TrustSec technology uses software-defined segmentation to simplify the provisioning of security policies, to accelerate security operations, and to consistently enforce policy anywhere in the network. TrustSec is embedded technology in Cisco switches, routers, wireless, and security devices. It is a secure network architecture that extends security across the network from campus to branch to data center. TrustSec is the foundation for using the Network as an Enforcer and mitigates risk by reducing attack surface through better segmentation, whilst also increasing operational efficiency and making compliance goals easier to achieve.

In , the TrustSec network service design enables you to choose preferred options for provisioning configurations to TrustSec-capable devices to enable 802.1X and other TrustSec functionality. You can configure wired 802_1x devices by creating TrustSec model-based configuration templates and choosing any one of the following navigation paths:

- Services > TrustSec
- Configuration > Templates > Features & Technologies > Security > TrustSec > Wired 802_1x

Note For the TrustSec 5.3 platform support list, see the Cisco TrustSec Release 5.3 System Bulletin.

For more details about configuring TrustSec model-based configuration templates, see Create a New Features and Technologies Template Using an Existing Template, on page 385.

Related Topics

Generate a Trustsec Readiness Assessment Report, on page 675

Generate a Trustsec Readiness Assessment Report

TrustSec Readiness Assessment displays TrustSec-based device details such as TrustSec Feature classification.

The devices are categorized as:

- Classification is the process of assigning a security group tags based on identity or context (dynamically with 802.1x or MAB or web auth or statically mapped to IP, subnet, VLAN or interface). These security group tags are transmitted to the devices using inline tagging or security group tag exchange protocol (SXP).
- Enforcement is the process of enforcing traffic policy based on the security group tags via a secure group ACL (SGACL on switches and routers) or security group firewall (SGFW).
- TrustSec Incapable are devices with no classification, propagation or enforcement capabilities.

To generate a TrustSec Readiness Assessment report, follow these steps:

Step 1 Choose Services > TrustSec > Readiness Assessment.

Step 2 Click TrustSec Readiness tab. The TrustSec table appears with the following types of devices:

- Classification Devices
- Enforcement Devices
- TrustSec Incapable Devices

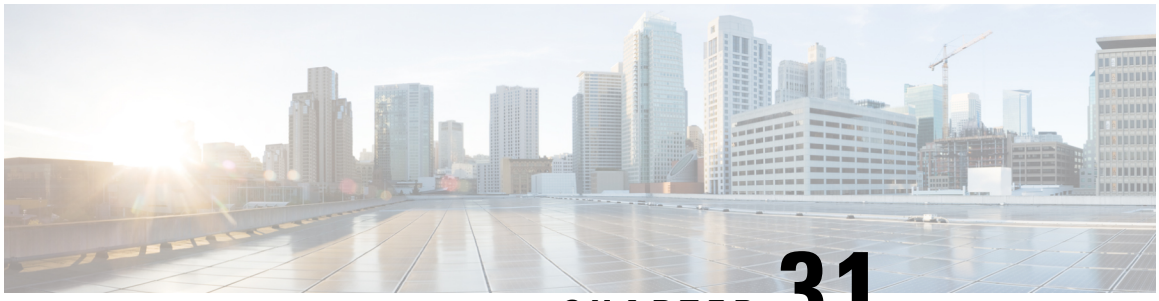
Step 3 Click the various device categories to view the details of the selected TrustSec-based device type. Each category displays the number of devices in percentage in a color coded circle. The color codes for each category are:

Classification, Enforcement and TrustSec Incapable Devices:

- Red — Number of TrustSec incapable devices.
- Light Green—Number of classification capable devices
- Dark Green—Number of enforcement capable devices.

Step 4 Choose the appropriate filter from the Show drop-down list to filter the devices in each category.

Step 5 Click the Export icon to download the device details as CSV or PDF file.



CHAPTER 31

Use IWAN to Improve Application Performance

Overview of Cisco Intelligent WAN (IWAN)

Cisco IWAN is a system that enhances collaboration and cloud application performance while reducing the operating cost of the WAN. This system leverages low-cost, high-bandwidth Internet services to increase bandwidth capacity without compromising the performance, availability, or security of cloud-based applications. Organizations can use IWAN to leverage the Internet as WAN transport, as well as for direct access to Public Cloud applications. See Cisco Intelligent WAN (IWAN) Design Guide, for more information.

positions the IWAN wizard workflow mostly for green field customers where the IWAN services need to be enabled for the first time. The enabled IWAN service cannot be modified for brown field customers. But customers can always overwrite the last-configured service by rewriting any of these services on required sites.

You can use to design, configure, and monitor the IWAN services for an enterprise. Cisco IWAN requires the configuration of DMVPN, PFR, AVC and QOS as part of enabling IWAN services on different devices.

Related Topics

Prerequisites for Enabling IWAN Services, on page 677

Configure IWAN Services Using the IWAN Wizard, on page 680

Prerequisites for Enabling IWAN Services

When designing or deploying IWAN services, configurations need to be decided. A network administrator needs to plan the branches on which the IWAN has to be enabled or reconfigured. In , you can access a set of CVD validated out of the box IWAN templates by navigating to Configuration > Templates > Features & Technologies > Feature Templates. All the templates under this Feature Templates folder are prefixed with "IWAN", and any new template that a user creates will automatically carry the IWAN prefix and will appear in the IWAN workflow.

The tags that are automatically used for the templates are as follows:

- DMVPN: IWAN-DMVPN

- PFR: IWAN-PFR
- QOS: IWAN-QOS
- AVC: IWAN-AVC
- ZBFW: DIA_ZBFW
- CWS: DIA-CWS

Note The Minimum software version required for the templates are as follows:

- IWAN-DMVPN–Cisco IOS Release 15.4 or later
- IWAN-DMVPN–Cisco IOS Release 15.4 or later
- IWAN-QOS–Cisco IOS Release 15.4 or later
- DIA-ZBFW–Cisco IOS Release 15.4 or later
- WAN-AVC– See What is AVC
- DIA-CWS
  - Cisco Validated Designs (CVD)-Cloud Web Security (CWS) Integrated Services Router-G2 platform from Cisco IOS Release 15.2(1)T1 or later
  - CVD-CWS-Integrated Services Router-4000 platform from Cisco IOS Release 15.5(3)S1 or later

The tags that are used for the IWAN Hub and IWAN Branch Categories based on the Device roles are as follows:

- Hub Category:
  - Primary Controller: IWAN-HUB-Primary-Controller
  - MPLS Hub: IWAN-HUB-MPLS
  - Internet Hub: IWAN-HUB-Internet
- Branch Category:
  - Single Router Branch: IWAN-Branch-Single-Router
  - Dual Router Branch-MPLS: IWAN-Branch-Dual-MPLS
  - Dual Router Branch-Internet: IWAN-Branch-Dual-Internet

Users can create their own templates from the bundle templates or modify the out of the box design templates, which can be recreated from the CVD templates and displayed in the IWAN workflow.

Note If you want to use a user-defined IWAN DMVPN template in the workflow, you must create a template with the following tags:

1. IWAN-DMVPN
2. Device roles tag based on the device role and category
3. DHCP or STATIC depending on whether you want the DHCP option to be enabled/disabled in the IWAN workflow
4. EIGRP or BGP depending on the overlay protocol

Therefore, enabling the complete IWAN services through is done based on two categories, SITE and ROLE. SITE can be HUB or SPOKE, and ROLE can be X, Y, Z, and so on. Depending on this selection, the templates will be organized and displayed in sequence for users to fill in the values. At the end of the workflow, the summary of the configurations to be deployed on the network is displayed. When the Deploy button is clicked, the configurations are pushed to the network.

Important Notes

- Ensure that the interface loopback 0 IP address is configured on all Primary Controllers before deployment.
- The loopback IP of the Primary Controller should be permitted in the DC-LOCAL-ROUTES prefix-list in HUB-Border-MPLS and HUB-Border-Internet routers for Border routers to reach MC.

Example:

```
ip prefix-list DC-LOCAL-ROUTES seq 40 permit <MC loopback0 ip>/32
```

- The DC_Prefix1 field in CVD-DMVPN-MPLS and CVD-DMVPN-Internet templates should match the DC subnet. If there is more than one subnet in DC, then the suffix “le 32” can be used to include all the subnets.

Example:

- - Subnet A–172.29.10.0/30
  - Subnet B–172.29.10.4/30
  - Subnet C–172.29.10.8/30
  - DC_Prefix1(x.x.x.x/x)–172.29.10.0/24 le 32
- In CVD-DMVPN, CVD-DMVPN-Dual-Internet, and CVD-DMVPN-Dual-MPLS templates, the subnet mask of the Loopback interface needs to be entered in the Loopback-Subnet field.
- %IPSEC-3-REPLAY_ERROR: IPSec SA receives an anti-replay error.

If this error message is seen on the HUB-Border-MPLS router, you may be able to resolve this by increasing the window size.

Example:

```
crypto ipsec security-association replay window-size 1024
```

Related Topics

Overview of Cisco Intelligent WAN (IWAN), on page 677
Configure IWAN Services Using the IWAN Wizard, on page 680

Configure IWAN Services Using the IWAN Wizard

provides a wizard to help you design and deploy IWAN services.

Step 1 Select Services > Network Services > IWAN Enablement.

Step 2 Click Next to choose the configuration.

Step 3 Choose the category, device role, overlay protocol and the technologies (DMVPN, PFR, QoS, AVC, DIA-ZBFW, CWS) that will be enabled through this workflow.

The CWS technologies will be enabled only for Single Router Branch and Dual Router Branch-Internet.

Step 4 (Optional) Choose the Post-IWAN template that can be used for pushing the required configuration after IWAN deployment.

Step 5 Click Next to choose the devices on which you want to configure the specified features. To configure IWAN on multiple branches at the same time, select multiple devices and enter the values for each variable.

Step 6 Click Next to choose the input option.

Step 7 Click Work Flow option, the wizard will guide you through entering the necessary values for the selected configuration.

Step 8 Alternately, click Export/Import CSV option, to update all the template properties for the selected devices using CSV export/import mechanism.

a) Uncheck the Do you want Optional Parameters check box, if you want to skip the optional fields while filling the configuration value in the CSV file.
b) Click Export CSV to download the CSV template to your local system.
c) Enter the configuration values in the downloaded CSV template.
d) Click Import CSV to upload the updated CSV file.

Step 9 After entering the necessary configuration values, click Next or click CLI Summary to confirm the device and template configuration values.

Step 10 Schedule the deployment job using Prepare and Schedule tab, if required.

Step 11 Click Next or click Confirmation tab to deploy the template.

Post deployment, ensure that you enable routing between Primary Controllers and Hub Border Routers and include the subnet of the loopback 0 interface as part of the routing domain.

Related Topics

Overview of Cisco Intelligent WAN (IWAN), on page 677
Prerequisites for Enabling IWAN Services, on page 677
Configure PKI Certificate-Based Authentication on Devices Using IWAN (APIC-EM), on page 681

Configure PKI Certificate-Based Authentication on Devices Using IWAN (APIC-EM)

To use PKI certificates (for DMVPN only) in the IWAN workflow, you must first add a valid APIC-EM controller to . See Integrate APIC-EM Policy Information into Plug and Play. The PKI option cannot be enabled if the CNS gateway is selected in the Global PnP/ZTD Settings (Administration > Servers > APIC-EM Controller > Global PnP/ZTD Settings). This is optional when you want to use a pre-shared key for IWAN DMVPN.

In the IWAN work flow, when the PKI option is enabled, in the back-end, the device is added to the APIC-EM Inventory and the PKI service is triggered to install the PKI certification on the device. The device can download the certificate in HTTP.

When the device is in the managed state, it can be used for IWAN provisioning. Here, PKI certificate-based authentication is done instead of using a pre-shared key.

Step 1 Choose Services > Network Services > IWAN Enablement.

Step 2 In the Before You Begin section, click Next.

Step 3 In the Choose Configuration section, select a category, device role from the drop-down lists. DMVPN, PFR, QOS, AVC values are auto-populated once the device role is selected. But these values can be edited. DMVPN is for PKI certificates only.

Step 4 Check the Deploy PKI check box so that the user can enable PKI certificate-based authentication for DMVPN Tunnels. Click Next.

Step 5 In the Select Devices section, select the devices and click Next.

Step 6 In the Demo_DMVPN_TEMP section, enter the values in the fields under Loopback, MPLS Tunnel and EDGRP. Click Apply and then click Next.

Step 7 In the CLI Summary section, the CLI commands in the DMVPN template are displayed along with the values that were entered by the user in the Demo_DMVPN_TEMP section. Click Next.

Step 8 In the Prepare and Schedule section, click Next if you want the job to start now and not recur. If you want the IWAN job to run at a later time in a recurring pattern, then specify the time and recurrence under Schedule. Specify the Job Option, if required.

Step 9 In the Confirmation section, click Deploy to configure the device.

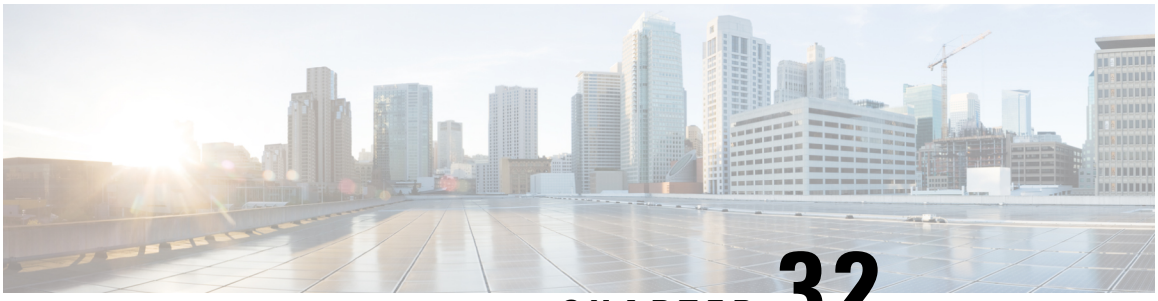
Step 10 The confirmation message appears. Click OK. The User Jobs pane under Administration / Jobs appears. The status of the IWAN DMVNP configuration and PKI certificate provisioning on the device can be tracked in the Job dashboard.

When either of the IWAN DMVPN config or PKI fail, the overall status of the IWAN provisioning will be displayed as “Failed” and the details will display whether the IWAN DMVPN configuration or the PKI failed.

For example, if there is any failure in the PKI IWAN service, an error message “Failed to install PKI certificate on device” will be displayed on the Job page of IWAN. When PKI service fails, all jobs will fail.

Related Topics

Overview of Cisco Intelligent WAN (IWAN), on page 677
Configure IWAN Services Using the IWAN Wizard, on page 680
Integrate APIC-EM Policy Information into Plug and Play, on page 650



CHAPTER 32

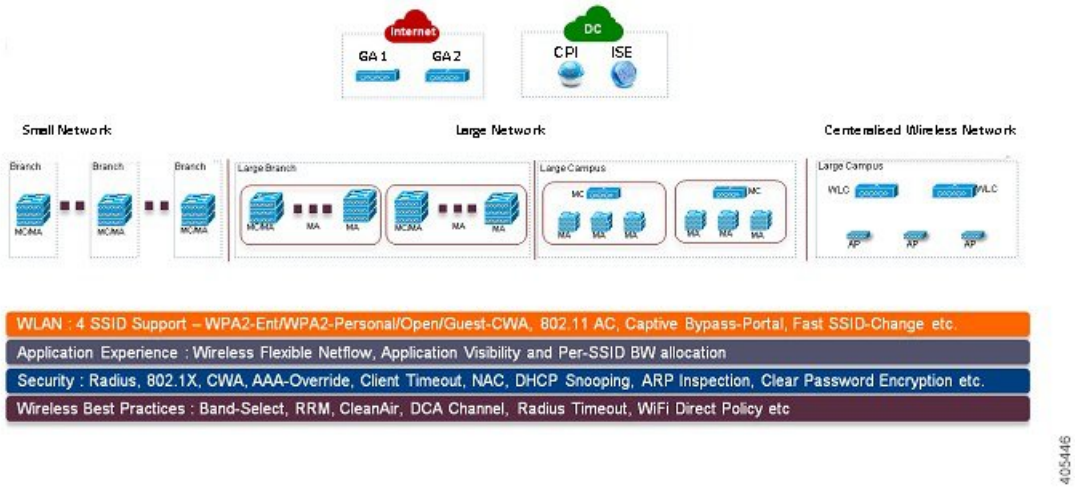
Configure Devices Using Converged Access Deployment Templates for Campus and Branch Networks

What Are Converged Access Workflows?

The Converged Access workflow simplifies, automates and optimizes deployment of various enterprise-class next generation wireless deployment models for campus and branch networks. can automate the converged access deployment of wireless networks using converged access components such as Catalyst 3650, 3850, 4500 SUP 8-E switches, and Cisco 5760 Wireless LAN controller (WLC). The catalyst switches can be deployed as Mobility Agent (MA), Mobility Controller (MC), and Guest Anchor controller (GA).

The following figure illustrates the wireless converged access deployment mode.

Figure 21: Converged Access Workflow Overview



Single-Switch Small Network Deployment Model

This deployment model assumes single Catalyst 3650, 3850 or 4500 SUP 8-E switch deployed in Access layer in combined MA and MC roles. The Catalyst switches can be deployed in individual standalone system mode or in stackwise redundant supervisor mode.

Controller-Less Single/Multi-Domain Deployment Model

This deployment model consists of multiple sub-domains and allows inter-domain MC peering for end-to-end seamless roaming across sub-domains. The MA switches are deployed in Access layer while the MC switches can be placed in Distribution layer.

Controller-Based Single/Multi-Domain Deployment Model

A large scale converged access campus building is deployed with external 5760 WLC as MC. The Access layer switches are deployed as MA across multiple buildings with centralized 5760 MC. In such large network, multiple 5760 WLCs may co-exist for better load balancing and redundancy. Depending on the roaming requirement across different buildings, the inter-domain mobility peering between 5760 WLCs can be established.

Centralized Wireless Campus Deployment Model

In this deployment model, the switches in Access layer remain in traditional switching mode and wireless communication between Access Point (AP) and WLC is built as overlay network. In large scale campus deployments, multiple 5760 WLCs can be deployed for better load balancing and redundancy. To provide seamless large mobility domains, the inter-domain mobility peering 5760 WLCs can be established.

Key Benefits

- Simple Automated Deployment—Simplifies the converged access deployment by automating the device configuration process. Requires only a few deployment specific inputs from the network administrator and pushes the complete converged access configurations to the network devices.

- Error Free Deployment—The template-based configuration used by avoids manual misconfigurations, making it easier to build/maintain enterprise-wide standardized configurations that are well understood by the network administrator.
- Optimized Deployment—The configuration templates used by incorporates a large number of Cisco best practice guidelines, improving the deployment quality. Some of the best practice wireless technologies/features that are automatically included in the template are Band-Select, Radio Resource Management (RRM), Fast SSID-Change, CleanAir, and Wireless QoS.
- High Scalability—Supports large enterprises with thousands of branches. It not only reduces efforts to deploy greenfield branches, but also simplifies large scale conversion of traditional Ethernet based branch networks to converged access branches in an error-free way.

Related Topics

Supported Cisco IOS-XE Platforms, on page 685
Prerequisites for Converged Access Deployment, on page 686
Configure Devices Using Converged Access Templates, on page 690
Field Reference: Converged Access Templates, on page 692
Example: Controller-Less Single-Switch Network, on page 695
Example: Controller-Less Single/Multi-Domain Wireless Network, on page 700
Example: Controller-Based Single/Multi-Domain Wireless Network, on page 701
Example: Centralized Wireless Campus, on page 703

Supported Cisco IOS-XE Platforms

The following tables describe the supported Cisco IOS-XE platforms for small, large, and centralized network deployment models.

Table 53: Supported Cisco IOS-XE for Small Network Deployment Mode

Device Role	Cisco IOS-XE Platform	System Mode	Software Version
Mobility Agent/Mobility Controller (Single-Switch)	Catalyst 3650	Single or StackWise	3.6.0 and later
	Catalyst 3850	Single or StackWise	3.6.0 and later
	Catalyst 4500 SUP 8-E	Single or Dual-SUP	3.7.0 and later
Guest Anchor WLC	CT5760 WLC	Single or StackWise	3.6.0 and later

Table 54: Supported Cisco IOS-XE for Large Network Deployment Model

Device Role	Cisco IOS-XE Platform	System Mode	Software Version
Mobility Agent	Catalyst 3650	Single or StackWise	3.6.0 and later
	Catalyst 3850	Single or StackWise	3.6.0 and later
	Catalyst 4500 SUP 8-E	Single or Dual-SUP	3.7.0 and later

Device Role	Cisco IOS-XE Platform	System Mode	Software Version
Mobility Controller	Catalyst 3650	Single or StackWise	3.6.0 and later
	Catalyst 3850	Single or StackWise	3.6.0 and later
	Catalyst 4500 SUP 8-E	Single or Dual-SUP	3.7.0 and later
	CT5760 WLC	Single or StackWise	3.6.0 and later
Guest Anchor Controller	CT5760 WLC	Single or StackWise	3.6.0 and later

Table 55: Supported Cisco IOS-XE for Centralized Wireless Deployment Mode

Device Role	Cisco IOS-XE Platform	System Mode	Software Version
Mobility Controller	CT5760 WLC	Single or StackWise	3.6.0 and later
Guest Anchor WLC	CT5760 WLC	Single or StackWise	3.6.0 and later

Related Topics

What Are Converged Access Workflows?, on page 683
Prerequisites for Converged Access Deployment, on page 686
Configure Devices Using Converged Access Templates, on page 690
Field Reference: Converged Access Templates, on page 692
Example: Controller-Less Single-Switch Network, on page 695
Example: Controller-Less Single/Multi-Domain Wireless Network, on page 700
Example: Controller-Based Single/Multi-Domain Wireless Network, on page 701
Example: Centralized Wireless Campus, on page 703

Prerequisites for Converged Access Deployment

To successfully deploy the Converged Access solution using the Converged Access Workflow, the wired infrastructure of the network should be set for further configuration required for converged access. This section describes the prerequisite configurations for Converged Access Workflow based deployment.

You can view the prerequisites using the click here link in the Before you Begin page in the Converged Access Workflow (Services > Network Services > Converged Access).

Related Topics

Prerequisites for Layer 2 and Layer 3, on page 686
Prerequisites for Server Configuration, on page 690

Prerequisites for Layer 2 and Layer 3

The following table describes the Layer 2 and Layer 3 prerequisites, and sample configuration for the Converged Access Workflow. In the sample configuration, the following nomenclature is used to represent the various wireless management VLANs in the MA and MC.

- WM_VLAN - Name of the Wireless Management VLAN

- WM_VLAN_id - ID of the Wireless Management VLAN
- WLAN1_Client_VLAN_Name - VLAN name of WLAN 1
- WLAN2_Client_VLAN_Name - VLAN name of WLAN 2
- WLAN3_Client_VLAN_Name - VLAN name of WLAN 3
- WLAN1_Client_VLAN_id - VLAN ID of WLAN 1
- WLAN2_Client_VLAN_id - VLAN ID of WLAN 2
- WLAN3_Client_VLAN_id - VLAN ID of WLAN 3

Note WLANx_Client_VLAN_id represents all the three client VLAN Ids.

Table 56: Layer 2 and Layer 3 Prerequisites for Converged Access Switches for Device Roles MA and MC

Task on Converged Access Switch	Sample Configuration
Wireless Management VLAN • Create wireless management VLAN with a network wide unique name. • Configure access ports connected to APs under this VLAN.	! Mgmt VLAN on Access Switch vlan <WM_VLAN_id> name <WM_VLAN> ! Apply VLAN to access ports connected to Access Points interface GigabitEthernet 1/0/x description Connected to Access-Points switchport mode access switchport access vlan <WM_VLAN_id>
Create Wireless Client VLANs • Create wireless client VLANs in VLAN database. The VLAN names are common across campus and branches.	! Create the wireless Client VLANs on Access Switch vlan <WLAN1_Client_VLAN_id> name <WLAN1_Client_VLAN_Name> vlan <WLAN2_Client_VLAN_id> name <WLAN2_Client_VLAN_Name> vlan <WLAN3_Client_VLAN_id> name <WLAN3_Client_VLAN_Name>
DHCP Snooping /ARP Inspection • Enable DHCP snooping and ARP inspection on each WLAN client VLANs in the access switch (for static or dynamic VLAN). • Configure upstream Layer 2 trunk as trusted for ARP inspection and DHCP snooping.	! Enable DHCP Snooping & ARP Inspection on all WLAN ! Client VLANs (Static or Dynamic) ip dhcp snooping ip dhcp snooping vlan name <WLANx_Client_VLAN_id> no ip dhcp snooping information option ip arp inspection vlan <WLANx_Client_VLAN_id> ip arp inspection validate source destination allow-zeros interface Port-Channel <id> description L2 Trunk to Upstream Router/Switch ip dhcp snooping trust ip arp inspection trust

Task on Converged Access Switch	Sample Configuration
Switch Trunk Ports • Configure trunk ports to the WAN router(s). The trunk must allow WM_VLAN and the Client VLANs, and must be a trusted port for DHCP snooping or ARP inspection. • Ensure that the other ends of the trunk ports are properly configured (not shown).	! Configure trunk port to other connected switches/router interface Port-channel1 description Connected to Upstream System switchport trunk allowed vlan add <WM_VLAN_id>, <WLAN1_Client_VLAN_id>,<WLAN2_Client_VLAN_id>, <WLAN3_Client_VLAN_id>, ip arp inspection trust ip dhcp snooping trust
Default Gateway • Ensure that default gateway is configured.	! Configure default-gateway <*ip default-gateway* >
Wireless Mobility Controller • If you want Catalyst 3650, 3850, and 4500 SUP 8-E switches to be deployed as MC then configure the switches as MC, and reload them to make the configuration effective.	wireless mobility controller write memory reload
AP Licenses • MC must have sufficient AP licenses to support all APs in its sub-domain, and activate the licenses on the APs. The activation does not require a reboot. • The GA does not require AP license.	! Activate AP license on branch converged access switch license right-to-use activate ap-count <count> slot <ID> acceptEULA
Security • Convert relevant authentication commands on the access switches to their Class-Based Policy Language (CPL) equivalents.	authentication convert-to new-style This command permanently converts the legacy configuration on the switch to identity-based networking services. On entering this command, a message is displayed for your permission to continue. Permit the conversion.

Task on Converged Access Switch	Sample Configuration

Update AP Interface Template
• Add wireless management VLAN to the AP interface template LAP_INTERFACE_TEMPLATE.
• Apply the updated template to each switch port connected to an AP.
• Verify that the VLANs are applied using the following command:
`show derived-config interface <interface id>`
This step is not necessary if autoconf enable command is globally configured. In this case, the switch automatically detects the device types of the connected devices, and applies appropriate interface templates.
	`template LAP_INTERFACE_TEMPLATE`
	`switchport access vlan <Wireless_Mgmt_VLAN_id>`
	`! Associate the LAP_INTERFACE_TEMPLATE to switch`
	`! ports connected to APs. This puts the interface`
	`! in shutdown state; so issue a "no shut" command`
	`interface Gig 1/0/x`
	`source template LAP_INTERFACE_TEMPLATE`
	`no shutdown`

The following describes the Layer 2 and Layer 3 prerequisites, and sample configuration for GA. In the sample configuration, the following nomenclature is used to represent the wireless management VLAN and Guest VLAN details for GA:

- WM_VLAN - Name of the Wireless Management VLAN
- WM_VLAN_id - ID of the Wireless Management VLAN
- GUEST_VLAN_Name - VLAN name of Guest Anchor Controller
- GUEST_VLAN_id - VLAN ID of Guest Anchor Controller

Table 57: Layer 2 and Layer 3 Prerequisites for Guest Anchor Controller

Task on Guest Anchor Controller	Sample Configuration for Guest Access Controller

Wireless Management VLAN
• Create wireless management VLAN with a network wide unique name.
	`! Mgmt VLAN on Access Switch`
	`vlan <WM_VLAN_id>`
	`name <WM_VLAN>`

Create Wireless Guest VLAN
• Create wireless Guest VLANs in VLAN database. The VLAN name must be common across all GAs.
	`! Create the wireless guest VLANS on Access Switch`
	`vlan <GUEST_VLAN_id>`
	`name <GUEST_VLAN_Name>`

DHCP Snooping / ARP Inspection
• Enable DHCP snooping and ARP inspection on the Guest VLAN.
• Configure Layer 2 trunk connected to the network as trusted for ARP inspection and DHCP snooping.
	`! Enable DHCP Snooping & ARP Inspection on Guest`
	`! VLAN`
	`ip dhcp snooping`
	`ip dhcp snooping vlan name <GUEST_VLAN_Name>`
	`no ip dhcp snooping information option`
	`ip arp inspection vlan <GUEST_VLAN_id>`
	`ip arp inspection validate source destination allow-zeros`
	`interface Port-Channel <id>`
	`description L2 Trunk to network`
	`ip dhcp snooping trust`
	`ip arp inspection trust`

Task on Guest Anchor Controller	Sample Configuration for Guest Access Controller
Default Gateway • Ensure that default gateway is configured.	`ip default-gateway <ip address>`
Security • Convert relevant authentication commands on the access switches to their Class-Based Policy Language (CPL) equivalents.	`authentication convert-to new-style` This command permanently converts the legacy configuration on the switch to identity-based networking services. On entering this command, a message is displayed for your permission to continue. Permit the conversion.

Related Topics

Prerequisites for Converged Access Deployment, on page 686
Prerequisites for Server Configuration, on page 690

Prerequisites for Server Configuration

- • All network-wide catalyst switches and 5760 WLCs must be configured with SNMP.
  • The Converged Access switches must be added to the inventory of . You need to provide SNMP and Telnet credentials to add the devices to the inventory.
  • Link with Cisco ISE engine as external server to centrally monitor end-to-end client connectivity and policy enforcement details.
- Cisco ISE/ACS
  - All network devices including catalyst switches and Guest Anchor WLC must be configured in Cisco ISE/ACS to enable centralized policy engine function.
  - AAA configuration is not required for converged access on individual network devices as it is automatically generated by Converged Access Workflow.
- DHCP Server—Internal or external DHCP server must be preconfigured with appropriate pool settings for wireless clients.
- DNS Server—Must be preconfigured with appropriate name-lookup process to successfully connect to the network.

Related Topics

Prerequisites for Converged Access Deployment, on page 686
Prerequisites for Layer 2 and Layer 3, on page 686

Configure Devices Using Converged Access Templates

uses different templates for different deployment models. You need to select the appropriate template-based on your network topology as explained in the following table:

Network Topology	Configuration Template
Single-switch small network	IOS-XE Controller - Small Network
Controller-less single/multi-domain branch	IOS-XE Controller - Large Network

Network Topology	Configuration Template
Controller-based single/multi-domain branch	IOS-XE Controller - Large Network
Centralized wireless campus	IOS-XE Centralized Wireless Network

To deploy a converged access template:

Step 1 Choose Services > Converged Access.

Step 2 Click Next to choose the deployment model.

Step 3 From the Select Deployment Model drop-down list, choose any one of the following options:

- IOS-XE Controller - Small Network
- IOS-XE Controller - Large Network
- IOS-XE Centralized Wireless Network

Step 4 Click Next to choose the devices to be deployed.

Step 5 Choose the devices and click Next to apply the selected network configuration.

The selected device will be listed out in the left pane, and in the right pane you can configure the templates by entering the values for the Wireless Management, WLANs, Guest WLAN, Mobility, Security, Application Visibility and Control (AVC), and Quality of Services (QoS).

Step 6 Choose the devices individually and enter the Wireless Management configuration values.

Step 7 Click Apply and then Next.

Step 8 Enter the WLANs configuration values that are common to all the selected devices.

By default, the All Selected Devices check box is enabled. You can enter the WLAN configuration values for all the devices at the same time.

Step 9 Click Applyand then Next.

Step 10 (Optional) Enter the Radio configuration values that are common to all the selected devices. By default, the All Selected Devices check box is enabled.

Step 11 Click Applyand then Next.

Step 12 (Optional) Enter the Guest WLAN configuration values that are common to all the selected devices.

By default, the All Selected Devices check box is enabled.

Step 13 Click Apply.

Step 14 Choose the devices individually and enter the Guest Controller configuration values.

Step 15 Click Apply and then Next.

Step 16 Select the individual devices and enter the Mobility configuration values. The Mobility configuration fields will be available in the Converged Access Wizard only for large and centralized network deployments.

Step 17 Click Applyand then Next.

Step 18 (Optional) Enter the Security configuration values that are common to all the selected devices. By default, the All Selected Devices check box is enabled.

Step 19 Click Apply and then Next.

Step 20 (Optional) Enter the AVC and QoS configuration values that are common to all the selected devices. By default, the All Selected Devices check box is enabled.

Step 21 Click Apply and then Next to view the confirmation screen.

The confirmation screen allows you to view the device configuration information before deployment.

Step 22 (Optional) Enter the job name and click the Date radio button to schedule the deployment job.

Step 23 Click Deploy.

Related Topics

Prerequisites for Converged Access Deployment, on page 686
Field Reference: Converged Access Templates, on page 692
Example: Controller-Less Single-Switch Network, on page 695
Example: Controller-Less Single/Multi-Domain Wireless Network, on page 700
Example: Controller-Based Single/Multi-Domain Wireless Network, on page 701
Example: Centralized Wireless Campus, on page 703

Guidelines for Entering Configuration Values

This section provides the field descriptions for converged access template and guidelines for entering the global and local configuration values for the following deployment models with specific examples.

- Controller-less single-switch deployment model
- Controller-less single/multi-domain deployment model
- Controller-based single/multi-domain deployment model
- Centralized wireless campus deployment model

Field Reference: Converged Access Templates

This section contains the field descriptions for converged access template.

Table 58: Wireless Management Field Descriptions

Field Name	Description
VLAN ID	VLAN ID of the selected device.
IP Address	Wireless management IP of the selected device.
Subnet mask	Subnet mask allocated to the selected device.

Table 59: WLAN Field Descriptions

Field	Description
SSID	Name of the wireless LAN.
ID	Wireless LAN ID. If SSID > 16, you need to manually enter the AP group name.

Field	Description
Security	Allows you to customize the login window for configuring an external web server such as ISE. The following security options are available for WLAN: • WPA2-Enterprise • WPA2-Personal • OPEN For Guest WLAN, WebAuth (external) option alone is available.
Pre-Shred Key	This is a mandatory field, if you have a selected WPA2-Personal.The value must be alphanumeric and at least eight characters long.
Client VLAN Name	Name of the client VLAN. Can be alphanumeric.
AP Group	AP Group name is used to assign group name for the APs associated with WLAN and Client VLAN.
DHCP Required	This is an optional field. Check the DHCP Required check box for WLAN. This forces the wireless clients to use DHCP to get IP addresses. Clients with static address cannot access the network.
Radio	Radio bands used by WLAN.
Device Classification	You can turn on/off the device classification on the switch, using OUI and DHCP.
Device Profiling	You can turn on/off the device profiling. The following two options are available for device profiling: • Local profiling based on HTTP attributes • Radius profiling based on HTTP attributes
Client Exclusion	Turns on/off the client exclusion for the WLAN. When it is turned on, the misbehaving clients are added in an exclusion list so that they cannot access the network until the timeout is over. Clients may be added in the exclusion list due to excessive authentication attempts and using IP address of another client.
Client Exclusion Timeout (sec)	The timeout period for excluded clients.
Session Timeout (sec)	The timeout period for a client session. The client is re-authenticated before this period is over.

Table 60: Wireless Radio Field Descriptions

Field	Description
RF Group Name	Name of the RF group. Multiple MCs can be placed under a single RF group, to perform RRM in a globally optimized manner and perform network calculations on a per-radio basis.
Radio 2 GHz	This is an optional check box.
Radio 5 GHz	This check box is checked by default and it’s mandatory. You cannot uncheck this check box.
Disable Rates	These data rates are disabled. Clients cannot use these data rates to connect to access points.
Mandatory Rates	Clients must support these data rates in order to associate to an access point, although it may connect to the AP using one of the supported data rates.

Field	Description
Supported Rates	Clients that support this data rate may communicate with the access using the supported date rate. However, clients are not required to use this data rate in order to associate with the AP.
Country Code	Country code enables you to specify a particular country of operation. Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulation.

Table 61: Guest Services Field Descriptions

Field	Description
Anchor Controller IP	Wireless management IP of Guest Anchor device.
Anchor Group Name	Group name of Anchor device.
Foreign Controller	Wireless management IP of MC to which the Guest Anchor device is associated.

Table 62: Security Field Descriptions

Field	Description
Radius Server (IPs)	IP address of the Remote Authentication Dial In User Service (RADIUS) server.
Key	Password of Radius server.
Device HTTP TACACS Authentication	Select this in order to enable TACACS based device authentication to access the converged access device.
TACACS+ Server IP(s)	IP address of the TACACS server.
Key	Password of the TACACS server.

Table 63: Application Services Field Descriptions

Field Name	Description
Netflow Collectors (IP:Port)	IP—The IP address of the server. Port—The port on which the NetFlow monitor will receive the exported data. For the default port is 9991. Example: 172.20.114.251:9991
WLAN-1 SSID Bandwidth(%)	Specify the maximum bandwidth percentage allowed for first WLAN.
WLAN-2 SSID Bandwidth(%)	Specify the maximum bandwidth percentage allowed for second WLAN.
WLAN-3 SSID Bandwidth(%)	Specify the maximum bandwidth percentage allowed for third WLAN.
Guest SSID Bandwidth(%)	Specify the maximum bandwidth percentage allowed for Guest WLAN.

Table 64: Wireless Mobility Field Descriptions

Field Name	Description
Role	Mobility Controller or Mobility Agent.
Controller IP	Wireless Management IP of Controller device.
Switch Peer Group Name	Peer group name in which the Agent is added.
Mobility Agent IP(s)	Wireless management IP of Mobility Agent devices. If you are entering more than one IP addresses, use semicolon to separate the IP addresses.
Peer Controller IP(s)	Wireless Management IP of peer controller device. If you are entering more than one IP addresses, use semicolon to separate the IP addresses.

Related Topics

Prerequisites for Converged Access Deployment, on page 686
Configure Devices Using Converged Access Templates, on page 690
Example: Controller-Less Single-Switch Network, on page 695
Example: Controller-Less Single/Multi-Domain Wireless Network, on page 700
Example: Controller-Based Single/Multi-Domain Wireless Network, on page 701
Example: Centralized Wireless Campus, on page 703

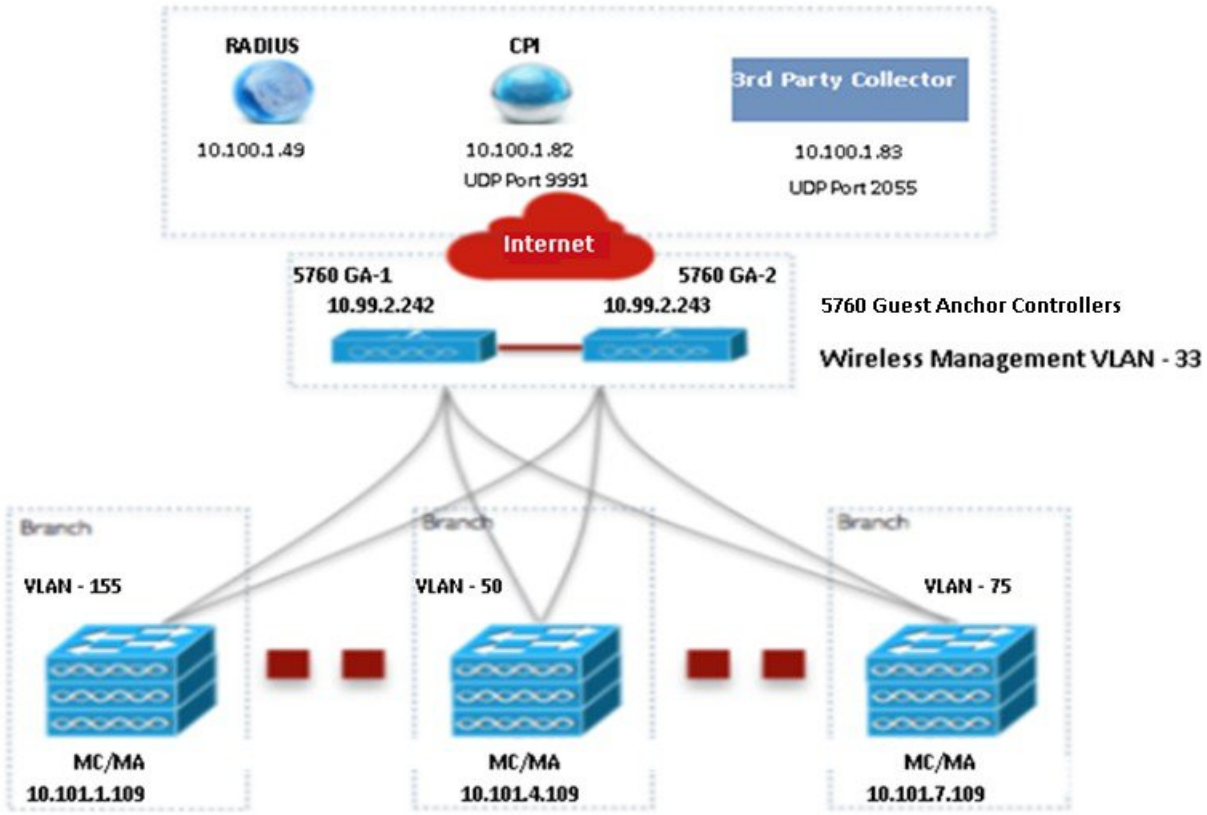
Example: Controller-Less Single-Switch Network

A small-sized remote branch office or retail store may consists of a single converged access switch (standalone or stack) to provide network connectivity to the wired and wireless users.

For such network designs, the switch integrates both MC and MA functions. These networks may need guest wireless services, as well as common security and network access policy enforcement across all deployed sites.

The network administrator can use IOS-XE Controller Small Network template to deploy converged access. The following figure 405448 illustrates the reference network for single-switch small network that shows three branch offices. Each site can be independently deployed using the workflow. Alternatively, one deployment workflow can deploy multiple sites. allows you to configure the devices in five WLANs. The following figure illustrates three WLAN configuration scenario in the single-switch small network topology.

Figure 22: Controller-less Single-switch Small Network Model



	SSID	Security	Client VLAN Name	Guest VLAN Name
WLAN 1	ABCCorp_802.1X	WPA2-Enterprise	8021x-WiFi_VLAN	
WLAN 2	ABCCorp_PSK	WPA2-Personal	PSK-WiFi_VLAN	
WLAN 3	ABCCorp-OPEN	OPEN	OPEN_WiFi-VLAN	
Guest WLAN	ABCCorp_Guest	WebAuth-External		Guest_WiFi-VLAN

You must enter the Wireless Management configuration values separately for each device. The following tablw describes the Wireless Management configuration values for MA/MC (10.100.1.109) and Guest Anchor (10.99.2.242) in the single-switch small network topology shown in above figure.

Table 65: Sample Wireless Management Configuration Values for MA/MC (10.100.1.109) and GA (10.99.2.242)

Data Field	MA/MC	GA
VLAN ID	155	33
IP	10.101.1.109	10.99.2.242
Subnet Mask	255.255.255.240	255.255.255.240

After applying the Wireless Management configuration values, you must enter at least one WLAN configuration values. The following table describes sample configuration of three WLANs for the single-switch small network topology shown in the above figure.

Table 66: Sample WLAN Configuration Values for MC/MA and GA

Data Field	WLAN 1	WLAN 2	WLAN 3
SSID	ABCCorp_802.1x	ABCCorp_PSK	ABCCorp_OPEN
ID	1	2	3
Security	WPA2-Enterprise	WPA2-Personal	OPEN
Pre-Shared Key	—	CISCO123	—
Client VLAN Name	8021X-WiFi_VLAN	PSK-WiFi_VLAN	OPEN_WiFi_VLAN
AP Group	Ap-group-1		Ap-group-HR
DHCP			Yes (Check the DHCP check box)
Radio	All	802.11g	802.11a/g
Device Classification		Yes (Check the Device Classification check box)	
Device Profiling	None	Local	Both
Client Exclusion	Yes (check the Client Exclusion check box)	Yes (check the Client Exclusion check box)	Yes (check the Client Exclusion check box)
Timeout (sec)	60	100	100
Session Timeout (sec)	1800	2000	300

After applying the WLAN configuration values, enter the Wireless Radio configuration values for all the devices at the same time. The following table shows the Wireless Radio configuration values for MC/MA and GA in the single-switch small network topology shown in the above figure.

Table 67: Sample Wireless Radio Configuration Values for MC/MA and GA

Data Field	Sample Configuration Value
RF Group Name	CA-RF
Radio 5 GHz	Yes (This check box is checked by default and it's mandatory. You cannot uncheck this check box.)
Disable Rates	RATE_6M;RATE_18M; RATE_54M
Mandatory Rates	RATE_6M;RATE_18M; RATE_54M
Supported Rates	RATE_6M;RATE_18M; RATE_54M
Radio 2 GHz	No (This is an optional check box)

Data Field	Sample Configuration Value
Disable Rates	—
Mandatory Rates	—
Supported Rates	—
Country Code	UNITED STATES

After applying the Wireless Radio configuration values, enter the Guest Services configuration values for all the devices at the same time. The following table describes the Guest WLAN configuration values for all the devices in the single-switch small network topology shown in the above figure.

Table 68: Sample Guest WLAN Configuration Values for MC/MA and GA

Data Field	Sample Configuration Values
SSID	ABCCorp_Guest
ID	15
Security	WebAuth-External
Pre-Shared Key	—
Client VLAN Name	Guest_WiFi_VLAN
AP Group	AP-group-guest
DHCP	yes (check the DHCP check box)
Radio	802.11a (or 802.11a/g, 802.11b/g, 802.11g, or All)
Device Classification	Yes (check the Device Classification check box)
Device Profiling	Both
Client Exclusion	ON
Timeout (sec)	100
Session Timeout (sec)	5000

The following table describes the sample Guest Controller configuration values for MC/MA (10.100.1.109) and GA in the single-switch small network topology shown in the above figure.

Table 69: Sample Guest Controller Configuration Values for MC/MA (10.100.1.109) and GA

Data Field	MC/MA	GA
Anchor Controller IP	10.99.2.242; 10.99.2.243	10.99.2.242; 10.99.2.243
Anchor Group Name	CA-Mobility-SubDomain-3	CA-Mobility-SubDomain-3

Data Field	MC/MA	GA
Foreign Controllers	10.101.4.109	10.101.1. 109; 10.101.4.109; 10.101.7.109

After applying the Guest Services configuration values, enter the Security configuration values for all the devices at the same time. The following table describes the sample Security configuration values for MC/MA and GA in the single-switch small network topology shown in the above figure.

Table 70: Sample Security Configuration values for MC/MA and GA

Data Field	Sample Configuration Values
Radius Server (IPs)	10.100.1.49
Key	CISCO
Device HTTP TACACS Authentication	Yes (check the Device HTTP TACACS Authentication check box)
TACACS+ Server IP(s)	10.100.1.51
Key	cisco

After applying the Security configurations values, enter the AVC and QoS configuration values for all the devices. The following table describes the sample configuration values for MC/MA and GA in the single-switch small network topology shown in the above figure.

Table 71: Sample AVC and QoS Configuration Values for MC/MA and GA

Data Field	Sample Configuration Values
Netflow Collectors (IP:Port)	10.100.1.02:9991; 10.100.1.03:2055
WLAN-1 SSID Bandwidth(%)	40
WLAN-2 SSID Bandwidth(%)	30
WLAN-3 SSID Bandwidth(%)	20
Guest SSID Bandwidth(%)	10

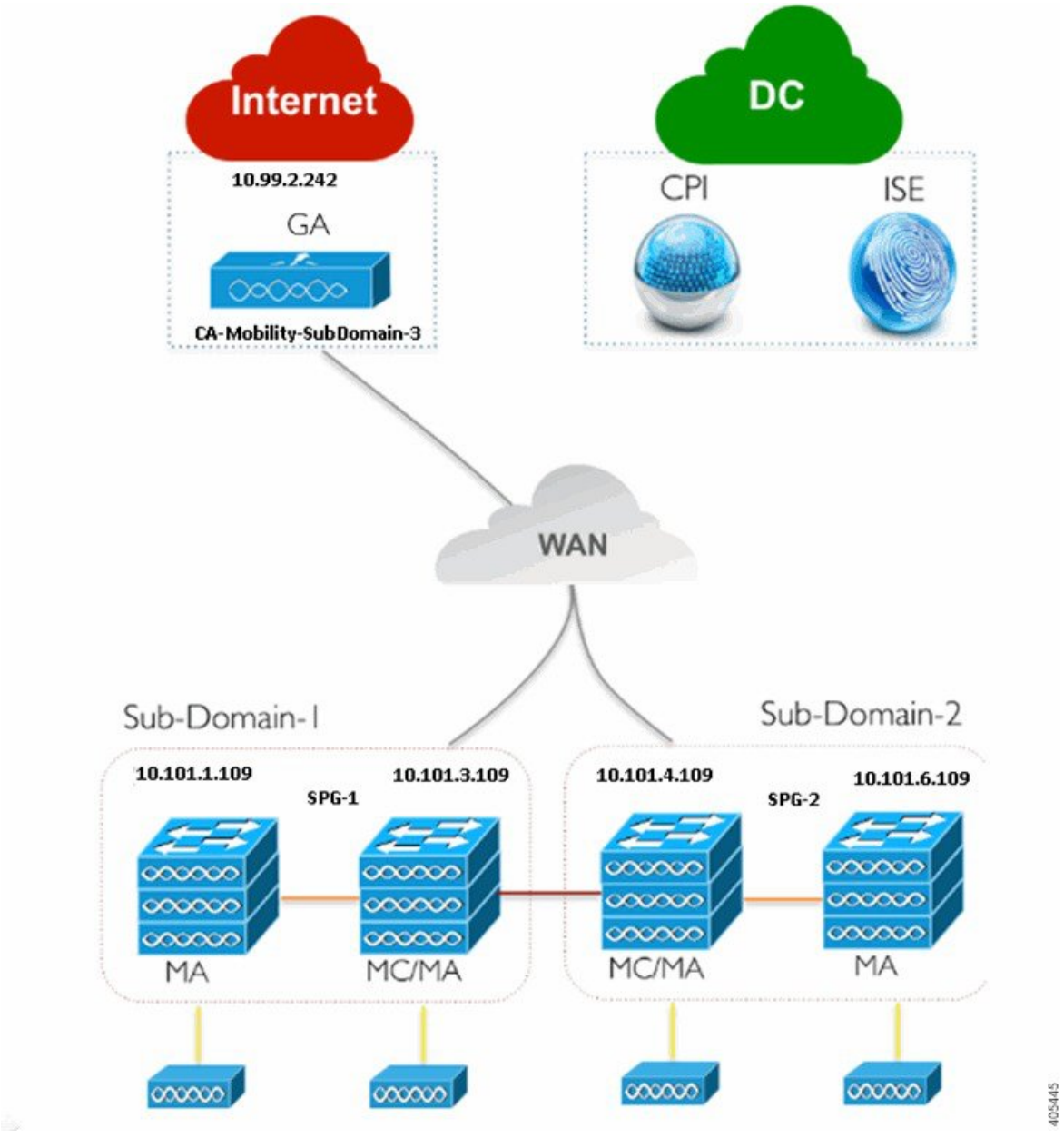
Related Topics

Prerequisites for Converged Access Deployment, on page 686
Configure Devices Using Converged Access Templates, on page 690
Field Reference: Converged Access Templates, on page 692
Example: Controller-Less Single/Multi-Domain Wireless Network, on page 700
Example: Controller-Based Single/Multi-Domain Wireless Network, on page 701
Example: Centralized Wireless Campus, on page 703

Example: Controller-Less Single/Multi-Domain Wireless Network

The following figure illustrates the controller-less deployment model that leverages Catalyst switches for MA and MC roles without depending on an external WLC. This converged access deployment model is suitable for large branches and campus, and can be implemented using IOS-XE Controller Large Network template.

Figure 23: Controller-Less Large Branch Network Model



Enter the Wireless Management, WLANs, Wireless Radio, and Guest WLAN configuration values for all the devices as described in single-switch small network deployment model. Enter the Guest Controller configuration values and Mobility configuration values for MA, MC, and GA for the topology shown in the above figure.

Table 72: Sample Guest Controller Configuration Values for MA, MC, and GA

Data Field	MA	MC	GA
Anchor Controller IP	10.99.2.242	10.99.2.242	10.99.2.242
Anchor Group Name	CA-Mobility-SubDomain-3	CA-Mobility-SubDomain-3	CA-Mobility-SubDomain-3
Foreign Controller	10.101.4.109	10.101.3.109	10.101.3.109

The following table describes the Mobility configuration values for MA, MC in SPG-1, and GA shown in the above figure.

Table 73: Sample Mobility Configuration Values for MA, MC, and GA

Data Field	MA	MC	GA
Role	Agent	Controller	Controller
Controller IP	10.101.3.109	10.101.3.109	—
Switch Peer Group Name	SPG-1	SPG-1	—
Mobility Agent IP(s)	—	10.101.1.109	—
Peer Controller IP(s)	—	10.101.4.109	—

Repeat the same procedure for MA and MC in SPG-2 as shown in the above figure.

After applying the Mobility configuration values, enter the Security, AVC and QoS configuration values as described in single-switch small network deployment model.

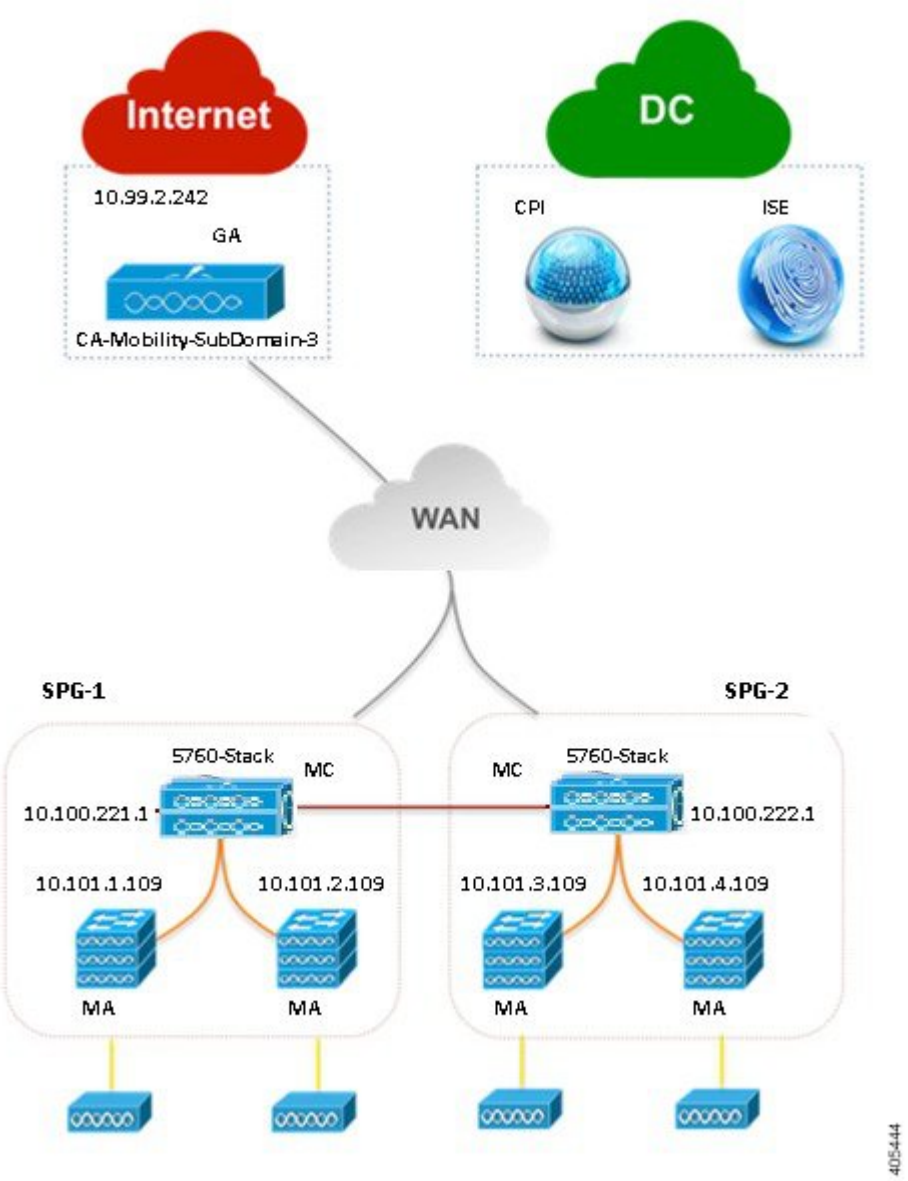
Related Topics

Prerequisites for Converged Access Deployment, on page 686
Configure Devices Using Converged Access Templates, on page 690
Field Reference: Converged Access Templates, on page 692
Example: Controller-Less Single-Switch Network, on page 695
Example: Controller-Based Single/Multi-Domain Wireless Network, on page 701
Example: Centralized Wireless Campus, on page 703

Example: Controller-Based Single/Multi-Domain Wireless Network

The following figure illustrates the controller-based single/multi-domain deployment model that leverages the same IOS-XE Controller Large Network template for deploying converged access with an external 5760 WLC as the MC.

Figure 24: Controller-Based Large Campus Model



Enter the configuration values as explained in controller-less single/multi-domain wireless deployment model.

Related Topics

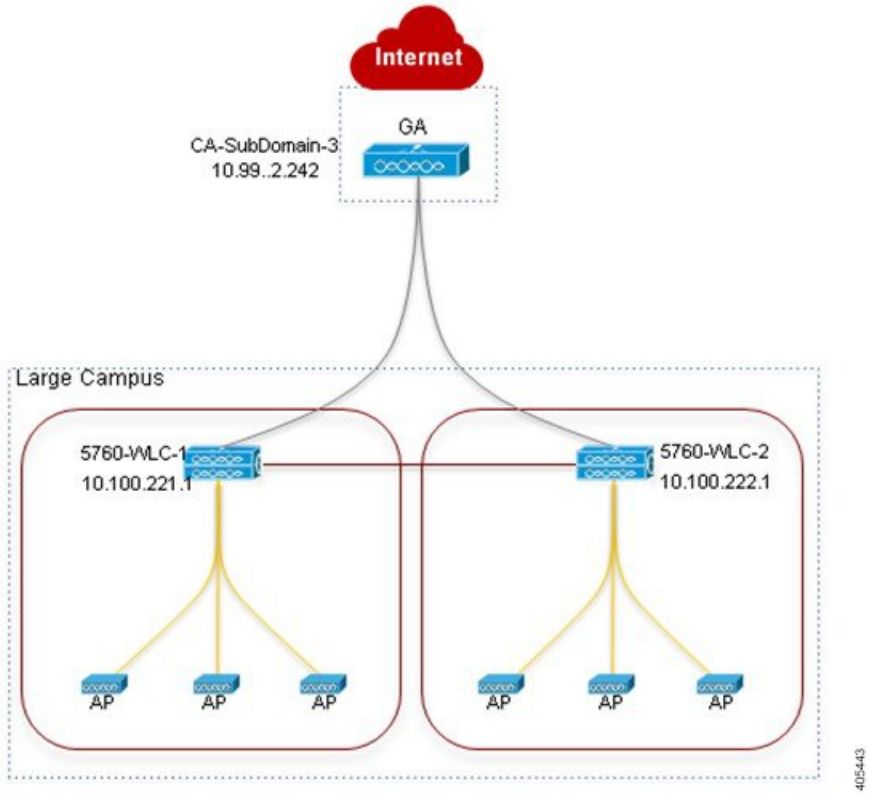
Prerequisites for Converged Access Deployment, on page 686
Configure Devices Using Converged Access Templates, on page 690
Field Reference: Converged Access Templates, on page 692
Example: Controller-Less Single-Switch Network, on page 695
Example: Controller-Less Single/Multi-Domain Wireless Network, on page 700
Example: Centralized Wireless Campus, on page 703

Example: Centralized Wireless Campus

IOS-XE Centralized Wireless template supports traditional wireless deployment model using next-generation 5760-WLC. In this model, any generation Access layer switches are deployed in traditional Ethernet switch mode over which WLC and the APs build an overlay network using CAPWAP Tunneling mechanism.

The following figure illustrates 5760-WLC based Centralized Wireless deployment using IOS-XE Centralized template.

Figure 25: Centralized Campus Network Model



Enter the Wireless Management, WLANs, Wireless Radio, and Guest WLAN configuration values for all the devices as described in single-switch small network deployment model. Enter the Guest Controller configuration values and Mobility configuration values for 5760 WLC in SPG-1 and GA for the topology shown in the above figure.

Table 74: Sample Guest Controller Configuration Values for 5760 WLC and GA

Data Field	5760 WLC	GA
Anchor Controller IP	10.99.2.242	10.99.2.242
Anchor Group Name	CA-Mobility-SubDomain-3	CA-Mobility-SubDomain-3
Foreign Controllers	10.100.222.1	10.100.221.1; 10.100.222.1

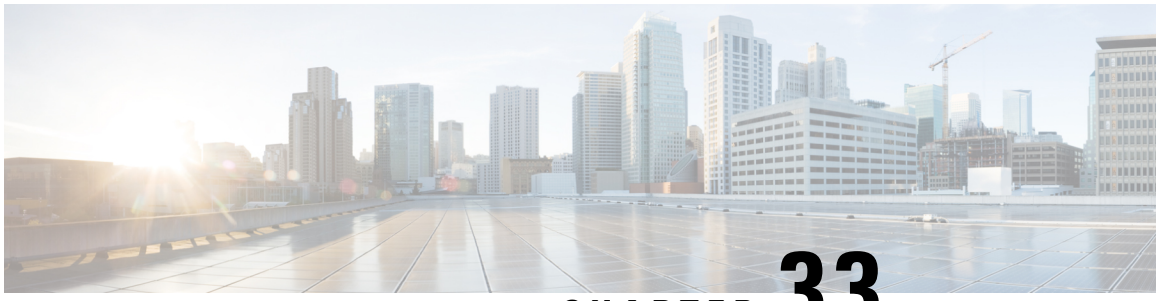
Table 75: Sample Mobility Configuration Values for 5760 WLC and GA

Data Field	5760 WLC	GA
Peer Controller IP(s)	10.100.222.1	—

Repeat the same procedure for 5760 WLC in SPG-2 shown in the above figure. After applying the Mobility configuration values, enter the Security, AVC and QoS configuration values as described in single-switch small network deployment model.

Related Topics

Prerequisites for Converged Access Deployment, on page 686
Configure Devices Using Converged Access Templates, on page 690
Field Reference: Converged Access Templates, on page 692
Example: Controller-Less Single-Switch Network, on page 695
Example: Controller-Less Single/Multi-Domain Wireless Network, on page 700
Example: Controller-Based Single/Multi-Domain Wireless Network, on page 701



CHAPTER 33

Configure Branch Threat Defense

Overview of Cisco Branch Threat Defense

Cisco Branch Threat Defense is a router security technology that strengthens protection and saves time and money without having to deploy multiple-point security products. This technology mitigates security vulnerabilities in branch offices with direct Internet connections that bypass your data center, and encrypt communication between enterprise branches, headquarters, and data centers. See Cisco Branch Threat Defense Guide.

You can use to configure Branch Threat Defense starting from Regulatory Compliance use cases, and configure the technologies such as Zone-Based Firewall (ZBFW), Snort Intrusion Prevention System (IPS), Cloud Web Security (CWS) and OpenDNS.

Related Topics

Supported IOS-XE Platforms, on page 705

Supported IOS-XE Versions, on page 705

Prerequisites for Enabling Branch Threat Defense, on page 706

Use the Branch Threat Defense Wizard, on page 706

Supported IOS-XE Platforms

The Branch Threat Defense functionality is supported on Cisco 4000 series Integrated Services Routers (ISR).

Supported IOS-XE Versions

The Branch Threat Defense functionality is available in Cisco IOS-XE Release 15.5(3)S1 (16.3.1 when OpenDNS is configured) and later releases.

Prerequisites for Enabling Branch Threat Defense

- This feature is available only in Security Packages which require a security license. Contact Cisco Support to obtain the license.
- Ensure that the Cisco 4000 series ISR has at least 8 GB of RAM. For more information, see the section "Virtual Service Resource Profile" in the Security Configuration Guide for Branch Threat Defense.
- Each router to be provisioned should already have a Snort IPS OVA present in the same location on its file-system. Use the "Copy OVA to Device" CLI template to distribute a Snort IPS OVA to each device to be provisioned before proceeding.

Related Topics

Supported IOS-XE Platforms, on page 705
Supported IOS-XE Versions, on page 705
Use the Branch Threat Defense Wizard, on page 706

Use the Branch Threat Defense Wizard

Step 1 Choose Services > Network Services > Branch Threat Defense.

Step 2 Click Next to choose the configuration.

Step 3 Read the description in the Choose Configuration page and choose the required use case from the Select a Use Case drop-down list.

The configuration options vary according to the selected use case.

Step 4 Choose the required configuration options and click Next.

Step 5 Choose the devices you want to configure and click Next.

Step 6 Enter the configuration values or use the import/export icon to configure the ZBFW, Snort IPS CLI, CWS and OpenDNS depending on the chosen use case.

Step 7 Click Apply and click Next to goto CLI Summary tab where you can confirm the device and template configuration values.

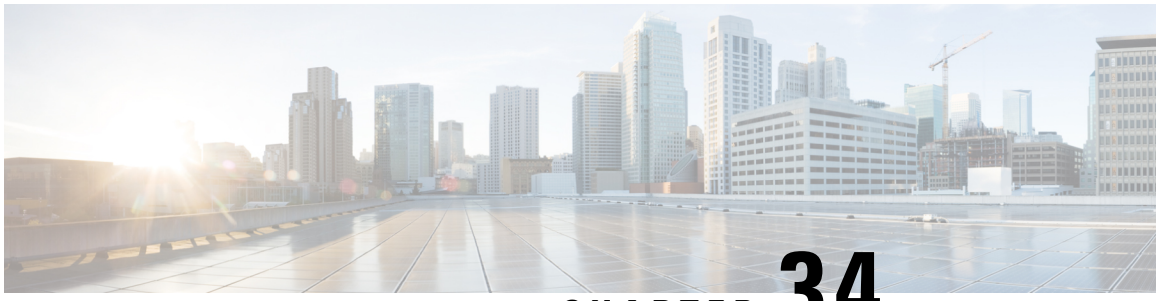
Step 8 Schedule the deployment job using Prepare and Schedule tab.

Step 9 Click Next and click Deploy in the Confirmation tab to deploy the Branch Threat Defense.

Step 10 Click Job Status to view the job details in the Job Dashboard.

Related Topics

Overview of Cisco Branch Threat Defense , on page 705
Supported IOS-XE Platforms, on page 705
Supported IOS-XE Versions, on page 705
Prerequisites for Enabling Branch Threat Defense, on page 706



CHAPTER 34

Access Network Workflow

Overview

The Access Network workflow in automates the access switch deployment in routed access networks in enterprise branch or campus networks. This includes building and managing access VLAN database, interface template management, and access ports configuration. The Access Network workflow provides complete automation for deploying access networks using Cisco catalyst 4500, 3850, 3650, 2960XR and 2960X series switches. In addition, it also automates the static or dynamic provisioning of access ports based on automatic device detection. The workflow reduces the deployment efforts and time by automatically deploying the applicable Cisco best practice configurations and provides a centralized view of the network for management purpose.

The Access Network workflow automates the following tasks:

- Simultaneous multiple access switch configuration—Allows the administrator to provision multiple access switches simultaneously, thus reducing the network provisioning efforts. Allows automatic access switch detection from a seed device, thus minimizing the efforts to detect all the access switches connected to a distribution switch.
- VLAN Management—Allows to create and maintain a database of access and voice VLANs used in the access layer. This database is used to configure access switches, ensuring uniformity in VLAN names and avoiding VLAN nomenclature/id mismatch errors.
- Provisioning Access Ports—Creates and applies templates and VLANs to automatically provision access ports for:
    - accepting Cisco devices that can be detected dynamically, such as Cisco IP phones, Cisco access points, Cisco video surveillance camera, Cisco TelePresence, and Cisco digital media player.
    - detecting non-Cisco devices that can be detected dynamically based on OUI or MAC address.
    - supporting devices such as laptops that cannot be detected dynamically.
- Deploys applicable Cisco Best Practice configurations, automatically.

Pre-requisites for Using Cisco Access Network Workflow

To successfully use the Cisco Access Network workflow, you must ensure that the following pre-requisites are met for the network devices and system:

- Routed Access network—Ensure that the access switches are connected to the distribution layer via layer 3 interfaces.
- Initial Device Setup—Devices are reachable from with SSH/Telnet and SNMP configured.
- Device On-boarding—Devices are added to Inventory.
- IOS Software—Devices have the recommended software version, see Supported Devices.
- Supported Platforms—Devices must belong the supported product families, see Supported Devices.

Supported Devices

The following table shows the supported switches for Access Network workflow.

Table 76: Supported Switches

Product	SKU Type	Mode	Modules	Minimum Software Version	Minimum Software License
WS-C2960X	Copper / POE	Standalone	-	IOS 15.2.2E	LANbase
WS-C2960X	Copper / POE	FlexStack	-	IOS 15.2.2E	LANbase
WS-C2960XR	Copper / POE	Standalone	-	IOS 15.2.2E	IP Lite
WS-C2960XR	Copper / POE	FlexStack	-	IOS 15.2.2E	IP Lite
WS-C3650	Copper / POE	Standalone	-	IOS-XE 3.7.3	IPBase
WS-C3650	Copper / POE	StackWise	-	IOS-XE 3.7.3	IPBase
WS-C3850	Copper / POE / mGig	Standalone	-	IOS-XE 3.7.3	IPBase
WS-C3850	Copper / POE / mGig	StackWise	-	IOS-XE 3.7.3	IPBase
WS-C45xx-E	Copper / POE / mGig	Standalone	Single and Dual Sup (SUP7E or SUP8E), with 47xx and 46xx series line cards	IOS-XE 3.6.4 and above	IPServices
WS-C45xx-R+E	Copper / POE / mGig	Standalone	Single and Dual Sup (SUP7E or SUP8E), with 47xx and 46xx series line cards	IOS-XE 3.6.4 and above	IPServices

Note Cisco Prime Infrastructure does not support IOS-XE SD-WAN image for any of the devices.

Using Access Network Workflow

To create to an Access Network deployment profile, do the following:

Step 1 Choose Services > Network Services > Access Network.

Step 2 Click New Deployment to create a new deployment profile.

Step 3 Ensure that the pre-requisites mentioned in the Before you Begin page are satisfied and then click Begin.

Step 4 Enter the Deployment Name, Description and click Save.

Step 5 Click Add Devices in the Action Panel and choose the devices you want to configure.

Step 6 Click Add.

The Cisco Best Practice configuration will be automatically added to the new devices.

Step 7 Alternately, you can add the devices by entering the seed device IP address to display the list of CDP neighbors of the seed device.

Step 8 Click Yes in the popup window, if you want to take back up of the device running configuration to the device local storage.

The Activity Log shows the Best Practice configuration job status and the back up job status of the newly added devices. You must wait until the jobs reach Completed status before moving to the Access Management page. If there are some errors in the Activity Log, the device may have some incompatible configurations that cause CLI deployment errors. Go to Administration > Dashboards > Job Dabshoard to see more information about the CLI errors. You can remove the failed devices, correct the errors, and add the device again.

Step 9 (Optional) If you want to remove any device from the Device Group pane, choose the device and click Remove Devices in the Action Panel.

Step 10 Click Next to move to the Access Management page to Add, Remove or Update the interface templates.

Step 11 Click the Add radio button in the Action Panel and do the following:

a) Choose the template type from the drop-down list containing workgroups, custom templates, and built-in templates (endpoints).
b) Enter the Name. The Template Name gets auto-populated based on the entered Name.
c) If you choose custom template, enter the device classification type and the classification value.
d) Choose a VLAN from the available VLANs or enter a new VLAN Name.

   If the VLAN does not exist, the workflow automatically creates a VLAN ID for the entered VLAN name. The VLAN name is expected to be common across switches, but may be associated with different VLAN IDs in different switches.

e) Click Apply.
f) (Optional) If you want to manually enter the VLAN ID when creating a new VLAN, click the VLANs tab in the Action Panel and set the Auto VLAN ID to OFF and enter the VLAN ID in the table.
g) Click Deploy.

Step 12 If you see templates with a red i icon indicating that these templates are missing in some devices or out-of-sync with other devices, choose Update to redeploy these templates to all devices to keep them in sync or choose Remove to remove the unwanted templates.

Step 13 Click Next to move to the Ports Management page to manage port groups, configure and administrate ports.

Step 14 Click the Add radio button and do the following in the Action Panel to create a new port group.

a) Enter the Group Name.
b) Choose the port group type from the drop-down list containing workgroups, custom groups, and built-in groups (endpoints).
c) Set the AutoConf and AutoQoS options to ON or OFF based on the chosen port group type.
d) Click Deploy.

Step 15 Click the Port Config tab in the Action Panel to bind the ports to port groups or configure individual ports.

a) Choose the device ports in the Ports Pane.
b) Click the Group Binding radio button in the Action Panel.
c) Choose the port group from the Group Name drop-down list to add the selected ports to the port group.
d) Click Apply.
e) Click Deploy.
f) Choose the device ports in the Ports Pane and click the Configure Ports radio button.
g) Choose the template type, template name, Data VLAN, AutoConf and Voice VLAN in the Action Panel.
h) Click Apply.
i) Click Deploy.
j) Choose the device ports in the Ports Pane and click the QoS Policy radio button and set the Automatic QoS to ON/OFF as required.

   QoS is not automatically enabled on the ports. If required, you can enable the Automatic QoS in the action panel. While enabling Automatic QoS, do not select the trunk ports, L3 ports or ports with existing QoS policies.

k) Click Apply.
l) Click Deploy.

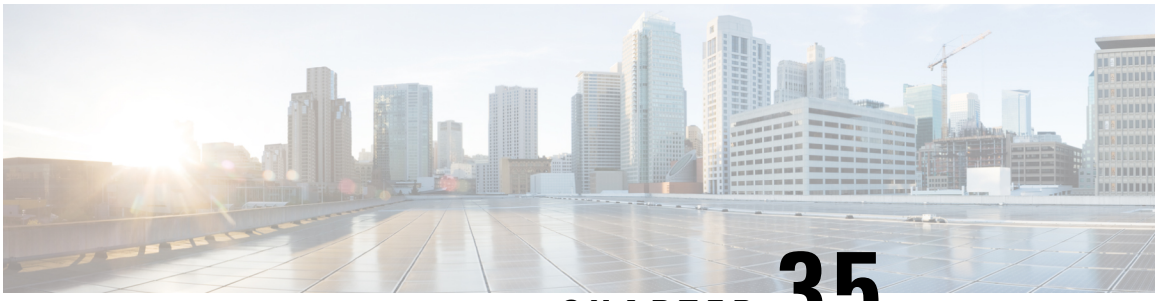
Step 16 Click the Admin tab in the Action Panel and do the following:

a) Choose the ports in the Ports pane.
b) Click the Up, Down, or Reset radio buttons as required to change the port status.
c) Click Deploy.

Step 17 Click Next to view the configuration summary of the created deployment profile.

Related Topics

Pre-requisites for Using Cisco Access Network Workflow, on page 708
Supported Devices, on page 708



CHAPTER 35

Improve Application Performance With Application Visibility and Control (AVC)

Improve Application Performance With Application Visibility and Control (AVC)

Use configuration templates in to design the set of device configurations that you need to set up the devices in a branch or change the feature configuration for a device from the Device Work Center.

Set Up Devices to Use AVC Features with WSMA

mainly uses the CLI method (over Telnet or SSHv2) to configure the devices. You can use WSMA (over SSHv2) for configuring specific features on the ASR and ISR devices. Cisco Web Services Management Agent is a more efficient and more robust method to configure the devices. supports Zone Based Firewall and Application Visibility configuration via WSMA on the ASR and ISR devices.

To configure Zone Based Firewall or Application Visibility via WSMA, follow these steps:

Step 1 Add or edit the device in to use SSHv2 (rather than Telnet) as the management transport protocol.

a) When you add the device with automatic discovery, enter the SSH credentials.

b) When you add the devices manually, in Step 2, select SSH2 as the protocol.

Step 2 If the device is also managed by which is not configured to use SSH2, edit the device credentials:

a) Choose Inventory > Device Management > Network Devices.
b) Select the device and click Edit.
c) Change the protocol to SSH2.
d) Click Update.

Step 3 Activate a WSMA profile on the device by configuring a WSMA configuration profile as follows:

Example:

```
#configure terminal
wsma agent config profile PIwsmaConfigServiceSSH
#exit
#wsma profile listener PIwsmaConfigServiceSSH
no wsse authorization level 15
transport ssh subsys wsma-config
#exit
```

Step 4 Configure a configuration archive, which will be used by WSMA for handling transactional configurations and rollbacks by using the following CLI commands on the device:

Example:

```
#configure terminal
archive
log config
hidekeys
path flash:roll
maximum 5
#end
```

Refer the following guides for more information:

- WSMA Configuration Guide
- Cisco IOS Configuration Fundamentals Command Reference Guide

What is AVC

The Application Visibility feature allows you to monitor traffic on specific interfaces and generate performance and bandwidth-statistics reports that supply information to the various dashlets and reports in . Devices send these reports to , and each report supplies information to a subset of the dashlets and reports. can configure Application Visibility either through CLI (over Telnet or SSH) or through WSMA. Application Visibility can be configured through WSMA in a more efficient and robust method and we recommend that you use the WSMA protocols for configuring Application Visibility. For more information on using WSMA with .

To simplify configuration, the Application Visibility feature is split into four types of metric and NetFlow reports:

Report	Description
Traffic Statistics	Sends the statistics on the bandwidth consumed by each of the NBAR-recognized applications on a per-user and per-interface basis. This report supplies information to the various application bandwidth dashlets and reports in as “Top N Applications”, “Application Bandwidth reports”, “Top N clients”, and so on.

Report	Description
HTTP URL Visibility	Sends performance and bandwidth reports for HTTP-based traffic, and this report supplies information to various URL dashlets and reports in as “Top N URL by hits” and “Top N URL by response time”. **Note** The HTTP URL Visibility tool is not supported on the ISR-G2 device.
Application Response Time	Sends performance-related information for TCP traffic, and this report supplies information to various response time dashlets and reports in as “applications ART analysis”, “worst N clients by transaction time”, and so on.
Voice/Video Metrics	Sends various RTP key-performance indicators for RTP-based voice/video traffic, and supplies information to dashlets and reports in under the voice/video category as “worst N RTP streams by packet lost.”

Set Up Devices to Use AVC Features with WSMA, on page 711
What is an NBAR Protocol Pack, on page 716
Create Application Visibility Templates, on page 716
Enable Default Application Visibility on Interfaces, on page 717

Supported Devices for AVC

The Application Visibility feature is supported on the following platforms:

- ASR 1000 series platform from Cisco IOS-XE Release 15.3(1)S1 or later
- ISR G2 platform from Cisco IOS Release 15.2(4)M2 or later as listed below:
  - Cisco 1900 Series Integrated Services Routers
  - Cisco MWR 1900 Mobile Wireless Routers
  - Cisco 2900 Series Integrated Services Routers
  - Cisco 3900 Series Integrated Services Routers
  - Cisco 812 CiFi Integrated Services Routers
  - Cisco 819 Non-Hardened Integrated Services Router
  - Cisco 819 Hardened Integrated Services Router
  - Cisco 819 Hardened 3G - Dual Radio 802.11n WiFi ISR
  - Cisco 861,861W Integrated Services Router G2
  - Cisco 867,867W Integrated Services Router G2
  - Cisco 866VAE Integrated Services Router
  - Cisco 880 3G Integrated Services Router G2
  - Cisco 881,881W Integrated Services Router G2
  - Cisco 881SRST,881SRSTW Integrated Services Router G2
  - Cisco 881W,881WD Integrated Services Router
  - Cisco 886,886W Integrated Services Router G2
  - Cisco 886SRST,886SRSTW Integrated Services Router G2
  - Cisco 886VA,886VAG Integrated Services Router G2
  - Cisco 886VA-W Integrated Services Router G2
  - Cisco 887,887W Integrated Services Routers G2
  - Cisco 887V Integrated Services Router G2
  - Cisco 886VA Integrated Services Router G2

- Cisco 887VA M Integrated Services Router G2
- Cisco 887VA-W Integrated Services Router G2
- Cisco 888,888W,888GW Integrated Services Router G2
- Cisco 888ESRST,888ESRSTW Integrated Services Router G2
- Cisco 888E,888EW Integrated Services Router G2
- Cisco 888EA Integrated Services Router G2
- Cisco 888SRST,888SRSTW Integrated Services Router G2
- Cisco 891,891W Integrated Services Router G2
- Cisco 892,892W Integrated Services Router G2
- Cisco 892F,892FW Integrated Services Router
- Cisco C892FSP Integrated Services Router
- Cisco C897VA Integrated Services Router
- Cisco C897VAW Integrated Services Router
- Cisco C891F Integrated Services Routers
- Cisco C881 Integrated Services Router
- Cisco C899 Secure Gigabit Ethernet with Multi-mode 4G LTE Router
- Cisco 800M with 4-Port LAN Integrated Services Router
- Cisco 800M with 8-Port LAN Integrated Services Router
-

- Cisco Integrated Services Virtual Router (ISRv) platform from Cisco IOS-XE Release 16.3 or later
- Cisco ISR 1000 platform from Cisco IOS-XE Release 16.6.1 or later

- Cisco ISR 4200, 4300 and 4400 series platform from Cisco IOS-XE Release 15.3(2)S or later
- CSR platform from Cisco IOS-XE Release 15.3(2)S or later

Prerequisites for Using Application Visibility and Control

Activating the Application Visibility feature can impact device performance. To minimize the potential impact, the template allows you to select the traffic interfaces to monitor and the reports to generate.

Application Visibility is configured differently on different platforms and IOS releases. Newer IOS releases provide new mechanisms with better performance for setting up the Application Visibility and Control (AVC). Thus when upgrading an ASR 1000, CSR or ISR 4400 platforms running IOS-XE release prior to 15.4(1)S to an IOS-XE release 15.4(1)S or later, or when upgrading an ISR-G2 platform running IOS release prior to 15.4(1)T to IOS release 15.4(1)T or later, we recommend that you re-configure the AVC on these devices.

To configure application visibility in your network:

1. (Optional) Set up WSMA on the devices to assure that the devices is configured via the WSMA protocol, rather than CLI. WSMA provides a more robust configuration mechanism.
2. Make sure that your devices are running an up-to-date NBAR protocol packs.
3. Estimate the potential resources impact on the device (CPU and memory) before activating application visibility on the device.

Activate application visibility on the device, either by creating a template and pushing it across the network, or by enabling AVC on an interface from the Device Work Center.

Estimate CPU, Memory and Network Resources on ASR Devices

The Readiness Assessment feature allows you to estimate CPU consumption, memory usage, and NetFlow export traffic when you deploy application visibility features on an ASR device. DRE helps you analyze the

demands for these resources on ASR devices based on typical predefined traffic profiles and device interface speeds.

DRE is supported on all ASRs running Cisco IOS-XE Release 15.3(1)S1 or later with one or more of these modules installed:

- cevModuleASR1000ESP5
- cevModuleASR1000ESP10
- cevModuleASR1000ESP20
- cevModuleASR1001ESP
- cevModuleASR1002FESP

To estimate the resource utilization on a specific device, follow these steps:

Step 1 Choose Services > Application Visibility and Control > Readiness Assessment.

Step 2 In the Interface column for the device that you want estimates on, click the down arrow icon.

The list shows only those interfaces supporting Application Visibility capability.

Step 3 Select Internet Profile or Enterprise Profile. The device resource estimation is based on a typical traffic profile. Select "Internet Profile" for typical service-provider traffic, or "Enterprise Profile" for a typical enterprise-traffic.

Step 4 Select the interfaces for which you want to estimate the resource utilization.

Speeds shown are those currently configured for each interface. If you want to base the estimate on a different speed, click Speed (Mbps) and enter a different value.

Step 5 Click Get Estimates.

The Estimated Resource Usage graph displays the current, additional, and total usage of the CPU and memory, along with the threshold limit for these resources. The estimated and maximum NetFlow export traffic are also given. For devices on which AVC is already enabled, only the current and additional usage is shown.

If resource usage is crossing threshold limits, optimize the problem device by:

- Decreasing current CPU utilization
- Increasing configured memory
- Reduce configured interface speed
- Redirecting traffic to another device

View DMVPN Details of Routers

To view the DMVPN details of routers, do the following:

Step 1 Choose Services > Application Visibility and Control > DMVPN Monitor Home to view the details of routers supporting DMVPN and the active spokes count.

Step 2 Click a device name to view the hub details including VRF, local tunnel IP, tunnel interface number and spokes count.

Step 3 Click the Show Spoke Details button to view the spoke details of the selected hub.

What is an NBAR Protocol Pack

The ability of the device to produce application visibility reports is based on the NBAR technology; NBAR, or Network-Based Application Recognition, is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/User Datagram Protocol (UDP) port assignments.

NBAR is updated frequently to support new applications and protocols, the software update for an NBAR is called a Protocol Pack.

Further information on NBAR protocol packs and information on how to upgrade NBAR protocol pack.

When you upgrade an NBAR protocol pack on the device, a corresponding update should be performed to update with the supported protocols/applications on the devices.

To achieve that there is a periodic software update (UBF file) issues when new protocol packs are released. Once you upgrade the NBAR protocol pack on the device, you should use software upgrade to make sure is also updated with the latest protocols.

At every point of time the network may contain various platforms (ISR-G2/ASR) running different Cisco IOS software releases and different protocol pack releases. While we do not recommend that you have different protocol pack releases installed on different devices reporting application visibility reports simultaneously, will be able to support this, by configuring only the supported subset of protocols/applications, defined as filtering conditions in your template, on each of the devices, when deploying an application visibility template across multiple devices running different versions of NBAR protocol packs.

For more information, see NBAR Configuration Guide

Create Application Visibility Templates

An application visibility monitoring policy is defined on a selected group of interfaces. When you define the template, ensure that you have defined an interface-role object which matches the group of interfaces on which you would like to monitor the traffic and generate NetFlow reports.

To create an Application Visibility template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Application Visibility > AVC Configuration.

Step 2 In the Template Basic area, enter a unique name and a description in the appropriate fields.

Step 3 In the Validation Criteria area, choose a device type from the list and enter the OS version.

Step 4 In the Template Detail area, choose an Interface Role from the drop-down list. The interface role designates the group of interfaces on which you can monitor the traffic and produce Application-Visibility reports.

Step 5 In the Traffic Statistics area, you can determine which traffic should be monitored to produce the traffic statistics reports, select the Off radio button if you do not want to collect the statistics on data packets.

a) Select the IP address/subnets.You can generate the report only on IPv4 traffic. We recommend to configure the required minimal set of filter.

Step 6 In the HTTP URL Visibility area, you can select the traffic that should be monitored to produce the report. Select the Off radio button if you do not want to collect URL statistics.

a) Select the IP address/subnets. You can select a specific set of IPv4 addresses or subnets to be monitored.

b) Select the application from the drop-down list. You can select a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all of the enterprise related http-based applications are include in the list.

Step 7 In the Application Response Time area, you can determine the traffic that should be monitored to produce the application response time reports. Also, optionally set a sampling option for the reports. Select the Off radio button if you do not want to collect ART metrics.

a) Select the IP address/subnets. You can select a specific set of IPv4 addresses or subnets to be monitored.
b) Choose the Application from the drop-down list. You can select a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all of TCP traffic is monitored.
c) In the Advanced Options, choose the Sampling Rate from the drop-down list. In High scale environments, collecting performance indicators for every TCP conversation can lead to high resources consumption on the device. The sampling option provides the ability to further optimize the resource consumption by collecting the performance indicators for "1" out of every "n" TCP conversation. This advanced option can be used to activate sampling and select the sampling rate for the tool. It is not recommended to activate sampling as activating sampling leads to less accurate results. Sampling should be used when it is necessary to limit the resource consumption on the devices.

Note Sampling option is not applicable for ISR-G2 routers. This option will be ignored for the n ISR-G2.

Step 8 In the Voice/Video metrics area, you can determine the traffic that should be monitored to produce the voice/video reports. Select the Off radio button if you do not want to collect the voice/video metrics.

a) Choose the IP address/subnets. You can choose a specific set of IPv4 addresses or subnets to be monitored.

Note IP filtering is not supported on the ISR-G2 routers until all UDP traffic is monitored.

b) Choose the Voice/Video Application from the drop-down list. You can choose a specific set of applications that should be monitored (there could be up to 32 monitored applications). By default, all RTP enterprise-related applications are monitored.

Step 9 Click Save as New Template.

Enable Default Application Visibility on Interfaces

From the Device Work Center, you can view the reports that are generated on each of the interfaces and enable or disable a default Application Visibility configuration on selected interfaces.

When a device does not have an application visibility configuration deployed on it, or it has a default application visibility configuration deployed on it (if all metrics are collected with a set of default parameters), the Device Work Center allows you to enable or disable a default application visibility configuration on the device by selecting interfaces on the device and enabling or disabling the default configuration on the interfaces.

Note When you deploy an application visibility template to the device, the application visibility template configuration will overwrite the default application visibility configuration that was enabled from the Device Work Center.

The default configuration collects all the possible visibility metrics on all applicable IPv4 traffic.

The Application Visibility feature is supported on the following platforms:

- ASR platform from Cisco IOS-XE Release 15.3(1)S1 or later
- ISR G2 platform from Cisco IOS Release 15.2(4)M2 or later
- ISR G3 platform from Cisco IOS-XE Release 15.3(2)S later
- CSR platform from Cisco IOS-XE Release 15.3(2)S later
- Cisco Integrated Services Virtual Router (ISRv) platform from Cisco IOS-XE Release 16.3 or later
- Cisco ISR 1000 platform from Cisco IOS-XE Release 16.6.1 or later

Note Application Visibility is configured differently on the ASR platform running Cisco IOS-XE15.3(1)S1 in comparison to Cisco IOS-XE15.3(2)S or later releases. After an ASR platform Cisco IOS release is upgraded from Cisco IOS-XE15.3(1)S1 to Cisco IOS-XE Releases 15.3(2)S and later, we recommend that you reconfigure Application Visibility on those devices.

To change the default application visibility configuration profile configured on the device, first disable the Application Visibility policy on all interfaces and then re-enable it on the selected interfaces with the new profile.

To enable or disable the default application visibility configuration on the specific interface, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from list, click Configuration. The Feature Configuration pane appears.

Step 3 Expand the App Visibility & controlfolder and choose App Visibility.

Step 4 Do one of the following:

- To activate an out-of-the-box AVC profile on an interface, select one or more interfaces then click Enable App Visibility and select the required profile. If at least one of the non-selected interface is attached to a different profile, a warning message will be displayed such that all non-selected interfaces that are attached to a different profile will be detached from that profile.
- Use the interfaces list to view the current App Visibility configuration on the device. The column App Visibility Policy displays the current profile/policy attached to the interface.

  Note The application visibility feature displays the user defined AVC policy per interface on the application visibility interfaces.

There are several options that can be displayed:

- If the application visibility control is configured on the interface using the Application Visibility Template, the template-name will be displayed.
- If the application visibility control is configured on interface using the “one-click” option, the name of the AVC Profile that was configured will be displayed.
- If the application visibility control is configured manually out-of-band by the user via CLI, the name of the policy-map or performance monitor context that was configured will be displayed.

Note A visual indication column (App Visibility Status) provides indication on whether AVC is currently activated on the interface. The column will also indicate cases when the interface is INCAPABLE of running AVC and cases when AVC is mis-configured on the interface (e.g. AVC configured to send netflows to servers other than).

- To Disable any of the Activated AVC profiles on an selected interface, click Disable App Visibility.

  Note When Enabling/Disabling AVC a pop up message will appear before the actual provisioning takes place. Selecting the CLI preview tab on that popup message will generate the list of CLIs to be pushed to the device.

Note Alternately, you can also enable or disable AVC for a device from Services > Application Visibility & Control > Interfaces Configuration

If HA is configured with IPv4 Virtual IP address, the same Virtual IP address gets automatically fetched in the configuration when AVC is enabled in a device or interface.

Troubleshoot Traffic Flows Using AVC

You can collect application visibility data on every flow that goes through the monitored interface. However, because this can have a significant impact on the device performance, application visibility data is collected in an aggregated manner. To further troubleshoot specific flows, you can activate the Application Visibility troubleshooting sessions on the device. The sessions are activated on specific interfaces and on specific traffic. They allow you to collect the non aggregated information on a flow-based level that supplies a raw-NetFlow report in . This information can be used later to analyze specific flows.

The Application Visibility Troubleshooting feature allows you to:

- Create and activate a troubleshooting session on a specific interface
- Deactivate and delete a troubleshooting session on a specific interface

Caution To avoid overloading the server, we recommend that you configure no more than ten active troubleshooting sessions. Application troubleshooting is not supported on the ISR-G2 platforms.

Note Troubleshooting sessions are configured differently on the ASR platform running Cisco IOS-XE Release 15.3(1)S1 in comparison to Cisco IOS-XE Release15.3(2)S or later releases. After, an ASR platform Cisco IOS Release is upgraded from Cisco IOS-XE Release 15.3(1)S1 to Cisco IOS-XE Release 15.3(2)S or later, we recommend that you deactivate and reactivate active troubleshooting sessions on those devices.

To troubleshoot Application Visibility, follow these steps:

Step 1 Choose Services > Application Visibility & Control > Application Troubleshooting.

Step 2 In the AVC Troubleshooting Session page, click Add and enter a session name.

Step 3 In the Source/Destination IPs field, click Edit, and choose the source and destination IP addresses from the drop-down list. You can select the IP traffic and collect Application Visibility troubleshooting information for that specific IP traffic. The options are: on all IPv6 traffic or on all IPv4 traffic or on specific IPv4 addresses/subnets. Also, you can select a list of IP constraint pairs. Each such pair designates a bi-directional symmetric condition on the source and destination IPs of the traffic. For example, the pair: Any IPv4 <=> IPv4 subnet 192.168.0.0/16 matches all of the flows from 192.168.0.0/16 to any other IP and vice-versa (all of the flows from any IP address to 192.168.0.0/16). You can add multiple pair conditions.

Step 4 To add more IP constraints in the format of IP source/destination pairs, click the + icon in the Select Source Destination dialog box.

Note The IP addresses on both sides of the pairs should be of the same IP version.

Step 5 Click OK.

Step 6 Choose the device from the Device Table list.

Step 7 Choose the interface from the Interface Table list.

Step 8 Choose the application from the object selector dialog box. When you choose the applications, you can have a combination of Categories, Sub-categories, Encrypted Applications, and Tunneled Applications from the available list. A maximum of 32 applications or categories or attributes can be selected.

Step 9 Click Save to automatically activate the session.

Step 10 After the troubleshooting session is activated, click Launch Report to generate the Raw NetFlow report.

Activate AVC Troubleshooting Sessions

You can activate an inactive troubleshooting session or deactivate an existing troubleshooting session.

To activate or deactivate a troubleshooting session, follow these steps:

Step 1 Choose Services > Application Visibility & Control > Application Troubleshooting.

Step 2 Choose a troubleshooting session from the list and click Activate or Deactivate.

Step 3 Click Save.

Edit AVC Troubleshooting Sessions

You can edit or delete an inactive troubleshooting session. (To edit or delete an active session, you must deactivate it first.)

To edit or delete a troubleshooting session, follow these steps:

Step 1 Choose Services > Application Visibility & Control > Application Troubleshooting.

Step 2 Do either of the following:

a) Choose a session from the list and click Edit.

Caution To avoid overloading the server, we recommend that you configure no more than ten active troubleshooting sessions.

b) Edit and save the troubleshooting session, then click Activate.

c) To delete a troubleshooting session, choose a session from the list and click Delete.

Configure the Data Sources You Want AVC To Use

depends on a variety of sources for accurate gathering and reporting of device, performance and assurance data. These sources include specialized monitoring devices such as NAMs, and protocols running on normal devices, such as Cisco Medianet, NetFlow, Flexible NetFlow, Network Based Application Recognition (NBAR), Performance Monitoring (PerfMon), and Performance Agent.

You will want to manage these sources to ensure that only the correct data is gathered from active sources. The Data Sources page allows you to review your current data sources, and delete those that are no longer active.

Use the Data Sources page to review current data sources.

Step 1 Select Services > Application Visibility & Control > Data Sources. displays a summary page that lists each data source's:

- Device Name—The host name of the data source
- Data Source—The IP address of the data source.
- Type—The type of data the source is sending to (example, "NetFlow").
- Exporting Device—The IP address of the device exporting the data to .
- Last 5 min Flow Record Rate—The flow rate for the data has received from this source during the last five minutes. You can click the hyperlink and view the flow rate and flow count of the Top N 5 flow data sources in a tabular or graphical format. You can also click the hyperlink corresponding to a particular data source and view the flow rate and flow count of that data source in a tabular or graphical format.
- Last Active Time—The latest date and time that received data from this source.

Step 2 For additional details on the Data Source's configuration template or for a Device 360 view of the Exporting Device, click the "i" icon shown next to the Data Source or Exporting Device listing.

Step 3 To delete inactive data sources select the checkbox next to the inactive data source you want to delete.

Step 4 Click Delete.

Step 5 Click OK to confirm the deletion.

You cannot delete a NetFlow data source until seven full days have elapsed without receipt of any data from that source. This delay helps protect the integrity of NetFlow data (which identifies and aggregates according to source) by giving network operators a full week to ensure that the data source has been retired. If the source becomes active again at any time during that seven-day period, its data will still be identified and aggregated properly with other data from the same source. If the source is deleted after seven days, and then becomes active again, all of its data will be identified and aggregated as coming from a new source.

Configure AVC Data Deduplication

Data deduplication allows you to identify authoritative data sources for the corresponding location groups.

stores all the data it receives about network usages from all the sources (including any duplicate data that it may receive from multiple sources). When you specify authoritative data sources, only the data from the specified source is displayed when you view a particular site.

The data deduplication page allows you to specify a data source per a specific site. For example if you have a Network analysis module (NAM) at a branch office as wel as Netflow data that is sent from the same branch, you can choose to see the site information as it is reported by the NAM or netflow data with authoritative data source.

The two authoritative data sources are:

- System detected—Based on the managed device product families. You can change the device family selection precedence. To change the precedence, click on the settings icon and drag and drop the device families. The authoritative datasources are selected according to this precedence.
- Customized—You can pick and choose from the managed data source.

Step 1 Choose Services > Application Visibility & Control > Data Deduplication. The Data Deduplication page appears.
Step 2 Click System Detected to identify the data sources in the location group or select the customized to select the data sources.
Step 3 Click Save.
Step 4 Click Apply.

Configure VPN IKE Policies and Settings Using Configuration Templates

To create an IKE policies template, follow these steps:

Step 1 Choose Configuration >Templates > Features & Technologies > Security > VPN Components > IKE Policies.
Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.
Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS version. For more information about the required field descriptions, see the Cisco Prime Infrastructure Reference Guide.
Step 4 Click Save as New Template.

Configure VPN IPSec Profiles Using Configuration Templates

To create an IPsec profile template, follow these steps:

Step 1 Choose Configuration >Templates > Features & Technologies > Security > VPN Components > IPSec Profile.
Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.
Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version.
Step 4 In the Template Detail area, click Add Row and enter the required information. A transform set represents a certain combination of security protocols and algorithms. During the IPsec negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform set describes a particular security protocol with its corresponding algorithms. For more information about the required field descriptions, see the Cisco Prime Infrastructure Reference Guide.
Step 5 Click Save as New Template.

Configure VPN Preshared Keys Using Configuration Templates

To create a preshared keys template, follow these steps:

Step 1 Choose Configuration >Templates > Features & Technologies > Security > VPN Components > Preshared Keys.
Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.
Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.
Step 4 In the Template Detail area, click Add Row and enter the required information.
Step 5 Click Save as New Template.

Configure VPN RSA Keys Using Configuration Templates

To create RSA keys template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Security > VPN Components > RSA Keys.
Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.
Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version.
Step 4 In the Template Detail area, click Add and enter the required information.
Step 5 Select the Exportable box to generate RSA as an exportable key, then click OK.
Step 6 Click Save as New Template.

Configure VPN Transform Sets Using Configuration Templates

To create a transform sets template, follow these steps:

Step 1 Choose Configuration >Templates > Features & Technologies > Security > VPN Components > Transform Sets.
Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.
Step 3 In the Validation Criteria area, choose a device type from the drop-down list and enter the OS version.
Step 4 In the Template Detail area, click Add Row and enter the required information.

Note The ESP encryption algorithm is used to encrypt the payload, and the integrity algorithm is used to check the integrity of the payload.

Step 5 Click Save as New Template.

View NetFlow Templates

Netflow templates define the metadata/structure that is used to process incoming UDP packets. These templates specify the metrics to be collected from the devices. Prime Infrastructure allows you to view the defined templates from Services > Application Visibility & Control > NetFlow Templates. You can configure the template either through AVC Profile in Application Control Page or through CLI manually.

Custom Reports option in the NetFlow Templates page is deprecated from Cisco Prime Infrastructure Release 3.2, due to high disk space usage. You can generate the report from the Reports > Reports Launchpad > Raw NetFlow page.

What Is An Easy VPN Server

Cable modems, xDSL routers, and other forms of broadband access provide high-performance connections to the Internet, but many applications also require the security of VPN connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated and typically requires tedious coordination between network administrators to configure the VPN parameters of the two routers.

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server. This server can be a dedicated VPN device; for example, any of the following:

- Cisco VPN 3000 concentrator
- Cisco PIX Firewall
- Cisco IOS router that supports the Cisco Unity Client Protocol

After the Cisco Easy VPN server is configured, a VPN connection is created with minimal configuration on an Easy VPN remote, such as a Cisco 800 series or 2800 series router. When the Easy VPN remote initiates the VPN tunnel connection, the Cisco Easy VPN server pushes the IPsec policies to the Easy VPN remote and creates the corresponding VPN tunnel connection.

Configure Web Browser Proxy Settings for an Easy VPN Server Using Configuration Templates

The Easy VPN Server Proxy feature allows you to specify the settings for Easy VPN clients. Using this feature, you do not have to manually modify the proxy settings of the web browser when you connect to the corporate network using the Cisco IOS VPN client or manually revert the proxy settings when you disconnect from the network.

To create an Easy VPN Server Proxy template, follow these steps:

Step 1 Choose Configuration >Templates > Features & Technologies > Security > Easy VPN Server Proxy Setting.

Step 2 Enter the basic template information.

Step 3 From the Device Type drop-down list, choose Routers.

Step 4 In the Template detail area enter a name, and choose the settings that you want to associate with the group.

Step 5 Choose the No Proxy Server option or Automatically Detect Proxy Settings option if you want the clients in this group to automatically detect a proxy server when they use the VPN tunnel.

Step 6 Choose the Manual Configuration option to manually configure a proxy server for clients in this group. If you choose this option, you should manually configure a proxy server.

Step 7 Select the Bypass proxy server for local addresses check box to prevent the clients from using the proxy server for local (LAN) addresses.

Step 8 Click Save as New Template.

Configure an Easy VPN Remote Using Configuration Templates

The Cisco Easy VPN Remote feature eliminates much of this tedious work by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server.

Before You Begin

Create an ACL template and publish the ACL template.

To create a Easy VPN Remote template, follow these steps:

SUMMARY STEPS

1. Choose Configuration >Templates >Features & Technologies > Security > Easy VPN Remote.
2. Enter the basic template information.
3. From the Device Type drop-down list, choose Routers.

4. In the Easy VPN Remote Interface Configuration area, enter the required information. For more information about the required field descriptions, see the Cisco Prime Infrastructure Reference Guide.
5. In the Remote Authentication Mechanisms area, choose the authentication method.
6. In the Remote Firewall Settings area, set the firewall settings for the Easy VPN Remote connection.
7. Click Save As NewTemplate.
8. Navigate to the My Templates folder and choose the template that you just saved.
9. Click the Publish icon in the top-right corner, then click OK.
10. Create a composite template, and add the ACL and Easy VPN Remote templates to the composite template.
11. Use the arrows buttons to arrange the templates in the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the EasyVPN Remote template.
12. Click Save as New Template.

DETAILED STEPS

Step 1	Choose Configuration >Templates >Features & Technologies > Security > Easy VPN Remote.
Step 2	Enter the basic template information.
Step 3	From the Device Type drop-down list, choose Routers.
Step 4	In the Easy VPN Remote Interface Configuration area, enter the required information. For more information about the required field descriptions, see the Cisco Prime Infrastructure Reference Guide.
Step 5	In the Remote Authentication Mechanisms area, choose the authentication method.
Step 6	In the Remote Firewall Settings area, set the firewall settings for the Easy VPN Remote connection.
Step 7	Click Save As NewTemplate.
Step 8	Navigate to the My Templates folder and choose the template that you just saved.
Step 9	Click the Publish icon in the top-right corner, then click OK.
Step 10	Create a composite template, and add the ACL and Easy VPN Remote templates to the composite template.
Step 11	Use the arrows buttons to arrange the templates in the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the EasyVPN Remote template.
Step 12	Click Save as New Template.

Configure an Easy VPN Server Using Configuration Templates

The Easy VPN Server feature introduces server support for the Cisco VPN software client Release 3.x and later and Cisco VPN hardware clients (such as the Cisco 800, Cisco 900, Cisco 1700, VPN 3002, and PIX 501 devices). Using IP Security (IPsec), Easy VPN Server allows a remote end user to communicate with any Cisco IOS Virtual Private Network (VPN) gateway. Also, centrally managed IPsec policies are pushed to the client device by the server and helps the end user to minimize the configuration.

Before You Begin

Do the following:

- Create AAA method list for the group and the user by using the CLI template.
- Create an IPsec Profile template.

- If you will use Crypto Map, create a Transform Set template.
- (Optional) Create a CLI template for RADIUS server group creation or configure the RADIUS server while creating the AAA method list.
- (Optional) Create an ACL template for the split tunnel ACL in the ISAKMP Group configuration.
- Create a Browser Proxy template for ISAKMP group configuration.

To create an Easy VPN Remote template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Security > Easy VPN Server.

Step 2 Enter the basic template information.

Step 3 From the Device Type drop-down list, choose Routers.

Step 4 In the Interface Configuration area, choose the configuration methods and complete the fields of the interface that is configured on the device.

Step 5 In VPN Components Assembly area, enter the Transform Set profile name that you created in the Transform Set template (Configure VPN Transform Sets) and complete the fields in this area.

Step 6 In the Group Authorization area, enter the Method List profile name that you created in the CLI template and complete the fields in this area.

Step 7 In the User Authorization area, enter the same Method List profile name that you created in the CLI template, and complete the fields in this area.

Step 8 In the ISAKMP Group configuration area, click Add Row to add the ISAKMP Group configuration.

Step 9 In the ISAKMP Group configuration dialog box, enter the ACL profile name that you created in the ACL template and the Browser Proxy profile name that you created in the Browser Proxy template, and complete the fields in this area.

Step 10 Click Save as New Template.

Step 11 Create a composite template (Configure VPN Transform Sets) and add the AAA Method List and Radius server, IPsec Profile (Configure VPN IPSec Profiles Using Configuration Templates), ACL Browser Proxy (What Is An Easy VPN Server), and Easy VPN_ Remote templates in the composite template.

Step 12 Using the arrow icons to arrange the templates in a order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, arrange the ACL template first, followed by the EasyVPN_Remote template.

Step 13 Click Save as New Template.

Configure GSM Profiles Using Configuration Templates

To create a GSM Profile template, follow these steps:

Step 1 Click Configuration > Templates > Features & Technologies > Interfaces > Cellular > GSM Profile.

Step 2 Enter the basic template information.

Step 3 From the Device Type drop-down list, choose Routers.

Step 4 In the Template Detail area, enter an Access Point Name and choose a profile number from the drop-down list.

Step 5 Choose the type of authentication that your service provider uses. (CHAP authentication is more secure than PAP authentication.)

Step 6 Enter the username given to you by your ISP or your network administrator, and enter a password.

Step 7 Click Save as New Template.

Step 8 Click OK.

Configure Cellular Profiles Using Configuration Templates

To create a Cellular Profile template, follow these steps:

Note To deploy the Cellular Profile template on any GSM HSPA, HSPA+R7, and LTE-Verizon modem, you should have the GSM profile (Configure GSM Profiles Using Configuration Templates) created on the router.

Step 1 Choose Configuration > Templates > Features & Technologies > Interfaces > Cellular > Cellular Profile.

Step 2 Enter the basic template information.

Step 3 From the Device Type drop-down list, choose Routers.

Step 4 In the Template Detail area, define the interface as Primary WAN Interface or Backup WAN Interface and complete the fields.

Step 5 In the Dialer Configuration area, choose Yes to enable the persistent data connection and complete the fields.

Step 6 Click Save as New Template.

Step 7 Click OK.

Enable Scanning of HTTP and HTTPS Traffic Using ScanSafe

ScanSafe Software as a Service (SaaS) Web Security allows you to scan the content of HTTP and HTTPS traffic. When ScanSafe Web Security is integrated with a router, selected HTTP and HTTPS traffic is redirected to the ScanSafe cloud for content scanning and malware detection.

When Cisco Integrated Services Router (ISR) Web Security with Cisco ScanSafe is enabled and the ISR is configured to redirect web traffic to ScanSafe, the Integrated Services Router (ISR) transparently redirects HTTP and HTTPS traffic to the ScanSafe proxy servers based on the IP address and port. You can configure the ISR to relay web traffic directly to the originally requested web server without being scanned by ScanSafe.

Allowed list Traffic

You can configure the ISR so that some approved web traffic is not redirected to ScanSafe for scanning. When you bypass ScanSafe scanning, the ISR retrieves the content directly from the originally requested web server without contacting ScanSafe. When ISR receives the response from the web server, it sends the data to the client. This is called Allowed list traffic.

See the Cisco ISR Web Security with Cisco ScanSafe Solution Guide for more information about ScanSafe.

Creating a ScanSafe Template

To create a ScanSafe template, you must specify:

- The ScanSafe server and interface information
- Allowed list information

To create a ScanSafe template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Security > ScanSafe

Step 2 In the Template Basic area, enter a name and a description in the appropriate fields.

Step 3 In the Validation Criteria area, choose a device type from the list and enter the OS version.

Step 4 In the Template Detail area, enter the required information. For more information about the required field descriptions, see the Cisco Prime Infrastructure Reference Guide.

Step 5 Click Save as New Template.

Configure CDMA Cellular WAN Interfaces

To configure a CDMA interface, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Interface folder, then click Cellular WAN Interfaces.

Step 4 For a CDMA Sprint modem:

a) Select a cellular interface with CDMA Sprint modem, and click Manage Modem.

b) In the Manage Modem dialog box, select the OMA-DM or Manual radio button. If you choose the Manual option, complete the fields to manually configure the CDMA Sprint modem, then click OK.

Step 5 For a CDMA Verizon modem:

a) Select a cellular interface with CDMA Verizon modem, and click Manage Modem.

b) In the Manage Modem dialog box, enter the Account Activation Information, then click OK.

Step 6 For a CDMA Generic modem:

a) Select a cellular interface with CDMA Generic modem, and click Manage Modem.

b) In the Manage Modem dialog box, complete the fields to configure the CDMA Generic Modem, then click OK.

Configure GSM Cellular WAN Interfaces

To configure a GSM interface, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Choose the device from the list or click Add to add a new device, then configure the device.

Step 3 After choosing the device, click Configuration. The Feature Configuration pane appears.

Step 4 Expand the Interface folder, then choose Cellular WAN Interfaces.

Step 5 Select the GSM interface and click Manage Modem.

Step 6 In the Manage Modem dialog box, click Add Row.

Step 7 Choose the Profile Number from the drop-down list, and enter the Access Point Name, then click OK.

Configuring Network Address Translation (NAT)

Network Address Translation (NAT) is a process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. NAT helps to limit the number of public IP addresses used by an organization or company, for both economy and security purposes.

The NAT feature allows organizations to resolve the problem of IP address depletion when they have existing networks and need to access the Internet. NAT allows the IP network of an organization to use different IP address space for the outside network. Thus, NAT allows an organization that does not have globally routable addresses to connect to the Internet by translating those addresses into globally routable address space. NAT also allows a more graceful renumbering strategy for organizations that are changing service providers or voluntarily renumbering into Classless Inter Domain Routing (CIDR) blocks. NAT is described in RFC 1631.

A router configured with NAT will have at least one interface to the inside network and one to the outside network. In a typical environment, NAT is configured at the exit router between a subdomain and a backbone. When a packet leaves the domain, the NAT translates the locally significant source address into a globally unique address. When a packet enters the domain, NAT translates the globally unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table. If NAT cannot allocate an address because it has run out of addresses, it drops the packet and sends an Internet Control Message Protocol (ICMP) host unreachable packet.

For more information on NAT, see IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S.

NAT Types

NAT operates on a router—generally connecting only two networks together—and translates your private (inside local) addresses within the internal network, into public (inside global) addresses before any packets are forwarded to another network. This functionality gives you the option to configure the NAT so that it will advertise only a single address for your entire network to the outside world. Doing this effectively hides the internal network from the world, giving you additional security.

NAT types include:

- Static Address Translation (SAT) —Allows one-to-one mapping between local and global addresses.
- Dynamic Address Translation (DAT)—Maps unregistered IP addresses to registered IP addresses from a pool of registered IP addresses.
- Overloading—A form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports. This method is also known as Port Address Translation (PAT). With PAT, thousands of users can be connected to the Internet using only one real global IP address.

Configuring NAT for IP Address Conservation

To configure NAT, perform the following steps:

1. Creating NAT IP Pools, on page 730(required for Dynamic NAT)
2. Create an ACL template and configure the ACL
3. Creating NAT44 Rules, on page 730
4. Configuring Interfaces, on page 731and assign rules on them
5. Limit the Number of Concurrent NAT Operations on a Router Using NAT MAX Translation, on page 731(Optional)

Note The NAT feature is supported on the following: ASR platform from Cisco IOS Release 3.5 or later and ISR platform from Cisco IOS Release 12.4(24)T or later.

Caution CLI changes that begin with "EMS_" are not supported and might cause unexpected behavior.

Creating NAT IP Pools

The IP Pool is a device object that represents IP ranges to be used with Dynamic NAT. The NAT IP Pools feature allows you to create a new pool that can be used with Dynamic NAT, change the existing pool, and delete the pool from the device.

To create an IP pool, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security, expand the NAT subfolder, and then click IP Pools. The NAT Pools page appears.

Step 4 Click Add IP Pool > IP+Prefix or IP Range + Prefix, and enter the Name, IP Address/Range, Prefix Length, and Description. You cannot change the name of the pool after creating the pool.

Note A valid IPv4 address consists of 4 octets separated by a period (.).

Step 5 Click Save to deploy the IP pool to the device, or Cancel to cancel your editing.

Step 6 To edit the existing IP Pool, in the NAT IP Pools page do the following:

a) Click in the selected IP Pools parameters row, and edit the parameters. or

b) Select the IP Pools, and click Edit. The selected IP Pools opens for editing. You can edit all of the parameters except the pool name.

Step 7 Click Save to deploy the changes to the device.

Creating NAT44 Rules

The NAT44 feature allows you to create, delete, and change NAT44 rules.

There are three types of NAT rules:

- Static
- Dynamic
- Dynamic PAT

To create the NAT44 rule, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security, expand the NAT subfolder, and then click NAT44 Rules.

Step 4 In the NAT 44 page, click the down arrow icon next to the Add NAT Rule button.

- Click Static to create Static Rule. For a description of the elements, see the Cisco Prime Infrastructure Reference Guide.
- Click Dynamic to create Dynamic NAT Rule. For a description of the elements, see the Cisco Prime Infrastructure Reference Guide.
- Click Dynamic PAT to create Dynamic PAT Rule. For a description of the elements, see the Cisco Prime Infrastructure Reference Guide.

Step 5 Click Save to save and deploy the changes to the device.

Step 6 To edit the existing NAT44 rule in the NAT44 page, do one of the following:

- Click the selected NAT44 rules parameters row, and edit the parameters.
- Select the NAT44 rule, and click Edit. The selected NAT44 rule opens for editing. You can edit all of the parameters.

Step 7 You can change the Source and Destination according to the creation rules. You can also change the Options selection according to the creation rules.

Step 8 Click Save to save the changes in the server.

Configuring Interfaces

A virtual interface is a logical interface configured with generic information for a specific purpose or for specific users, plus router-dependent information.

To configure a virtual interface, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security, expand the NAT subfolder, and then click Interfaces.

In the Interface page, select the interface that you want to change and choose the association from the drop-down list. The options are: Inside, Outside, and None.

Step 4 Click Save to save the changes in the server.

Limit the Number of Concurrent NAT Operations on a Router Using NAT MAX Translation

The NAT MAX Translation feature provides the ability to limit the maximum number of concurrent NAT operations on a router. In addition, the NAT MAX feature gives users additional control to use the NAT addresses. The Rate Limiting NAT Translation feature can be used to limit the effects of viruses, worms, and denial-of-service attacks. For more information on Configuring the Rate Limiting NAT Translation Feature, see Configuring NAT for IP Address Conservation in IP Addressing: NAT Configuration Guide, Cisco IOS XE Release 3S.

The NAT MAX Translation feature allows you to reset the global translation attribute values.

To set up the MAX Translation, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Choose the device from the list or click Add to create a new device, then configure the device.

Step 3 After choosing the device, click Configuration. The Feature Configuration pane appears.

Step 4 Expand the Security, expand the NAT subfolder, and then click Advanced Settings > Max. Translation.

Step 5 Reset the parameter values. Configure the maximum number of NAT entries that are allowed for all of the parameters. A typical range for a NAT rate limit is from 100 to 300 entries.

Step 6 Click Save to save the changes in the server.

Configure IPSec Topologies Using DMVPN

The DMVPN feature allows you to scale large and small IP Security (IPsec) VPNs by combining generic routing encapsulation (GRE) tunnels, IPsec encryption, and Next Hop Resolution Protocol (NHRP).

A typical VPN connection is a point-to-point IPsec tunnel connecting two routers. DMVPN enables you to create a network with a central hub that connects other remote routers, referred to as spokes, using a GRE over an IPsec tunnel. IPsec traffic is routed through the hub to the spokes in the network.

See Dynamic Multipoint IPsec VPNs (Using Multipoint GRE/NHRP to Scale IPsec VPNs) for more information about DMVPN (requires a Cisco.com login ID).

Cisco Network Control System allows you to configure your router as a DMVPN hub, DMVPN spoke or cluster. You can configure the router in the following ways:

Related Topics

Configure a DMVPN Hub and Spoke Topology, on page 733
Configure a DMVPN Fully Meshed Topology, on page 734
Configure a DMVPN Cluster Topology, on page 734

Create DMVPN Tunnels

To create a DMVPN tunnel, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security folder, and then click DMVPN. Click Add to create the DMVPN.

Step 4 In the Device Role and Topology Type area, select the topology and the device role. The options are: Spoke, Hub, and Dynamic Connection between Spokes.

Step 5 In the Multipoint GRE Interface Information area, choose the WAN interface that connects to the Internet from the drop-down list.

Step 6 Enter the IP address of the Tunnel Interface, and Subnet Mask.

Step 7 Complete the fields in the NHRP and Tunnel Parameters area.

Note The Network ID is a unique 32-bit network identifier from a Non Broadcast Multiaccess (NBMA) network. The tunnel key is used to enable a key ID for a particular tunnel interface. The MTU size of IP packets that are sent on a particular interface.

Note The default MTU value for Ethernet and the serial interface is 1500. The default value varies depending upon the media type. The Tunnel throughput delay is used to set the delay value for a particular interface.

Step 8 In the Encryption policy field, click the anchored plus button (+) to add the Transform Set Profile (see Security > VPN Components > Transform Sets in Cisco Prime Infrastructure Reference Guide).

Step 9 In the Transform Set Profile dialog box, enter the Name and choose the acceptable combination of security protocols and algorithm from the drop-down list to configure the transform set.

Step 10 Select the IP Compression check box to enable the IP compression for the transform set.

Step 11 Choose the mode for the transform set. The options are: Tunnel mode or Transport mode.

Step 12 In the NHS Server Information area, enter the IP address for the physical interface of the hub and tunnel and the Fallback Time. If the device supports the cluster then add the next hop server information, such as Cluster ID, Max Connection, Hub IP address, and Priority.

Note The NHS server information is required only for spoke configuration. If you select the Use Cluster for NHS check box, add the information, such as Cluster ID, Max Connection, and Next Hub Server. The template with the NHS cluster configuration will be applied only to the device running Cisco IOS Software Release 15.1(2)T or later.

Step 13 In the Routing Information area, choose the routing information. The options are: EIGR, RIPV2, and Other.

Note The routing information is required only for hub configuration.

Step 14 Choose the existing EIGRP number from the drop-down list or enter an EIGRP number. Use the Other option to configure the other protocols.

Step 15 Click Save to save the single NHS server entry details and the priority of the server, save the entire group of server, and save the NHS cluster information. when you save the NHS cluster information, the NHS server will be populated in the non-editable field.

Step 16 Click OK to save the configuration to the device.

Configure a DMVPN Hub and Spoke Topology

To configure the hub and spoke topology, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security folder, and then click DMVPN. Click the Add button to create the DMVPN tunnel.

Step 4 In the Device Type and Topology area, choose Hub and Spoke as the topology, and select either Hub or Spoke as a device role.

Step 5 Choose the WAN interface from the drop-down list, and then configure the Multipoint GRE IP Address and the subnet mask for the tunnel interface.

Step 6 Configure the NHRP and the Tunnel Interface parameters, such as the IP address, NHRP parameters and map, MTU value, Source of the Tunnel, Tunnel Mode, and Tunnel Key.

Step 7 Create the transform-set for protecting the data flow between the devices. You can specify up to four transforms: One Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IPsec protocols and the algorithms.

Step 8 Configure the routing protocol to be used.

Step 9 Click Save to save the configuration to the device.

Configure a DMVPN Fully Meshed Topology

The dynamic spoke-to-spoke option allows you to configure a DMVPN fully meshed topology. In this topology, you can configure the router as a spoke, capable of establishing a directIPsec tunnel to other spokes in the network.

To configure a DMVPN Fully Meshed topology, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Choose the device from the list or click Add to create a new device, then configure the device.

Step 3 After selecting the device, click Configuration. The Feature Configuration pane appears.

Step 4 Expand the Security folder, and then click DMVPN. Click the Add to create the DMVPN tunnel with fully meshed topology.

Step 5 In the Create DMVPN Tunnel configuration page, select the Full Mesh radio button to configure the network type as full mesh topology.

Step 6 Repeat Step 6 through Step 8 in the Configure a DMVPN Hub and Spoke Topology section.

Step 7 For Fully Mesh spoke topology, in the NHS Server Information area, add the next hub server information, such as the IP Address of Hub's physical interface and the IP address of Hub's tunnel interface.

Step 8 Click Save to save the configuration to the device.

Configure a DMVPN Cluster Topology

To configure a cluster topology, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 Feature Configuration pane, expand the Security folder, and then click DMVPN. Click Add to create the DMVPN tunnel.

Step 4 From the Create DMVPN Tunnel configuration page, select Spoke radio button to configure the device role as a spoke.

Step 5 Repeat Step 6 through Step 8 in the Configure a DMVPN Hub and Spoke Topology section.

Note The device must be running IOS version of 15.1(2)T or later.

Step 6 Click Add Row to configure the cluster related information, and add the Cluster-ID and Maximum Connection values.

Step 7 Click Expand Row (next to the radio button) and click Add Row to add the NHS server information.

Step 8 Enter the NHS server, the GRE Tunnel IP addresses, and the Priority of this NHS server. Click Save to save the NHS server entry configuration.

Step 9 Click Save to save the NHS server group information.

Step 10 Click Save again to save the NHS group information with the cluster configuration. This will automatically populate the NHS server IP address in the table.

Delete a DMVPN Tunnel from a Device

To delete a DMVPN tunnel, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.
Step 2 Choose the device from the list to delete the DMVPN tunnel. If the device is not added, click Add to add the device.
Step 3 After selecting the device, click Configuration. The Feature Configuration pane appears.
Step 4 Expand the Security folder, and then click DMVPN. The available tunnel is displayed.
Step 5 Select the tunnel, and click Delete.
Step 6 Click Yes on the warning message to delete the selected tunnel.
Step 7 Click No on the warning message if you do not want to delete the selected tunnel.
Step 8 Click Cancel to cancel all of the changes that you have made without sending them to the router.

Configure QoS for a Device

To enable or disable QoS for a device follow the below steps.

Step 1 Choose Configuration > Network > Network Devices.
Step 2 Click on the device name for which you want to enable QoS, then select App Visibility & Control > QoS.
Step 3 Select the QoS capable interface and click Enable QoS.
Step 4 Check the Enable QoS on Ingress check box or Enable QoS on Egress check box or both the check boxes depending on your requirement.
Step 5 If you select Enable QoS on Ingress, choose a profile from the Select Profile drop-down list and click OK.
Step 6 If you select Enable QoS on Egress, do the following:
a) Click theClassify based on profile radio button and choose a profile from the Select Profile drop-down list.
b) For QoS scheduling, choose a Scheduling action based on profile from the Select Profile drop-down list.

Note You must choose the same profile, if you have chosen both Enable QoS on Ingress and Enable QoS on Egress in Step 4.

Step 7 Click the CLI Preview tab to preview the QoS configuration before deployment.
Step 8 Click Deploy.
Step 9 To disable QoS for a device, do the following:
a) Click Disable QoS and select on which direction (ingress/egress) to remove QoS configuration from the device.
b) Click Deploy.

Alternately, you can also enable or disable QoS for a device from Services > Interface Configuration.

Configure IPSec Topologies Using GETVPN

A Group Encrypted Transport VPN (GETVPN) deployment has three primary components: Group Member, Key Server, and Group Domain of Interpretation protocol. Group Members encrypt and decrypt the traffic, and Key Server distributes the encryption key to all group members. The Key Server decides on a single data encryption key for a given lifetime. Because all Group Members use the same key, any Group Member can decrypt the traffic encrypted by any other Group Member. GDOI protocol is used between the Group Member and Key Server for group key and group Security Association (SA) management. A minimum one Key Server is required for a GETVPN deployment.

Unlike traditional IPsec encryption solutions, GETVPN uses the concept of group SA. All members in the GETVPN group can communicate with each other using a common encryption policy and a shared SA. Therefore, there is no need to negotiateIPsec between Group Members on a peer-to-peer basis, thereby reducing the resource load on the Group Member routers.

Group Member

The Group Member registers with the Key Server to get the IPsec SA that is necessary to encrypt data traffic within the group. The Group Member provides the group identification number to the Key Server to get the respective policy and keys for this group. These keys are refreshed periodically by the Key Server, before the current IPsec SAs expire, so that there is no traffic loss.

Key Server

The Key Server is responsible for maintaining security policies, authenticating Group Members and providing a session key for encrypting traffic. Key Server authenticates the individual Group Members at the time of registration. Only after successful registration can the Group Members participate in a group SA.

A Group Member can register at any time and receive the most current policy and keys. When a Group Member registers with the Key Server, the Key Server verifies the group identification number of the Group Member. If this identification number is valid, and the Group Member has provided valid Internet Key Exchange (IKE) credentials, the Key Server sends the SA policy and the keys to the group member.

The keys sends two types to Group Member: the Key Encryption Key (KEK) and the Traffic Encryption Key (TEK). The TEK becomes part of the IPsec SA with which the group members within the same group encrypt the data. The KEK is used to secure rekey messages between the Key Server and the Group Members.

The Key Server sends out rekey messages either because of an impending IPsec SA expiration or because the security policy has changed on the Key Server. Keys can be distributed during rekey using either multicast or unicast transport. the multicast method is more scalable because keys need not be transmitted to each group member individually. Unlike in unicast, the Key Server will not receive acknowledgment from the Group Member about the success of the rekey reception using the multicast rekey method. Usign the unicast rekey method, the Key Server will delete a Group Member from its database if the Group Member does not acknowledge three consecutive rekeys.

Group Domain of Interpretation

Group Domain of Interpretation protocol is used for Group key and group SA management. Group Domain of Interpretation uses Internet Security Association Key Management Protocol (ISAKMP) for authenticating the Group Members and Key Servers. All of the standard ISAKMP authentication schemes like RSA Signature (certificates) and preshared key can be used for GETVPN.

For more information on GETVPN, See http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/deployment_guide_c07_554713.html.

Configure GETVPN Group Members

Use the Add GroupMember configuration page to configure a GETVPN group member.

To create a GETVPN group member, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security folder, and then click GETVPN-GroupMember. Click Add to create the GET VPN group member.

Step 4 In the Add GroupMember dialog box, choose the General tab, and enter the Group Name and Group Identity. Choose the Registration Interface from the drop-down list.

Step 5 Enter the Primary Key Server and Secondary Key Server IP addresses. Click Add Row or Delete to add or delete the secondary key server IP addresses.

Note The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizes with the secondary key servers. The server with the highest priority is elected as a primary key server.

Step 6 Click the row or field to edit the secondary key server IP address.

Step 7 Click Save to save the configuration.

Step 8 In the Add Group Member dialog box, choose the Advanced tab, and choose the Local Exception ACL and Fail Close ACL from the drop-down list.

If the Fail Close feature is configured, all of the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself.

Step 9 Choose the Migration tab, and select the Enable Passive SA check box to enable passive SA. Use this option to turn on the Passive SA mode for this group member.

Step 10 Click OK to add the Group member in the table. To display the commands, click CLI preview. After the scheduled deploy is completed, the configuration is applied on the device.

Configure GETVPN Key Servers

Use the Add KeyServer configuration page to configure the GETVPN key server.

To create a GETVPN key server, follow these steps:

SUMMARY STEPS

1. Choose Inventory > Device Management > Network Devices.
2. After choosing the device from the list, click Configuration. The Feature Configuration pane appears.
3. In the Feature Configuration pane, expand the Security folder, and then click GETVPN-KeyServer. Click Add to create the GETVPN key server.
4. In the Add Key Server dialog box, choose the General tab, and enter the Group Name, Group Identity, WAN IP address, and Priority of this key server.
5. Enter the Co-operative Key Servers IP address. Click Add Row or Delete to add or delete the Co-operative key server IP address. Click the row or field, and edit the IP address.

6. In the Add KeyServer dialog box, choose the Rekey tab, and choose the Distribution method from the drop-down list.
7. In the Add KeyServer dialog box, choose the GETVPN Traffic tab, and enter the Traffic to be encrypted, Encryption Policy, and Anti Replay.
8. Click OK to add the Group member in the table. To display the commands, click CLI preview. After the scheduled deployment is completed, the configuration is applied on the device.

DETAILED STEPS

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security folder, and then click GETVPN-KeyServer. Click Add to create the GETVPN key server.

Step 4 In the Add Key Server dialog box, choose the General tab, and enter the Group Name, Group Identity, WAN IP address, and Priority of this key server.

Step 5 Enter the Co-operative Key Servers IP address. Click Add Row or Delete to add or delete the Co-operative key server IP address. Click the row or field, and edit the IP address.

Step 6 In the Add KeyServer dialog box, choose the Rekey tab, and choose the Distribution method from the drop-down list.

The distribution method is used to send the rekey information from key server to group members. When you choose the distribution method as multicast, specify the multicast address to which the rekey needs to be transmitted.

Step 7 In the Add KeyServer dialog box, choose the GETVPN Traffic tab, and enter the Traffic to be encrypted, Encryption Policy, and Anti Replay.

The access list defines the traffic to be encrypted. Only the traffic which matches the “permit” lines will be encrypted. Be sure not to encrypt certain traffic that should always be permitted even if the crypto sessions are not active.

Step 8 Click OK to add the Group member in the table. To display the commands, click CLI preview. After the scheduled deployment is completed, the configuration is applied on the device.

VPN Components

The Internet Key Exchange (IKE) is a standard method for arranging secure and authenticated communications. The IKE establishes session keys (and associated cryptographic and networking configuration) between two hosts across network. IKE policies protect the identities of peers during authentication.

IKE negotiations must be protected; therefore, each IKE negotiation begins by each peer agreeing on a common (shared) IKE policy. This policy states the security parameters that will be used to protect subsequent IKE negotiations. After the peers agree on a policy, the security parameters of the policy are identified by a security association established at each peer. These security associations are applied to all subsequent IKE traffic during the negotiation.

When negotiation begins, IKE looks for an IKE policy that is the same on both peers. The peer that initiates negotiation sends all of its policies to the remote peer. The remote peer looks for a match by comparing its own highest priority policy against the other peer’s received policies. A match is found when policies from both peers contain the same encryption, hash, authentication, and Diffie-Hellman (D-H) parameter values, and when the remote peer’s policy specifies a lifetime that is less than or equal to the lifetime of the policy it

is being compared to. If the lifetimes are not identical, the shorter lifetime from the remote peer's policy is used.

Related Topics

Configure VPN IKE Policies, on page 739
Configure VPN IPSec Profiles, on page 739
Configure VPN PreShared Keys, on page 740
Configure VPN RSA Keys, on page 740
Configure VPN Transform Sets, on page 741

Configure VPN IKE Policies

To configure IKE policies, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, Expand the Security folder, and then choose VPN Components > IKE Policies.

Step 4 Click Add Row to create the IKE policies.

Step 5 In the IKE Policies page, enter the Priority, Authentication, D-H Group, Encryption, Hash, and Lifetime.

For a description of the elements on the IKE Policies page, see Security > VPN Components > IKE Policies in the Cisco Prime Infrastructure Reference Guide.

Step 6 Select the Enable IKE and Enable Aggressive Mode check box to globally enable the IKE policies for your peer router and the aggressive mode.

Step 7 Choose the IKE Identity from the drop-down list.

Step 8 Enter the Dead Peer Detection Keepalive and Dead Peer Detection Retry time in seconds.

For a description of the elements on the IKE Policies page, see Security > VPN Components > IKE Policies in the Cisco Prime Infrastructure Reference Guide.

Step 9 Click Save to save the configuration, then click Save again to generate the CLI commands.

Configure VPN IPSec Profiles

The IPsec profiles, also called ISAKMP profiles, enable you to define a set of IKE parameters that you can associate with one or more IPsec tunnels. An IPsec profile applies parameters to an incoming IPsec connection identified uniquely through its concept of matching identity criteria. These criteria are based on the IKE identity that is presented by incoming IKE connections and includes IP address, Fully Qualified Domain Name (FQDN), and group the VPN remote client grouping.

The IKE Profile feature allows you to create an IPsec profile.

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, Expand the Security folder, and then choose VPN Components > IPsec Profile.

Step 4 Click Add Row to create the IPsec Profile.

Step 5 In the IPsec Profile page, enter the information such as Name, Description, and Transform Set, and the IPsec SA Lifetime.

Note When you edit a profile, you cannot edit the name of the IPsec profile. A transform set represents a certain combination of security protocols and algorithms. During the IPsec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow. A transform describes a particular security protocol with its corresponding algorithms

Step 6 Enter the IPsec SA Lifetime in seconds to establish a new SA after the set period of time elapses.

Step 7 To edit the IPsec profile parameters, click Field and edit the parameter of that IPsec profile.

Step 8 To delete the IPsec profile, select the IPsec Profile from the list, and click Delete.

Step 9 Click Save to save the configuration, then click Save again to generate the CLI commands.

Configure VPN PreShared Keys

The preshared Keys feature allows you to share a secret key between two peers. This key is used by the IKE during the authentication phase.

To create a preshared key, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, Expand the Security folder, and then choose VPN Components > Preshared Keys.

Step 4 Click Add Row to create the preshared key.

Step 5 In the Preshared Keys page, enter the IP Address, Host Name, Subnet Mask, and Preshared Keys.

Step 6 To edit the preshared key parameters, click the Field and edit the parameter of that preshared key.

Step 7 To delete the preshared key, choose the preshared key from the list, and click Delete.

Step 8 Click Save to save the configuration, then click Save again to generate the CLI commands.

Configure VPN RSA Keys

An RSA key pair consists of a public key and a private key. When setting up your Public Key Infrastructure (PKI), you must include the public key in the certificate enrollment request. After the certificate is granted, the public key is included in the certificate so that peers can use it to encrypt the data that is sent to the router. The private key is kept on the router and used both to decrypt the data sent by the peers and to digitally sign transactions when negotiating with the peers.

RSA key pairs contain a key modulus value. The modulus determines the size of the RSA key. The larger the modulus, the more secure the RSA key. However, it takes longer to generate, encrypt, and decrypt keys with large modulus values.

To create an RSA keys, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security folder, and then choose VPN Components > RSAKeys.

Step 4 Click Add Row to create the RSA keys.

Step 5 The Add RSA Keys dialog box appears.

Step 6 In the Add RSA Keys dialog box, enter the Label, Modulus, and Type.

Note For a modulus value between 512 and 1024, enter an integer value that is a multiple of 64. If you want a value higher than 1024, you can enter 1536 or 2048. If you enter a value greater than 512, key generation may take a minute or longer. The modulus determines the size of the key. The larger the modulus, the more secure the key, but keys with a large modulus take longer to generate, and encryption/decryption operations take longer with larger keys.

Step 7 Select the Make the Key exportable check box to generate the RSA as a exportable key.

Step 8 Click OK to save the configuration.

Step 9 To import the RSA key, click Import. The Import RSA Key dialog box appears.

Step 10 In the Import RSA Key dialog box, enter the label of the RSA key, Key type, and password to decrypt the key. If the key type is general-keys, signature or encryption, copy and paste the public and private key data that was saved.

Step 11 To import usage-key, enter the public and private key data of both the signature and encryption keys.

Step 12 Click Import to import the RSA key.

Step 13 To export the RSA key, choose the RSA key from the list and click Export. The Export RSA Key Pair dialog box appears.

Step 14 In the Export RSA Key Pair dialog box, enter the password to encrypt the RSA key and choose the encryption algorithm from the drop-down list.

Step 15 Click OK to display the exported keys.

Step 16 To delete the RSA key, choose the RSA key from the list, and click Delete.

Configure VPN Transform Sets

To define a transform set, specify one to three transforms. Each transform represents an IPsec security protocol (AH or ESP) plus the algorithm that you want to use. When the particular transform set is used during negotiations for IPsec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

To configure a transform sets, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 After choosing the device from the list, click Configuration. The Feature Configuration pane appears.

Step 3 In the Feature Configuration pane, expand the Security folder, and then choose VPN Components > Transform Sets.

Step 4 Click Add Row to create the transform sets.

Step 5 In the Transform Sets page, enter the Name and select the acceptable combination of security protocols and algorithm to configure the transform set.

Note The ESP encryption algorithm is used to encrypt the payload and the integrity algorithm is used to check the integrity of the payload.

Step 6 Specify the mode for a transform set:

- Transport—Encrypt data only. Transport mode is used when both endpoints support IPsec. Transport mode places the authentication header or encapsulated security payload after the original IP header; thus, only the IP payload is

encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets.

- Tunnel—Encrypt data and IP header. Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as a router to act as an IPsec proxy for multiple VPN users; tunnel mode should be used in those configurations.

Step 7 Click Save to save the configuration, then click Save again to save the configuration changes.

Control Firewall Policies Between Groups of Interfaces using Zone-Based Firewalls

The Zone-Based Firewall feature allows you to easily manage Cisco IOS unidirectional firewall policy between groups of interfaces known as zones.

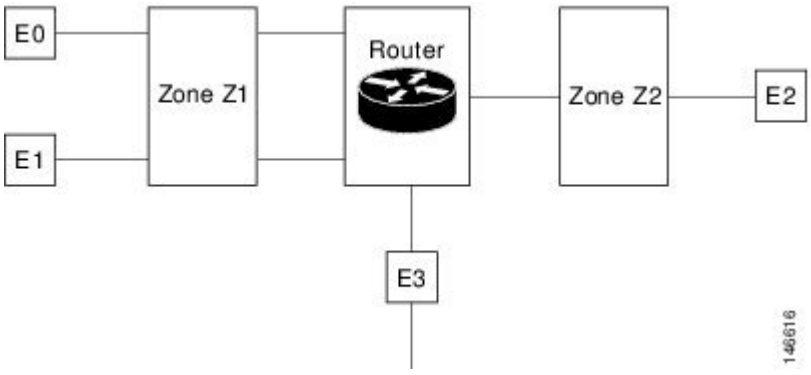
A zone is a group of interfaces that have similar functions or features. For example, on a router, Gigabit Ethernet interface 0/0/0 and Gigabit Ethernet interface 0/0/1 may be connected to the LAN. These two interfaces are similar because they represent the internal network, so they can be grouped into a zone for firewall configurations.

By default, the traffic between interfaces in the same zone is not subjected to any policy. The traffic passes freely.

When an interface is a member of a security zone, all traffic to and from that interface (except traffic going to the router or traffic going to another interface on the same zone) is dropped.

To permit traffic between interfaces that belong to different zones, a firewall policy with concrete rules must be pushed to the device. If the policy permits the traffic between these two zones (through inspect or pass actions) traffic can flow through the zones. Figure 48-1 describes the security zone.

Figure 26: Security Zone Diagram



The following describe the relationships between the interfaces and security zones shown in the above figure.

- Interfaces E0 and E1 are members of the security zone Z1.
- Interface E2 is a member of the security zone Z2.
- Interface E3 is not a member of any of the security zone.

In this scenario, the following situations exist:

- Traffic flows freely between interfaces E0 and E1 because they are members of the same security zone (Z1).
- If no policies are configured, traffic will not flow between zones (for example, E0 and E2, E1 and E2, E3 and E1, and E3 and E2).
- Traffic can flow between interface E0 or E1 and E2 only when an explicit policy is configured to permit the traffic between zone Z1 and zone Z2.

Traffic can never flow between E3 and interface E0, E1or E2 because E3 is not a part of any security zone.

supports the zone-based firewall feature on Cisco ASR, ISR, and CSR routers. Using , you can configure a zone-based firewall policy template and deploy it to multiple devices. After you deploy the zone-based configuration, you can navigate to the Device Work Center to view the deployed firewall configuration on a specific device.

To monitor the zone-based firewall, check the Zone-Based Firewall Monitor Hits capability on the Device Work Center or the syslog feature, which supports zone-based firewall syslog messages.

can configure Zone-Based Firewall either through CLI (over Telnet or SSH) or through WSMA. Zone-Based Firewall can be configured through WSMA in a more efficient and robust method and we recommend that you use the WSMA protocols for configuring Zone-Based Firewall. For more information on using WSMA with , see Set Up Devices to Use AVC Features with WSMA.

Configure a Zone-Based Firewall: Workflow

To configure a zone-based firewall on more than one device, use a zone-based template to make the changes. For zone-based firewall templates, you must first design the zone-based firewall in the network by defining the zones in the network. In , zones are represented by interface role global object, which dynamically selects the list of interfaces that belong to the zone. Next, define and create network objects in the firewall environment. The Zone-based firewall feature supports only IPv4 network in . (IPv6 is not supported.)

Note The Zone-Based Firewall feature is supported on the following: ASR platform from Cisco IOS-XE Release 15.2(2)S or later, ISR G2 platform from Cisco IOS Release 15.0(1)M or later, ISR G3 platform from Cisco IOS-XE 15.3(2)S Release or later, CSR platform from Cisco IOS-XE 15.3(1)S Release or later, Cisco ISRv platform from Cisco IOS-XE Release 16.3 or later, and Cisco ISR 1000 platform from Cisco IOS-XE Release 16.6.1 or later.

To configure a zone-based firewall template:

1. Define the zones. A security zone is defined as an interface role.
2. Define the IPv4 network objects.

   Note 2.0 supports only IPv4 network objects.

3. Design a firewall policy and deploy it to multiple devices (for more information, see Create a Policy Rule for a Single Device's Zone-Based Firewall).
4. Validate the configuration for a specific device (see Control Firewall Policies Between Groups of Interfaces using Zone-Based Firewalls).
5. Modify the global objects and template configuration (see Configure the Policy Rules for a Zone-Based Firewall).

6. Monitor the policy rules (see Monitor and Troubleshoot Policy Rules for a Single Devices Zone Based Firewall, on page 747).
7. Monitor the syslog messages.

To modify security zones, IPv4 network objects, and firewall policies, edit the firewall policy and redeploy it to the relevant devices.

Configure the Policy Rules for a Zone-Based Firewall

After you create a shared policy objects, create a zone-based firewall policy rules template.

To create a Zone-Based Firewall Policy Rules template, follow these steps:

Step 1 Choose Configuration > Templates > Features & Technologies > Security > Zone Based Firewall > Policy Rules.

Step 2 In the Template Basic area, enter a name and a description in the appropriate fields.

Step 3 In the Validation Criteria area, choose a Device Type from the list and enter the OS Version.

Step 4 Enter the required fields. For descriptions of the template parameters, see the Cisco Prime Infrastructure Reference Guide.

Step 5 Click Save as New Template.

Remove the Zone-based Firewall Configuration Using CLI Templates

Users can remove the zone-based firewall configuration from the devices using the CLI templates by performing the steps provided below:

Step 1 Navigate to Configuration > Templates > Features & Technologies.

Step 2 Expand the CLI Templates tree and select the System Template-CLI option.

Step 3 Select the Delete_ZBFW_Configuration template.

Step 4 You must sync-up the devices for which you wish to remove the zone-based firewall configuration and then click the Deploy button.

Step 5 Select a devices from which you wish to remove the zone-based firewall configuration.

The list of devices configured with the zone-based firewall are displayed in the CLI Preview pane.

Step 6 You must sync-up the devices again to ensure the zone-based firewall configuration is removed..

Configuring the Policy Rules for a Zone-Based Firewall on Single Devices

To configure a zone-based firewall on a single device, use Device Work Center zone-based configuration to make the changes.

Create a Security Zone for a Single Device's Zone-Based Firewall

To create a security zone, follow these steps:

Note The Zone Based Firewall feature is supported on the ASR platform on Cisco IOS-XE Release 15.2 (2)S or later, ISR G2 platform on Cisco IOS release 15.0 (1) M or later, ISR G3 platform on Cisco IOS-XE Release 15.3(2)S or later, and CSR platform on Cisco IOS-XE Release 15.3(1)S.

Before you begin

Step 1 Choose Inventory > Device Management > Network Devices, then click on the device.

Step 2 In the Configuration tab, expand the Security subfolder.

Step 3 In the Security subfolder, expand the Zone Based Firewall > Common Building Blocks, then click Zones.

Step 4 Click Add Zone to create the security zone.

Step 5 Select a Zone Name.

Step 6 (Cisco ASR devices only) To make this the default zone for Cisco ASR devices, click Enable Default.

The default zone will host all of the interfaces that are not related to any zone.

Step 7 Click OK to save the configuration.

Step 8 Select the VRF of the zone.

a) Select a VRF before assigning interfaces to the security zone. Only the interfaces that are assigned to the selected VRF can be assigned to the zone.

a) If the user selects the "global VRF", only interfaces which are not assigned to any VRF can be assigned to the zone.

Step 9 To assign the interfaces to the security zone, click the down arrow icon. The Interface Object Selector dialog box appears.

a) In the Interface selector dialog box, select the Interface check box to select the interface from the list (can be multiple selection).

b) Click OK to save the configuration or click Cancel to cancel all of the changes that you have made without sending them to the router.

Step 10 In the Advanced options column, click Configure. The Advanced Parameters Configuration dialog box appears.

Step 11 Define a set of advanced parameters which would be applicable for the inspected traffic that goes through the interfaces that belongs to the zone. For each parameter, select the check box to the left of the parameter name to override the default value for the parameter and then select the new value for the parameter. (Optional) In the Advanced Parameters Configuration dialog box, do the following:

Note Advanced Parameters option is supported only on ASR1K series devices.

a) Select the Alert check box and select the On radio button to set the alert. Select the Maximum Destination check box to set the maximum destination. Select the TCP SYN-Flood Rate per Destination check box to set the TCP flood rate.

b) Select the Maximum Destination check box to set the maximum destination.

c) Select the TCP SYN-Flood Rate per Destination check box to set the TCP flood rate.

d) Select the Basic Threat Detection Parameters check box and select the On radio button to configure the FW drop threat detection rate, FW inspect threat detection rate, and FW SYN attack threat detection rate.

Step 12 Click:

- OK to save the configuration.

- Cancel to exit without saving.
- Cancel to exit without saving.

Step 13 To edit the existing security zone parameters, select the zone, and click Edit in the Advance options column. The Advanced Parameters Configuration dialog box appears.

Step 14 In the Advanced Parameters Configuration dialog box, edit the values and click Save to save the changes. When you hover your mouse over the Advanced Options icon, the configured parameters will be displayed in the quick view window.

Step 15 Enter the description for the zone, then click Save.

Create a Policy Rule for a Single Device's Zone-Based Firewall

To create a policy rule, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices, then select a device.

Step 2 In the Feature Configuration pane, expand the Security subfolder.

Step 3 In the Security subfolder, expand the Zone Based Firewall and then click Policy Rules. The Policy Rules page appears.

Step 4 To edit an existing policy rule, choose one of the following options:

- Click the Rules parameters row and edit the parameters.
- Select the check box to select the rule, and then click Edit. The selected Rule opens for edit. You cannot edit the name of the policy rule.

  Note You can specify the Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) port range in the firewall rule service. When you add a new rule or edit an existing rule under the Service column, click object selector to assign the TCP / UDP, and click OK. You can define the port numbers in the text box that appears near the protocol icon. Also, you can define the port range in the format of <start-port-number>-<end-port-number>, and this range can be configured for that specific protocol (TCP or UDP).

- You can re-order firewall rules by dragging a rule and dropping it in a different location.

Step 5 From the Policy Rules page, click Add Rule and complete the fields. When you add a rule, you can place a rule at the top or bottom of the policy or after/before an existing rule. Firewall Rules are processed according to their order. To control the order of the rules, select the location of the rule in the table and use Add Top or Add Bottom option to add the rule to the top or the bottom of the table. Select a rule and use Add After or Add Before option to add the rule before or after an existing rule.You can place a rule at any given location and later use drag and drop to change its location.

Step 6 (Optional) Enter the firewall rule name. If you do not provide the name for the firewall rule, the system generates a name for the firewall rule. You cannot use these formats rule_<number> or EMS_rule_<number> to create the firewall rule name (For example, rule_1). These are system reserved formats.

Step 7 Select the source and destination zones for the rule, the rule is applicable only for traffic that flows from the source zone to the destination zone. Note that the source and destination zones must be different.

Step 8 To add the source and the destination IP address, click the add icon. The Source/Destination IP address dialog box appears.

a) In the Source/Destination IP address dialog box, select the Any check box to set the value to any.
b) Enter the Source/ Destination IP addresses.

c) Click the + button to add the new IP address and the subnet.
d) Click the - button to remove an IP/subnet.
e) Click OK to save the configurations or click Cancel to cancel all of the changes that you have made without sending them to the router.

Step 9 (Optional) Set the Service values. To add or remove the service, click the down arrow icon. The Firewall Service dialog box appears. You can also select a predefined Service. For creating services, see Create a Policy Rule for a Single Device's Zone-Based Firewall.

a) In the Firewall Service dialog box, select the service or port-based application check box to select the application or the service for the rule.
b) Select specific TCP / UDP ports by selecting TCP or UDP, close the window and enter the list of ports to be used in the text box that appears next to the TCP or UDP icon. For viewing port-based applications, see Assign Application TCP/UDP Ports for a Single Device's Zone-Based Firewall.
c) Use the navigation arrow buttons to navigate backward.
d) Click OK to save the configurations.

Step 10 Select the appropriate action. The options are: Drop, Drop and Log, Inspect, Pass, and Pass and Log.

Step 11 If you select the action to inspect, click Configure in the Advance options column. The Advanced Parameters Configuration dialog box appears.

Step 12 In the Advanced Parameters Configuration dialog box, do the following:

a) To customize the device default value, select the Parameter check box and set the new value.
b) To apply the device default value, unselect the Parameter check box.
c) To view the firewall rule default parameters, see Configure Default Parameters for a Single Cisco ISR Device's Zone-Based Firewall.
d) When you hover your mouse cursor over the Advanced Options icon, the configured parameters are displayed in the quick view window.

Step 13 Click Save to apply the rule to the device. For description of the elements, see the Cisco Prime Infrastructure Reference Guide.

Monitor and Troubleshoot Policy Rules for a Single Devices Zone Based Firewall

The monitoring feature allows you to monitor policy rules. You can identify the most-used rules, and you can troubleshoot a specific rule and verify hits for the selected rule.

To monitor policy rules, follow these steps:

Step 1 Choose Inventroy > Device Management > Network Devices, then select a device.

Step 2 In the Feature Configuration pane, expand the Security folder.

Step 3 In the Security subfolder, expand the Zone Based Firewall and then click Policy Rules. The Firewall Rules Page appears.

Step 4 In the Firewall Rules page, click Hit Counters and use the one of the following options to analyze the sessions and packets hit counters for the firewall rules.

Step 5 Click the Show All option to view the packets and sessions counters for the firewall rules. The packets and sessions counters are displayed in two separate columns.

Note When you select the Show all option, the system will display a warning message stating that it may take more time to complete this operation. Sessions hit counters are not applicable for Drop/Pass rules. Similarly, packet hit counters are not applicable for Inspection rules.

Step 6 To know the time of last update for the rules, hover the mouse cursor over the column names or click the Last Update Time option in the Hit Counters.

Step 7 Click the Show for selected rules option to show the hit counters for a specific rule or a couple of selected rules. The hit counters would be displayed in a popup dialog box with the refresh button which allows the quick refresh of the data.

Step 8 Use the predefined filters options available in the top-right corner of the table to display the rules at the top or bottom based on the packets/sessions counts.

Step 9 Click Reset All Counters to discard all of the rules counters on the device. The application will display a warning message before resetting the rules counters.

Create a Service Group for a Single Device's Zone-Based Firewall

You can create, update or delete a service groups. Service group provides an option to group together several port-based applications to logical groups which could be used in firewall policies.

For example, you can define a browsing service-group object and assign both HTTP and HTTPS applications to it. Then you can use this browsing service-group in firewall rules to permit or deny browsing traffic, rather than selecting both HTTP and HTTPS in those rules.

To create a service group, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices, then select a device.

Step 2 In the Feature Configuration pane, expand the Security subfolder.

Step 3 In the Security subfolder, expand the Zone Based Firewall > Common Building Blocks, and then click Service Groups. The Service Groups page appears.

Step 4 To create the Service Group:

a) In the Service Group page, click Add Service Group and enter the Service Group Name. You cannot change the name after creating the Service Group. Also, you cannot create a service group without an application (see Create Custom Applications to Monitor Their Performance).

b) To assign Applications, click the down arrow icon.

c) In the Applications dialog box, select the Applications check box to select one or more applications from the list, then click OK.

Step 5 To edit an existing Service Group, do one of the following:

- In the Service Groups page, click the Service Group parameters row and edit the parameters.
- Select the service group and click Edit. You can add new applications or remove an already selected application.
- To remove an application from the selected list, hover your mouse cursor over the application name and click X.

Step 6 Click Save to apply your changes to the device.

Assign Application TCP/UDP Ports for a Single Device's Zone-Based Firewall

You can assign or unassign the Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) ports to an application.

Note When you click Save in the following procedure, your changes are deployed on the device. You cannot review the requested operation or remove the request from the pending changes queue.

To assign or unassign TCP/UDP ports for an application, follow these steps:

SUMMARY STEPS

1. Choose Inventory > Device Management > Network Devices, then select a device.
2. In the Feature Configuration pane, expand the Security subfolder.
3. In the Security subfolder, expand the Zone Based Firewall > Common Building Blocks, and then click Port Mappings. The Port Application Mapping page appears.
4. To assign or unassign the TCP/UDP ports to an application, click the application and update its TCP/UDP ports value. The TCP/UDP Port values are assigned to the specific application.
5. Click Save to save the configurations.

DETAILED STEPS

Step 1 Choose Inventory > Device Management > Network Devices, then select a device.

Step 2 In the Feature Configuration pane, expand the Security subfolder.

Step 3 In the Security subfolder, expand the Zone Based Firewall > Common Building Blocks, and then click Port Mappings. The Port Application Mapping page appears.

Note The Port Application Mapping page displays the application name that is driven from the device.

Step 4 To assign or unassign the TCP/UDP ports to an application, click the application and update its TCP/UDP ports value. The TCP/UDP Port values are assigned to the specific application.

a) Assign port(s) by defining one or more ports separated by comma (For example: 1234, 2222 and so on).
b) Assign port(s) by defining the port range (For example: 1111-1118). You can also assign a combination of ports and port ranges.
c) Unassign port(s) by deleting the existing port values.

Step 5 Click Save to save the configurations.

Configure Default Parameters for a Single Cisco ISR Device's Zone-Based Firewall

To configure a default parameters, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices, then select a device.

Step 2 In the Feature Configuration pane, expand the `Security` subfolder.

Step 3 In the Security subfolder, expand the Zone Based Firewall and then click Default Parameters. The Default Parameters page appears.

Step 4 In the Default Parameters page, change the parameters value.

Note You can change the default parameters only on ISR devices.

Step 5 Click Save to save the configuration.

Assign an Interface to a Different Zone in a Single Device's Zone-Based Firewall

The interfaces view gives an overview of the interfaces on the device which are applicable for firewall inspection. The view allows viewing and modifying the assignment of those interfaces to security zones.

To assign or unassign an interface for a zone, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices, then select a device.

Step 2 In the Feature Configuration pane, expand the Security subfolder.

Step 3 In the Security subfolder, expand the Zone Based Firewall and then click Interfaces.

Step 4 In the Interface page, select the interface that you want to change and click the down arrow icon. The Zone dialog box appears.

Step 5 In the Zone dialog box, select the new security zone for the interface. If the selected interface is already assigned to a zone, you will get a warning message.

Step 6 Click Yes on the warning message if you want to change the assignment of that interface.

Step 7 To un-assign the interface from the specific zone, select the interface and delete the zone information.

Step 8 Click Save to save and apply your changes.

How to Transition Between the CLI User Interfaces in

The following figure illustrates how to transition between the and Linux CLI user interfaces on deployments running .

Add NAM Application Servers as Data Sources

supports various features to be configured on NAM, remotely. The NAM Application Servers feature enables you to configure the NAM device with Application servers.

To Configure the parameters of the Application servers, with NAM device, follow these steps:

Step 1 Choose Inventory > Device Management > Network Devices, then select a device.

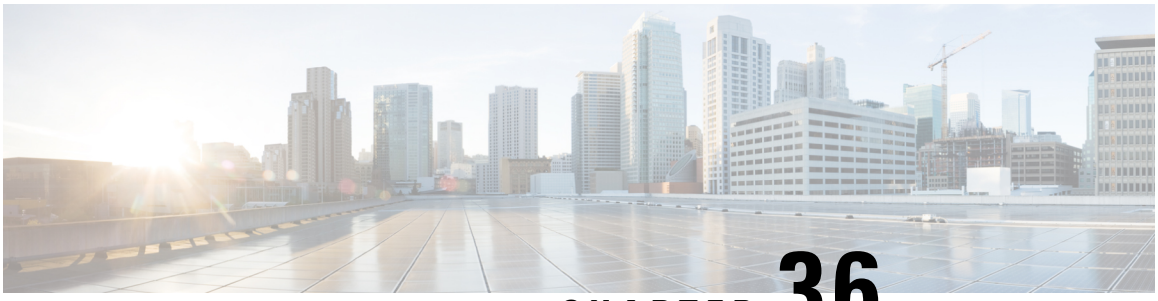
Step 2 Click Add.

Step 3 Enter the IP address of the server in Add Servers dialog box and click Add button inside the dialog box. The list of server IPaddresses are displayed under IP address column.

Step 4 Select the IP addresses of the servers to be deployed to the NAM device, then Click Add to NAM Server lists.

Step 5 Select the IP Address of one or more of the NAM devices in the Add Server(s) to NAM Server Lis dialog box, and click Add button within the dialog box.

The selected device IP addresses are displayed under Part of NAM Server List on column, and the server parameters get configured on the selected NAM devices.



CHAPTER 36

How Does Prime Infrastructure Ensure Consistent Application Experiences for WAN End Users?

Ensure Consistent Application Experiences for WAN End Users

can help ensure high-quality WAN end-user experiences across applications at multiple sites.

- View Application Key Performance Indicators for Sites
- Set Up the Application Performance Dashboard for WAN Optimization
- Identify Low-Performing WAN Applications, Clients, Servers, and Links
- View WAN Optimization Results
- View WAN Client-Server and Site-to-Site Optimized Traffic Flows

Note To use this feature, your implementation must include Assurance licenses.

Network operations staff must share a common data resource that gives them complete visibility into network performance data throughout every stage of the optimization cycle, including:

- Identifying the sites and applications that are candidates for optimization, so that network designers can plan where application optimization is critical (see View Application Key Performance Indicators for Sites).
- Establishing site and application performance baselines (see Set Up the Application Performance Dashboard for WAN Optimization).

performs baselining for key performance metrics and detects abnormal deviations of baselined values. The key performance metrics include:

- Server Response Time
- Client Transaction Time
- Network Round-Trip Time
- MOS score
- Jitters
- Packet loss
- Bytes sent/received

- Interface utilization
- CPU Utilization
- Memory Utilization

determines the baseline (mean) for each metric by taking the average values of the metric during the last 30 days. Average values are computed separately for each hour of the day for each monitored entity (such as interface, host, site, or application). For example, the baseline for HTTP response time of a given server between 9AM to 10AM today will be different from the baseline of the same server between 7PM to 8PM yesterday.

also computes the metrics' standard deviations using the last 30 days of data. Similar to averages, standard deviations are computed separately for each hour of the day for each monitored entity.

- Post-implementation validation that WAN performance and application stability have actually improved (see View WAN Optimization Results).

Because the mean and standard deviation of each metric vary over time, continuously reevaluates the thresholds used to compute the health scores (adaptive thresholds). computes baselines and thresholds every hour, and evaluates health scores every five minutes. In each interval:

1. Health scores are computed for every application-site combination.
2. These health scores are aggregated to derive the overall health of each business-critical application (across all sites) and overall health of each site (across all business-critical applications).

When aggregating across sites/applications, the worst scores are used. For example, if any business-critical application of a given site is rated "red," that site is also rated "red" for that interval. See Customize Service Health Rules for Application Performance for more information.

- Ongoing monitoring and troubleshooting of the optimized flows (see View WAN Client-Server and Site-to-Site Optimized Traffic Flows).

Using the baseline means and standard deviations, can monitor application and service health issues by detecting abnormal deviations of key metrics from their baselined values and assign a health scores (red, yellow, or green) for each application and site for each monitoring interval.

- A red score indicates a highly abnormal deviation from baseline (deviations from baselines with a probability of less than 0.1%).
- A yellow score indicates a mildly abnormal deviation (deviations with a probability of less than 1%).
- A green score indicates that the metric is within its normal range.
- A gray score indicates there is insufficient data for a site/application.

offers a consistent data resource for each of these stages in performance optimization.

View Application Key Performance Indicators for Sites

Choose Services > Application Visibility & Control > Service Health to view the sites and their business critical applications. Each application for a site is given a score for each of the KPIs (Key Performance Indicators) that are available in the system:

- Traffic (megabits per second)
- Client Experience (varies based on application type: average transaction time for transaction-based applications such as HTTP, or MOS code for real-time applications such as RTP)
- Network Performance (average network time for HTTP, jitter and Package Loss for RTP)
- Application Response (applicable only for transaction-based applications such as HTTP)

The KPI scores can come from multiple data sources; scores are computed across all data sources for all of the KPIs, and the overall score in the main dashboard is an aggregate of these scores. Scores are assigned as red, yellow, or green based on the warning and critical threshold values assigned in Health rules page. You can navigate to this page by clicking Launch Health Rules in the Services > Application Visibility & Control > Service Health page.

For data to be displayed in Service Health, there must be at least one hour of data. After the first hour, the previous hour's data is overlaid on the data line as the historical data for the next hour. After the first day, standard deviation and mean are based on the hourly data for the previous day.

These scores are stored for seven days. When you view the data for a previous day, the maximum moving time interval is six hours (you can look at up to six hours of data at a time).

Create Custom Applications to Monitor Their Performance

Choose Services > Application Visibility & Control > Applications and Services to create and manage custom applications and services. Services are groups of applications. provides a default set of applications and services consistent with the Cisco NBAR standard. (See NBAR Home page for more information.)

The All Applications table shows the list of all predefined and user-defined applications. You can configure some of the applications as Business Critical applications.

You can create custom applications that contain the definitions you require and which are not available (either from the device or from). After you create an application, you can deploy the application to the supported devices. Deploying the application definition to the device makes Netflow exported data consistent with and other management tools.

If you deploy a custom application to a device and later want to remove it, you must undeploy the application using the Applications and Services option. If you delete the custom application from only, the custom application remains active on the device.

Applications without definitions are displayed as "unknown."

Custom applications are organized under services; services are organized by category and subcategory to align with the Cisco NBAR standard. For more information about NBAR, see NBAR Home page.

To create a custom application, follow these steps:

Step 1 Choose Services > Application Visibility & Control > Applications and Services.

Step 2 Click Create.

Step 3 Complete the required General and Attributes fields.

Step 4 Choose the traffic classification rule from the Rule drop-down list.

Note Protocol is applicable for NAM and NBAR2 supported IOS devices.

Server/DSCP is applicable for NBAR2 supported IOS devices ver 15.5(2) and above.

URL - Applicable for NAM ver 6.0(2) above and NBAR2 supported IOS devices.

NAM Server IP Address - Applicable for NAM 6.0(2) and above devices only.

RTP Payload Type - Applicable only for Prime Infrastructure.

Step 5 Click the Condition drop-down list and enter the required values in the applicable fields based on the chosen rule.

Step 6 Click the Plus icon to add more traffic rules and conditions.

Step 7 Click Create.

The newly created application appears in the All Applications table.

Step 8 Choose the newly created application and click Deploy.

Note You can undeploy existing application. To undeploy, select the custom application from Application and Services and click Undeploy.

Step 9 Choose the devices on which you want to deploy this application and click Submit.

Step 10 Click View Jobs to view the status of the deployment job.

Step 11 In the device selection pane of the Application Deployment dialog box, you can:

- Select a parent group or a child group to deploy all the devices listed inside the group.

  Note You must select only one parent group at a time. However, you can select one or more child groups within a parent group.

- Expand a group and select one or more devices individually.
- View the number of devices selected in the CLI Preview screen.

  Note Expanding a parent or child group and then selecting the respective check box will only select the initial set of devices listed within and not the successive devices. You must first select the check box of a parent group and then expand it to select all the underlying devices.

View Service Health Using the AVC Service Health Window

Choose Services > Application Visibility & Control > Service Health, then click Health Summary. changes to display the heath information in a timeline.

The Service Health window allows you to view the information shown in the figure below:

The information displayed in the Service Application Visibility and Control Service Health Window is described below:

Table 77: Services Application Visibility and Control Service Health Window Descriptions

1	Lists the location groups for the filter you selected.
2	Click to toggle between the Health Summary and the Health Timeline.
3	Provides quick links to: • Health Rules page, where you can modify the health rule settings as necessary for your network. • View and modify the currently defined business critical applications.
4	Displays the filter you're currently viewing. You can click any filter to remove it and refresh the window.
5	Lists the business critical applications.
6	Colored symbols indicate good, warning, and critical threshold values based on the health rule setting specified in Health Rules page.
7	Move the slider to specify the time range in which you want to view service health information.

Customize Service Health Rules for Application Performance

The data displayed in Services > Application Visibility & Control > Service Health is computed using health rules. You can customize the health rules by clicking the desired row and editing the Critical and Warning values.

- Critical—turns red when the data value exceeds the specified Critical value.

- Warning—turns yellow when the data value exceeds the Warning value.

If the health rule does not exceed the specified Critical or Warning values, it is green.

For example, for Traffic Rate, you might specify the T1 the baseline value of 100 Mbps for a given site, application, and datasource, and the standard deviation value of 20 Mbps.

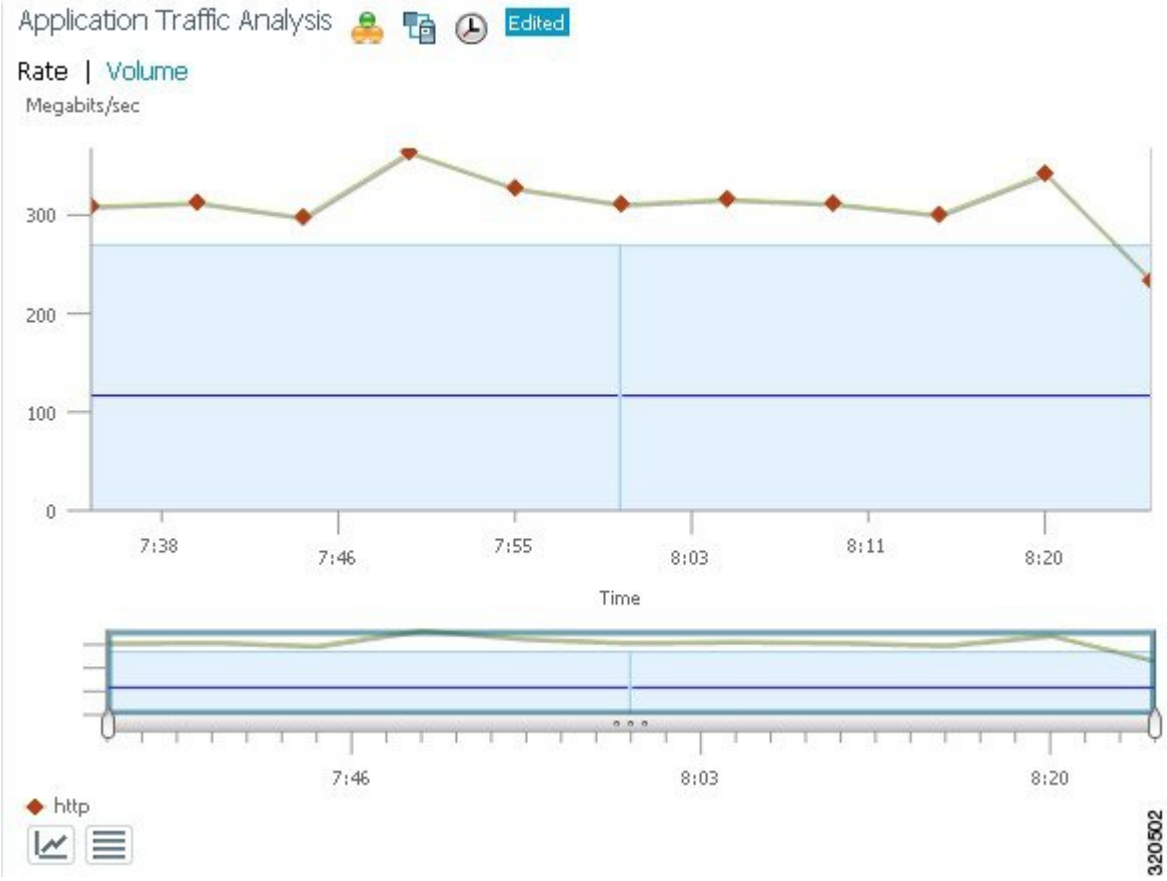
If the Traffic Rate exceeds 161.8 Mbps, which is 100+(3.09 x 20), you see a red bar indicating a critical warning.

You can click any of the colored bars to get further details.

Enable Baselines for Computing Application Performance

Standard deviation and mean values are used to compute the scores in Service Health. Baselining is not enabled by default. When baselining is enabled:

- The blue box indicates the standard deviation.
- The blue line indicates the mean value for that hour.



To enable baselining, follow these steps:

Step 1 Choose Dashboard > Performance > Application.

Baselining is supported by these dashlets:

a. Application Traffic Analysis—Shows the aggregate bandwidth rate/volume for a site/enterprise one application, service, or set of applications.

b. Application ART Analysis—Shows the response times for a transaction.

Step 2 To enable application traffic analysis baselining:

a) Open the Application Traffic Analysis dashlet, hover your cursor over the dashlet icons and click Dashlet Options.
b) Select the Baseline check box and save your changes.

Step 3 To enable application response time analysis baselining:

a) Open the Application ART Analysis dashlet, hover your cursor over the dashlet icons and click Dashlet Options.
b) Choose a metric from the Metric Type drop-down list.

If you choose the Server Response Time metric, you can select an individual Application Server to see what the response time of that server has been in the past.

c) Select the Baseline check box and save your changes.

Set Up the Application Performance Dashboard for WAN Optimization

Follow these steps to establish the standard performance characteristics of your candidate applications and sites before implementing WAN optimizations.

Step 1 Choose Dashboard > Performance > Application.

Step 2 Add the following dashlets (see Add Dashlets to Dashboards, on page 10) to this page:

- Worst N Clients by ART Metrics
- Worst N Sites by ART Metrics
- Application Server Performance
- Application Traffic Analysis

Step 3 Use these dashlets to establish the performance characteristics of your optimization candidates as currently configured.

- Worst N Clients by ART Metrics: For the worst-performing clients and applications: Maximum and average transaction times, and 24-hour performance trend.
- Worst N Sites by ART Metrics: The same information for the worst-performing sites and applications.
- Application Server Performance: For all application servers: the maximum and average server response time, and a 24-hour performance trend.
- Application Traffic Analysis: Gives 24-hour application traffic metrics in bytes per second and packets per second. Calculates statistical mean, minimum, maximum, median, and first and second standard deviation for the period.

You can sort by any column in any dashlet by clicking the column heading. You can also filter the data in the dashlets by Time Frame, Site, and Application.

Step 4 Click the Site tab and use Top N Applications, Top N Devices with Most Alarms, Top N Clients and Worst N Clients by ART Metrics as you did in Step 3.

Identify Low-Performing WAN Applications, Clients, Servers, and Links

Follow these steps to identify your network's lowest performing applications, clients, servers, and network links.

Step 1 Choose Dashboard > Performance > WAN Optimization.

Step 2 Add the following dashlets (see Adding Dashlets) to this dashboard.

- Application Traffic
- Server Traffic
- Client Traffic
- Network Links

Step 3 Using these dashlets, identify the optimization candidates.

- All of the dashlets show the current traffic rate (in bytes per second), average number of concurrent connections, and average transaction time in milliseconds, for every application, client, server, or network link.
- Network Links also shows the sites for that client and server endpoints of each link, and the average length of time that the link exists.
- Server Traffic shows both the server IP address and the application that it serves.

Step 4 Sort and filter the performance data as needed.

- To sort on any column in any dashlet, click the column heading.
- To filter the data displayed in all of the dashlets by Time Frame, Site, or Application, enter or select the filter criteria that you want on the Filters line and click Go.
- To filter within a dashlet, click its Filter icon and specify a Quick or Advanced Filter, or use a Preset Filter.

Step 5 For a quick report of the same data:

a) Choose Report > Report Launch Pad.
b) Specify filter and other criteria for the report, then click Run.

View WAN Optimization Results

After you have deployed changes at candidate sites, follow these steps to validate the return on your optimization investment.

Step 1 Choose Dashboard > Performance > WAN Optimization.

The dashlets on this page show:

- Transaction Time (Client Experience)—Graphs average client transaction times (in milliseconds) for the past 24 hours, with separate lines for optimized traffic and pass-through traffic (in which optimization is turned off). With optimization enabled, you should see a drop in the optimized traffic time when compared to the pass-through time.
- Average Concurrent Connections (Optimized vs Passthru)—Graphs the average number of concurrent client and pass through connections over a specified time period.
- Traffic Volume and Compression Ratio—Graphs the bandwidth reduction ratio between the number of bytes before compression and the number of bytes after compression.
- Multi-Segment Network Time (Client LAN-WAN - Server LAN)—Graphs the network time between the multiple segments.

Step 2 You can filter the data in the dashlets by Time Frame, Client Site, Server Site, and Application.

Step 3 To generate a report:

a) Choose Tools > Reports > Report Launch Pad, then choose Performance > WAN Application Performance Analysis Summary.

b) Specify the filter and other settings for the report, then click Run.

View WAN Client-Server and Site-to-Site Optimized Traffic Flows

Follow these steps to monitor optimized WAN traffic.

Step 1 Choose Dashboard > Performance > WAN Optimization.

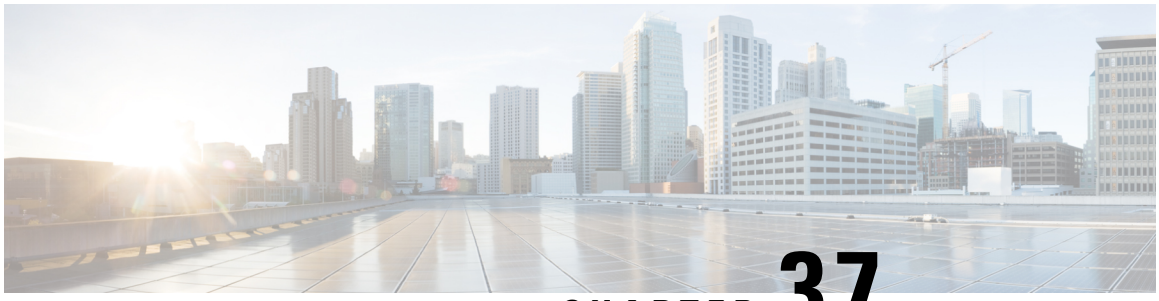
Step 2 In the Multi-Segment Analysis dashlet, click View Multi-Segment Analysis.

Step 3 Click the Conversations tab to see individual client/server sessions, or the Site to Site tab to see aggregated site traffic. For each client (or client site) and server (or server site) pair and application in use, these pages show:

- Average and Max Transaction Time—The time between the client request and the final response packet from the server. Transaction time will vary with client uses and application types, as well as with network latency. Transaction Time is a key indicator in monitoring client experiences and detecting application performance problems.
- Average Client Network Time—The network time between a client and the local switch or router. In Wide Area Application Services (WAAS) monitoring, Client Network Time from a WAE client data source represents the network RTT between the client and its edge WAE, while Client Network Time from the WAE server data source represents the WAN RTT (between the edge and core WAEs).
- Average WAN Network Time—The time across the WAN segment (between the edge routers at the client and server locations).
- Average Server Network Time—The network time between a server and NAM probing point. In WAAS monitoring, Server Network Time from a server data source represents the network time between the server and its core WAE.
- Average Server Response Time—The average time it takes an application server to respond to a request. This is the time between the client request arriving at the server and the first response packet being returned by the server. Increases in the server response time usually indicate problems with application server resources, such as the CPU, Memory, Disk, or I/O.
- Traffic Volume—The volume of bytes per second in each of the Client, WAN, and Server segments.

Step 4 Sort and filter the performance data as needed.

- To sort any column, click the column heading.
- You can filter the data displayed by Time Frame, or click the Filter icon and specify a Quick or Advanced Filter, or use a Preset Filter.



CHAPTER 37

Monitor Microsoft Lync Traffic

How to Monitor Microsoft Lync Traffic

You can use to monitor the Microsoft Lync traffic in your network. The Microsoft Lync Software Defined Network (SDN) API provides an interface for network management systems to access Microsoft Lync network diagnostic data for monitoring Lync network traffic and optimizing Microsoft Lync quality of service. processes and filters Microsoft Lync quality update messages and aggregates Microsoft Lync calls. You can view volume trends over time and get a summary of call types, including filtering based on time and location groups. You can also view individual calls and troubleshoot individual call streams.

Note Prime Infrastructure does not support SDN 2.2 and higher versions.

Set Up Lync Monitoring

You must register as a receiver of Microsoft Lync data in order to monitor and provide a centralized view of how Microsoft Lync is deployed in your network.

On your SDN server, edit the LyncDialogListener.exe file to add the following lines. The LyncDialogListener.exe.config file is located in the Lync SCN API installation directory at the following default location: C:\Program Files\Microsoft Lync Server\Microsoft Lync SDN API.

<add key="submituri" value="https://PI_server_name/webacs/lyncData"/>

where https://PI_server_name is the name of your as specified in the Trusted Root Certification Authorities certificate.

<add key= "clientcertificateid" value="value"/>

where value is the certificate value of your server as specified in the Trusted Root Certification Authorities certificate.

Alternately, if you use the Microsoft SDN interface to enter your server details, you must accept the SSL certificate in order to enable XML communication over secure HTTP.

After you register as a receiver of Microsoft Lync data, all Microsoft Lync details are sent to .

View Microsoft Lync General Data

After you register as a receiver of Microsoft Lync data, all Microsoft Lync details are sent to . To monitor Microsoft Lync data:

Step 1 Choose Services > Application Visibility & Control > Lync Monitoring.

Step 2 Click on any of the colored bars, which represent the different call types and the respective call volume over the specified time period, to display additional details. The Lync Conversations table lists the aggregated conversations for the call type you select.

Step 3 From the Lync Conversations table, click the arrow next to a Caller to expand and view the details of that conversation, from the Caller to the Callee. For example, if you expand a video conversation, there are 4 rows describing the following details:

a. Audio details from Caller to Callee

b. Audio details from Callee to Caller

c. Video details from Caller to Callee

d. Video details from Callee to Caller

Step 4 Click the Filter icon to view a list of conversations in a selected time frame, from a specific caller site, or from a specific callee site.

Set Up Lync Monitoring, on page 761
Troubleshoot User Problems with Microsoft Lync Calls, on page 762
View Site-to-Site Microsoft Lync Data, on page 763

Troubleshoot User Problems with Microsoft Lync Calls

If you receive a call that an end-user is experiencing is having a problem with calls, you can use to view the Microsoft Lync calls for a particular user, and view the list of calls that have the most jitter or packet loss.

Step 1 Choose Services > Application Visibility & Control > Lync Monitoring.

Step 2 Click the Filter icon, and then select the site in which the end-user belongs.

displays the call volume over the last 6 hours.

Step 3 If you know the time in which the end-user was experience call problems, click the Filter icon and under Time Filter, enter the parameters for the desired time.

Step 4 Click on the colored bars that corresponds to Audio call in the time period in which the problems occurred. The Lync Conversations table lists the aggregated conversations for the call type you select.

Step 5 From the Lync Conversations table, click the arrow next to the end-user who experienced call issues to expand and view the details of that conversation, from the Caller to the Callee. For example, if you expand a video conversation, there are 4 rows describing the following details:

a. Audio details from Caller to Callee

b. Audio details from Callee to Caller

c. Video details from Caller to Callee

d. Video details from Callee to Caller

displays the call metrics of the conversation.

Related Topics

Set Up Lync Monitoring, on page 761
View Microsoft Lync General Data, on page 762
View Site-to-Site Microsoft Lync Data, on page 763

View Site-to-Site Microsoft Lync Data

You can use to view the Microsoft Lync data between sites. For example, you can monitor all Microsoft Lync calls that are placed from a particular site to a particular site.

Step 1 Choose Services > Application Visibility & Control > Lync Monitoring.

Step 2 Click the Filter icon, and under Caller Site, select a site from where the Microsoft Lync calls are placed.

Step 3 From the Filter icon, under Callee Site, select a site for where the Microsoft Lync calls are received.

displays the call volume in 5-minute increments for the previous 6 hours for the total calls of each type—video, voice, and appsharing—between the sites you selected.

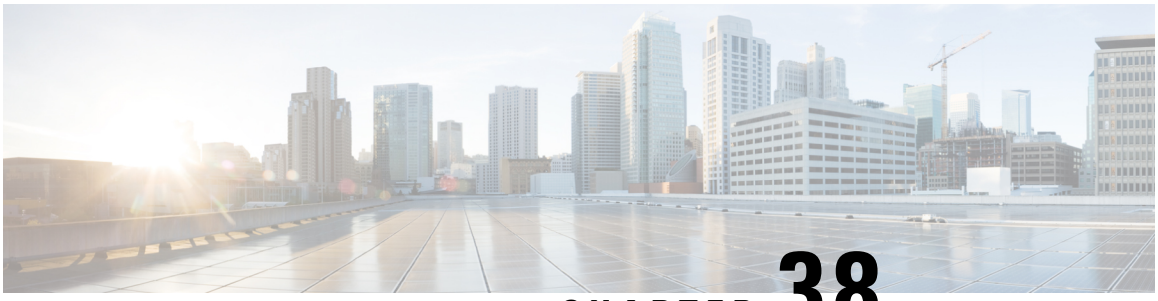
Step 4 Choose Services > Application Visibility & Control > Lync Monitoring > Call type (audio, video, or application sharing) to view the call metrics.

Audio call details include a numerical mean opinion score (MOS) value, for which assigns a value that describes the voice quality of the experience that is being delivered to end users as described in the following table:

MOS Value	Value
Greater than 3.5	Good
2-3.5	Fair
Less than 2	Poor

Related Topics

Set Up Lync Monitoring, on page 761
View Microsoft Lync General Data, on page 762
Troubleshoot User Problems with Microsoft Lync Calls, on page 762



CHAPTER 38

Troubleshoot RTP and TCP Flows Using Mediatrace

What is Mediatrace

The Mediatrace troubleshooting tool generates a table that lists the currently active RTP streams or TCP sessions. Using these Mediatrace tables and their associated options, you can:

- Identify and select RTP or TCP flows with problems.
- Troubleshoot problems with RTP or TCP flows.
- Troubleshoot problems with RTP or TCP flows between any two arbitrary endpoints.
- Troubleshoot problems with RTP flows starting from the RTP Conversations dashlet.
- Identify and compare flow performance indicators and data sources.

View Currently Active RTP Streams and TCP Sessions Using Mediatrace

The flow information shown in the RTP Streams and TCP Sessions tables is collected and aggregated from NAM and NetFlow data generated throughout the network.

Many rows in the RTP Streams table are arranged in a tree hierarchy. This will occur whenever an RTP application flow involves more than one data stream. In these cases, the flows between the two application endpoints are aggregated into a single row with a triangle icon.

By default, automatically refreshes the RTP Streams table data every 60 seconds; you can also use one of the preset filters.

refreshes TCP Sessions data once every 300 seconds (5 minutes); you can use the Filter by Application filtering option to include or exclude applications from the list.

You can also click either table's Refresh button at any time. You can turn off automatic refresh by unselecting the Enable auto refresh check box.

To use the Mediatrace tables:

Step 1 Choose Services > Application Visibility and Control > Mediatrace.

Step 2 From the Application drop-down list, choose RTPor TCP. The page shows the corresponding table: RTP Streams or TCP Sessions.

Step 3 Find the flow that you want to troubleshoot:

- To review all flows with a particular type of issue, click the appropriate column heading to sort on that column.

  For example, if you are monitoring RTP performance across the network and want to see the streams with the worst jitter or packet loss, click the Jitter or Packet Loss column headings to sort the streams on these performance indicators. You can then select any of the streams for troubleshooting.

- To find a particular flow with a problem, click the Quick Filter icon and enter a filter criterion under one or more row headings.

  For example, an end user having trouble accessing an application might report the IP address and the name of that application. You can do a quick filter on the TCP table for either the Client IP address or Application ID, then select that session for troubleshooting.

- To spot issues in RTP subflows, click the triangle icon next to any aggregated RTP flow.

  For example, an RTP voice/video flow between any two endpoints will appear in the RTP Streams table as a single flow with a triangle icon. Clicking the icon will show you the four subflows: an incoming and outgoing video subflow, and an incoming and outgoing voice subflow.

Step 4 To troubleshoot the flow, see the Running Mediatrace from Selected RTP or TCP Flows.

Related Topics

Launch a Mediatrace from an RTP or TCP Flow, on page 766
Launch a Mediatrace from Endpoints, on page 767
Troubleshoot Worst RTP Endpoints Reported By Mediatrace, on page 769
Compare Flow Data From Multiple Sources Using Mediatrace, on page 770

Launch a Mediatrace from an RTP or TCP Flow

To troubleshoot RTP or TCP flows using Mediatrace:

Step 1 Choose Services > Application Visibility and Control > Mediatrace. In the Application drop-down list, choose RTPor TCP, then find the flow that you want by using the steps in View Currently Active RTP Streams and TCP Sessions Using Mediatrace.

Step 2 Select the flow and click Trace Service Path. displays the RTP or TCP Stream Details page for the selected flow, with all of the routers in the flow's path in the Troubleshooting Status table, in the order of their distance from the flow's source endpoint. Routers that are Medianet-capable are indicated by a filmstrip icon.

Step 3 To run Mediatrace or Traceroute from a router in the flow's path, click the Start Mediatrace or Start Traceroute link next to that router in the table.

The Start Mediatrace link is present when the device is Mediatrace-capable; the Start Traceroute link is present when the device is not Mediatrace-capable.

Mediatrace can take a minute or more to run, depending on traffic, congestion, and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the Logs tab to see useful information, including:

- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where non-Medianet-capable routers where encountered and how they were processed.
- Medianet-capable routers on which Medianet is not configured.

Step 4 When the operation is complete, the Troubleshooting tab displays a topology map of all of the devices between the flow's two endpoints. Device icons in the map consist of:

- Alarm Severity—The most severe alarm currently recorded for the device.
- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign on red background—The device is Medianet-capable but not configured as a Medianet responder. RTP/TCP performance statistics will not be available for the device. To remedy this situation, you must configure the device as a Medianet responder as explained in Troubleshoot Worst RTP Endpoints Reported By Mediatrace.
- Minus sign—The device is unmanaged.

Step 5 To see key performance metrics, such as CPU and memory utilization, jitter, and packet loss, for all Medianet-capable devices in the RTP or TCP flow's path, click the Medianet Path View tab. To see the performance metrics in numerical and graphic form, click the subtabs in the Medianet Path View pane.

Note The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

Step 6 Use the appropriate links in the Troubleshooting Status table to:

- Launch a Mediatrace or Traceroute operation on a different router.
- Restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Related Topics

View Currently Active RTP Streams and TCP Sessions Using Mediatrace, on page 765
Launch a Mediatrace from Endpoints, on page 767
Troubleshoot Worst RTP Endpoints Reported By Mediatrace, on page 769
Compare Flow Data From Multiple Sources Using Mediatrace, on page 770

Launch a Mediatrace from Endpoints

You can quickly launch a Mediatrace against all RTP or TCP flows between any two endpoints in the network. This can include either specific flows running between any two endpoints on the same or different sites, or between a pair of routers on two different sites.

This is handy if your network lacks NAM monitoring, or when you are in a hurry and you know at least the IP addresses of the two endpoints of the RTP or TCP flow. You must still navigate to and start the trace from the appropriate RTP or TCP Mediatrace table.

To launch an ad hoc Mediatrace from two endpoints:

Step 1 Choose Services > Application Visibility and Control > Mediatrace. From the Application drop-down list, choose RTP or TCP.

Step 2 Click Specify Session for Mediatrace.

Step 3 Enter the required information:

- For an RTP flow:
  - Select the Source Site.
  - Enter the Source Endpoint IP address.
  - Enter the Destination EndPoint IP address.
- For a TCP flow:
  - Select the Client Site.
  - Enter the Client Endpoint IP address.
  - Enter the Server EndPoint IP address.

Step 4 Provide any additional endpoint information that you have:

- For an RTP flow, select or enter the Source Endpoint Port and Destination Endpoint Port.
- For a TCP flow, select or enter the Server Endpoint Port.

Step 5 Click Trace Service Path (for an RTP flow) or OK (for a TCP flow). displays the RTP or TCP Stream Details page for the specified flow, with all of the routers in the flow's path in the Troubleshooting Status table, in the order of their distance from the flow's source or client endpoint. Routers with a "filmstrip" icon next to them are Medianet-capable.

Step 6 To run Mediatrace or Traceroute from a router in the flow's path, click the Start Mediatrace or Start Traceroute link next to that router in the table.

Mediatrace can take a minute or more to run, depending on traffic, congestion, and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the Logs tab to see useful information, including:

- The progress of the operation.
- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where and how non-Medianet-capable routers where encountered and processed.
- Medianet-capable routers on which Medianet is not configured.

Step 7 When the operation is complete, the Troubleshooting tab displays a topology map of the all the devices between the flow's two endpoints. Device icons in the map will be badged as follows:

- Alarm Severity—The most severe alarm currently recorded for the device.

- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign on red background—The device is Medianet-capable but not configured as a Medianet responder. RTP/TCP performance statistics will not be available for the device. To remedy this situation, you must configure the device as a Medianet responder.
- Minus sign—The device is unmanaged.

Step 8 To see key performance metrics for all Medianet-capable devices in the flow's path, click the Medianet Path View tab. Click the subtabs in the Medianet Path View pane to see the performance metrics in numerical and graphic form.

Note The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

Step 9 Use the appropriate links in the Troubleshooting Status table to launch a Mediatrace or Traceroute operation on a different router, restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Related Topics

View Currently Active RTP Streams and TCP Sessions Using Mediatrace, on page 765
Launch a Mediatrace from an RTP or TCP Flow, on page 766
Troubleshoot Worst RTP Endpoints Reported By Mediatrace, on page 769
Compare Flow Data From Multiple Sources Using Mediatrace, on page 770

Troubleshoot Worst RTP Endpoints Reported By Mediatrace

You can quickly launch a Mediatrace against the poorest performing RTP flows in your network using the Worst N RTP End Point Pairs. and RTP Conversation dashlets. This works only for RTP flows.

The RTP Conversations dashlet shows the complete history for a source endpoint, including flows that are no longer active. You will want to select only the most recent flows. If you launch Mediatrace on such an inactive flow, you will receive an error message advising you of this fact.

Step 1 Choose Dashboard > Performance > End User Experience.

Step 2 In the Worst N RTP End Point Pairs dashlet (if this dashlet is not already in the dashboard, see Add Dashlets to Dashboards, on page 10), note the Source Address for your worst performing RTP flows.

Step 3 In the RTP Conversations dashlet in the same page, find the most recent conversation for the same Source Address.

Step 4 Select that conversation in the RTP Conversations dashlet, then choose Troubleshoot > Trace Service path. displays the RTP Stream Details page for the selected flow, with all of the routers in the flow's path in the Troubleshooting Status table, in order of their distance from the flow's source endpoint. Routers that are Medianet-capable are indicated by a filmstrip icon.

Step 5 To run Mediatrace or Traceroute from a router in the flow's path, click the Start Mediatrace orStart Traceroute link next to that router in the table.

Note The Start Mediatrace link is present when the device is Mediatrace-capable; the Start Traceroute link is present when the device is not Mediatrace-capable.

Mediatrace can take a minute or more to run, depending on traffic, congestion, and the total number of hops between the flow endpoints.

While running Mediatrace or Traceroute, click the Logs tab to see useful information, including:

- The progress of the operation.

- Errors encountered during the operation, including router response timeouts and other steps that did not complete.
- Where and how non-Medianet-capable routers where encountered and processed.
- Medianet-capable routers on which Medianet is not configured.

Step 6 When the operation is complete, the Troubleshooting tab displays a topology map of the all of the devices between the flow's two endpoints. Device icons in the map will be badged as follows:

- Flag—The device on which the Mediatrace or Traceroute was initiated.
- Filmstrip—The device is Medianet-capable.
- Minus sign—The device is unmanaged.

Step 7 To see key performance metrics for all Medianet-capable devices in the flow's path, click the Medianet Path View tab. To see the performance metrics in numerical and graphic form, click the subtabs in the Medianet Path View pane.

Note The Medianet Path View tab is available only when you are able to start a Mediatrace operation from the Troubleshooting Status table. If you can only trigger Traceroute operations, it will not be shown.

Step 8 Use the appropriate links in the Troubleshooting Status table to:

- Launch a Mediatrace or Traceroute operation on a different router.
- Restart a Mediatrace or Traceroute operation that is completed, or stop one in progress.

Related Topics

View Currently Active RTP Streams and TCP Sessions Using Mediatrace, on page 765
Launch a Mediatrace from an RTP or TCP Flow, on page 766
Launch a Mediatrace from Endpoints, on page 767
Compare Flow Data From Multiple Sources Using Mediatrace, on page 770

Compare Flow Data From Multiple Sources Using Mediatrace

When interpreting Mediatrace performance data, you might find it helpful to:

- Identify the NAM, NetFlow, and other sources reporting this performance data.
- If you have multiple NAM or NetFlow data sources, compare how those sources are reporting key performance indicators for a particular flow.

To compare flow data from multiple sources:

Step 1 Choose Services > Application Visibility and Control > Mediatrace.

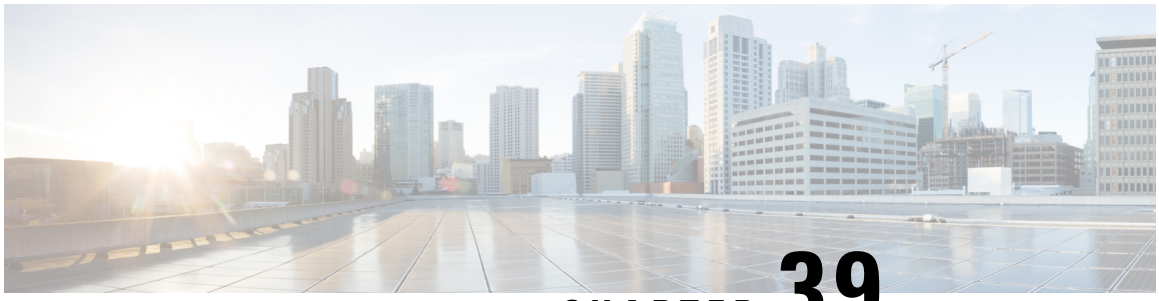
Step 2 From the Application drop-down list, choose RTP or TCP, then find the flow that you want using the steps in View Currently Active RTP Streams and TCP Sessions Using Mediatrace.

Step 3 Expand a row (for an RTP or TCP flow) to view the details of the key performance indicators appropriate for the selected flow and the data source for each such set of indicators.

Step 4 When you are finished, click Ok.

Related Topics

View Currently Active RTP Streams and TCP Sessions Using Mediatrace, on page 765
Launch a Mediatrace from an RTP or TCP Flow, on page 766
Launch a Mediatrace from Endpoints, on page 767
Troubleshoot Worst RTP Endpoints Reported By Mediatrace, on page 769



CHAPTER 39

Cisco Mobility Services Engine and Services

Overview of Cisco Mobility Services Engine (MSE)

The Cisco MSE supports various services within the overall Cisco Unified Wireless Network (CUWN).

The Cisco MSE currently supports the following services:

- Location Service—Also known as Context Aware Service (CAS). This is the core service of the MSE that turns on Wi-Fi client tracking and location API functionality. Allows MSE to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as presence, location, telemetry data, and historical information.
- Wireless Intrusion Protection Service—Provides wireless-specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption within the CUWN infrastructure. wIPS visualizes, analyzes, and identifies wireless threats, and centrally manages mitigation and resolution of security and performance issues using Cisco monitor mode and Enhanced Local Mode (ELM) Access Points. Proactive threat prevention is also supported to create a hardened wireless network core that is impenetrable by most wireless attacks.
- Mobile Concierge—Mobile Concierge enables the Cisco Mobility Services Advertisement Protocol (MSAP). This protocol enables direct communication between the MSE and mobile devices, allowing

content to be pushed directly to the mobile device pre-association. This functionality is dependent on the mobile device supporting 802.11u and MSAP.

- CMX Analytics Service—The CMX Analytics service analyzes wireless device location information in a particular network. The CMX Analytics service uses the data provided by the MSE to calculate the location of Wi-Fi devices in the Wireless Local Area Network (WLAN). In addition, the FastLocate feature sends information about the RSSI strength of data packets to the Cisco WLC that can be used for location calculations.

When a wireless device is enabled in a network, it transmits probe request packets to identify the wireless network in its neighborhood. Even after connecting to the access point in the WLAN, the client devices continue to transmit probe request packets to identify other access points for better quality of service. The access points gather these request and the associated RSSI from the various wireless devices and forwards them to the Wireless LAN Controller (WLC). The controller then forwards this information to the MSE.

The basic data that is collected from various APs, when analyzed, produces information and knowledge about the movement and behavior patterns of people who are using Wi-Fi devices in the building. For example, the building can be an airport, shopping mall, city center, and so on. The CMX Analytics service helps the airport authorities or the building owners to understand the movement of passengers or customer within their building. This helps them improve the signage, make changes to the under utilized areas, and so on.

Related Topics

Add MSEs to , on page 774
Data That is Synchronized With MSE, on page 780
Configure Mobile Concierge Using MSE, on page 830

Add MSEs to

You can add an MSE using the Add Mobility Services Engine dialog box in the Mobility Service page. In this dialog box, you can add licensing files, tracking parameters, and assign maps to the MSE. If you launch the wizard with an existing MSE for configuration, then the Add MSE option appears as Edit MSE Details.

To add an MSE to , log in to and follow these steps:

Before you begin

- To learn more about Cisco Adaptive wIPS features and functionality, go to https://www.cisco.com/to watch a multimedia presentation. Here you can find the learning modules for a variety of topics. Over future releases, we will add more overview and technical presentations to enhance your learning.
- recognizes and supports the MSE 3355 appropriately. You can access the MSE installation guide at https://www.cisco.com/c/en/us/td/docs/wireless/mse/3355/user/guide/mse3355_qsg/mse_qsgmain.html.
- The Services > Mobility Services > Mobility Services Engines page is available only in root virtual domain.

Step 1 Verify that you can ping the mobility service engine that you want to add from .

Step 2 Choose Services > Mobility Services > Mobility Services Engines to display the Mobility Services page.

Step 3 From the Select a command drop-down list, choose Add Mobility Services Engine, and click Go.

The Add Mobility Services Engine page appears.

Step 4 Enter the following information:

- Device Name—User-assigned name for the MSE.
- IP Address—The IP address of the mobility service engine.

An MSE is added only if a valid IP address is entered. The Device Name helps you distinguish between devices if you have multiple with multiple mobility services engines, but it is not considered when validating an MSE.

- Contact Name (optional)—The mobility service engine administrator.
- Username—The default username is admin. This is the communication username configured for MSE.
- Password—The default password is admin.This is the communication password configured for MSE.

If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, we recommend that you rerun the automatic installation script and change the username and password.

- Select the Delete synchronized service assignments check box if you want to permanently remove all service assignments from the MSE.

This option is applicable for network designs, wired switches, controllers, and event definitions. The existing location history data is retained, however you must use manual service assignments to perform any future location calculations.

Step 5 Click Next. automatically synchronizes the selected elements with the MSE.

After the synchronization, the MSE License Summary page appears. You can use the MSE License Summary page to install a license, add a license, remove a license, install an activation license, and install service license.

Configuring Services for MSE

Step 6 To enable a service on the MSE, select the check box next to the service. The different type of services are:

- Context Aware Service—If you select the Context Aware Service check box, then you must select a location engine to perform location calculation. You can choose CAS to track clients, rogues, interferers, and tags. You can choose Cisco Context-Aware Engine for Clients and Tag to track tags.
- WIPS—The Wireless Intrusion Prevention System check box, it detects wireless and performance threats.
- Mobile Concierge Service—The Mobile Concierge Service check box, it provides service advertisements that describe the available services for the mobile devices.
- CMX Analytics Service—The CMX Analytics Service check box, it provides a set of data analytic tools packaged for analyzing Wi-Fi device location data that comes from the MSE.
- CMX Connect & Engage—The CMX Connect and Engage service provides a guest Wi-Fi onboarding solution, as well as zone and message configuration for the CMX Software Development Kit (SDK).
- HTTP Proxy Service—The HTTP Proxy service on the MSE terminates all HTTP traffic intercepted using Policy Based Routing (PBR) and acts as a forward proxy by pulling contents on behalf of wireless clients.

From release 7.5 onward, wIPS service requires a dedicated MSE because it does not support CAS and wIPS on the same MSE.

Configuring MSE Tracking and History Parameters

Step 7 After you enable services on the MSE, the Select Tracking & History Parameters page appears.

If you skip configuring the tracking parameters, the default values are selected.

Step 8 You can select the clients that you want to keep track of by selecting the corresponding Tracking check box(es). The various tracking parameters are as follows:

- Wired Clients
- Wireless Clients
- Rogue Access Points
    - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

Step 9 You can enable the history tracking of devices by selecting the corresponding devices check box(es). The different history parameters are as follows:

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

Step 10 Click Next to Assign Maps to the MSE.

Assigning Maps to the MSE

The Assigning Maps page is available only if you select CAS as one of the services to be enabled on the MSE.

Step 11 Once you configure MSE tracking and history parameters, the Assigning Maps page appears.

The Assign Maps page shows the following information:

- Name
- Type (building, floor, campus)
- Status

Step 12 You can see the required map type by selecting either All, Campus, Building, Floor Area, or Outdoor Area from the Filter option available on the page.

Step 13 To synchronize a map, select the Name check box, and click Synchronize.

Upon synchronization of the network designs, the appropriate controllers that have APs assigned on a particular network design are synchronized with the MSE automatically.

Step 14 Click Next to configure mobile app enablement.

Mobile App Enablement

Enabling this integration will allow the MSE to send floor maps and wireless client position notification to Meridian. Meridian used this information to provide location-based services to your users without requiring them to connect to your network and access the MSE directly. After enabling Meridian, you will receive an e-mail with instructions on how to activate your account and share access with others in your organization. You can utilize Meridians platform to provide location services to your visitors either through the Meridian mobile app or your own apps using their mobile SDKs for Android and iOS. The data bandwidth for each wireless client position or zone notification from MSE to Meridian can be maximum of 1 MB/second.

Once you assign maps to the MSE, the Mobile App Enablement page appears.

Step 15 Select the Enable Mobile App Integration check box to enable the mobile application integration. You can click an icon to open the Mobile App Enablement Help page.

Step 16 Enter the name for the location on the Location Name text box. The name you enter here will appear in the Meridian app so that you can try out the location services on your own device.

Step 17 Enter the email address in the E-mail Address text box to access the Meridian online editor and SDK. Meridian will email these addresses with instructions on how to access your account and share it with others in your organization.

Step 18 Enter the server where the MSE can register its UDI and send the maps that are synchronized to the MSE in theRegistration Endpoint text box.

Step 19 Enter the server detail where the MSE can send location update notifications in the data format specified in the Notifications Endpoint text box.

Step 20 Select the Notifications Data Format radio button. This is the data format of the notifications sent from the MSE. The different data formats are: Legacy SOAP/XML, XML, JSON, and Protocol Buffers.

Step 21 Enter the street address of your location in the Street Address text box.

Step 22 Enter the phone number where Meridian can reach you for additional information in the Phone Number text box.

Step 23 Click Advanced to open the Advanced pane.

Step 24 If you want MSE to send real-time notifications to Meridian when ever the wireless clients enter the selected zones, then select the Enable Zone Notifications for zones check box and choose floors and zones from the drop-down list.

The Enable zone notifications for zones drop-down list shows all the floors and zones that are added to and synced to the MSE.

Step 25 Click OK after selecting zones and floors.

Step 26 Click Save.

Step 27 Click Done to save the MSE settings.

Note The below listed features of MSE are not supported by CMX:

- Managing CMX High Availability
- Synchronization History
- Context Aware Notifications
- Mobile Concierge
- wIPS and Wireless Security
- Location Accuracy

Related Topics

View MSEs, on page 779

Delete MSE License Files, on page 778
Delete MSEs from Prime Infrastructure, on page 779

MSE Licensing

The Cisco MSE provides a wide variety of location-based services. To enable these services, the following are required:

- Cisco MSE hardware or software appliance
  - Physical Appliance—An activation license is not required.
  - Virtual Appliance—Virtual Appliance instance requires an MSE Virtual Appliance Activation license (L-MSE-7.0-K9). It is not sufficient to simply have a service/feature license on an MSE Virtual Appliance.
- Licenses
- Support
- See the chapter Licenses and Software Updates in the Cisco Prime Infrastructure Administrator Guide, for more information.

For complete details on ordering and downloading licenses, see the Cisco Mobility Services Engine Licensing and Ordering Guide at the following URL : http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

Delete MSE License Files

To delete an MSE license file, follow these steps:

SUMMARY STEPS

1. Choose Services > Mobility Services > Mobility Service Engine.
2. Click Device Name to delete a license file for a particular service.
3. From the Select a command drop-down list, choose Edit Configuration.
4. Click Next in the Edit Mobility Services Engine dialog box.
5. Choose the MSE license file that you want to delete in the MSE License Summary page.
6. Click Remove License.
7. Click OK to confirm the deletion or Cancel to close this page without deleting the license.
8. Click Next to enable services on the MSE.

DETAILED STEPS

Step 1 Choose Services > Mobility Services > Mobility Service Engine.

The Mobility Services page appears.

Step 2 Click Device Name to delete a license file for a particular service.

Step 3 From the Select a command drop-down list, choose Edit Configuration.

Step 4 Click Next in the Edit Mobility Services Engine dialog box.

The MSE License Summary page appears.

Step 5 Choose the MSE license file that you want to delete in the MSE License Summary page.

Step 6 Click Remove License.

Step 7 Click OK to confirm the deletion or Cancel to close this page without deleting the license.

Step 8 Click Next to enable services on the MSE.

Related Topics

View MSEs, on page 779
Add MSEs to , on page 774
Delete MSEs from Prime Infrastructure, on page 779
Data That is Synchronized With MSE, on page 780

View MSEs

To see a list of current Mobility Services, choose Services > Mobility Services > Mobility Services Engines.

The Mobility Services Engines page provides device information and features for each device and a Select a command drop-down list.

Location and MSE features of do not support partitioning.

Related Topics

Add MSEs to , on page 774
Delete MSE License Files, on page 778
Delete MSEs from Prime Infrastructure, on page 779
Data That is Synchronized With MSE, on page 780

Delete MSEs from Prime Infrastructure

To delete an MSE from the Prime Infrastructure database, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

The Mobility Services page appears.

Step 2 Select the MSE(s) to be deleted by selecting the corresponding Device Name check box(es).

Step 3 From the Select a command drop-down list, choose Delete Service(s).

Step 4 Click Go.

Step 5 Click OK to confirm that you want to delete the selected MSE from the Prime Infrastructure database.

Step 6 Click Cancel to stop the deletion.

Related Topics

View MSEs, on page 779
Add MSEs to , on page 774

Data That is Synchronized With MSE

This section describes how to synchronize and MSEs manually and smartly.

After adding an MSE to , you can synchronize network designs (campus, building, floor, and outdoor maps), controllers (name and IP address), specific Catalyst 3000 Series and 4000 switches, and event groups with the MSE.

- Network Designs—A logical mapping of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus and the floors of each building constitute a single network design.
- Controllers—A selected controller that is associated and regularly exchanges location information with an MSE. Regular synchronization ensures location accuracy.
- Event Groups—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked.
- Wired Switches —Wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.
    - The MSE can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.
    - The MSE can also be synchronized with the following Catalyst series switches 4000: WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE.
- Third Party Elements—When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.
- Service Advertisements—Mobile Concierge Service provides service advertisements on the mobile devices. This shows the service advertisement that has synchronized with the MSE.

Be sure to verify software compatibility between the controller, , and the MSE before synchronizing.

Communication between the MSE, , and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with the UTC time. The MSE and its associated controllers must be mapped to the same NTP server and the same server. An NTP server is required to automatically synchronize time between the controller, , and the MSE.

Related Topics

View MSEs, on page 779
Synchronize Product Data With MSE, on page 780
Change the MSE Assignment for a Wireless Controller, on page 782
Synchronize Third Party NEs with MSE , on page 783
Set Up Synchronization Between MSE Databases and Product Database, on page 785
View the History of MSE Database and product Database Synchronizations, on page 787

Synchronize Product Data With MSE

To synchronize network designs, controllers, wired switches, or event groups with the MSE, follow these steps:

SUMMARY STEPS

1. Choose Services > Mobility Services > Synchronize Services.
2. Choose the appropriate menu option (Network Designs, Controllers, Event Groups, Wired Switches, Third Party Elements, or Service Advertisements) from the left sidebar menu.
3. To assign a network design to an MSE, from the left sidebar menu, choose Network Designs.
4. Select all the maps to be synchronized with the MSE by selecting the corresponding Name check box.
5. Click Change MSE Assignment.
6. Select the MSE to which the maps are to be synchronized.
7. Click either of the following in the MSE Assignment dialog box:
8. Click Synchronize to update the MSE(s) database(s).

DETAILED STEPS

Step 1 Choose Services > Mobility Services > Synchronize Services.

Step 2 Choose the appropriate menu option (Network Designs, Controllers, Event Groups, Wired Switches, Third Party Elements, or Service Advertisements) from the left sidebar menu.

Step 3 To assign a network design to an MSE, from the left sidebar menu, choose Network Designs.

Step 4 Select all the maps to be synchronized with the MSE by selecting the corresponding Name check box.

Through 6.0, you can assign only up to a campus level to an MSE. Beginning with 7.0 this option is granular to a floor level. For example, you can choose to assign floor1 to MSE 1, floor2 to MSE 2, and floor3 to MSE 3.

Step 5 Click Change MSE Assignment.

Step 6 Select the MSE to which the maps are to be synchronized.

A network design might include a floor in a campus or a large campus with several buildings, each monitored by a different MSE. Because of this, you might need to assign a single network design to multiple MSEs.

Step 7 Click either of the following in the MSE Assignment dialog box:

- Save—Saves the MSE assignment. The following message appears in the Messages column of the Network Designs page with a yellow arrow icon:

  "To be assigned - Please synchronize”

- Cancel—Discards the changes to the MSE assignment and return to the Network Designs page.
- You can also click Reset to undo the MSE assignments.

A network design may include a floor in a campus or a large campus with several buildings, each monitored by a different MSE. Because of this, you may need to assign a single network design to multiple MSEs.

Network design assignments also automatically picks up the corresponding controller for synchronization.

Step 8 Click Synchronize to update the MSE(s) database(s).

When items are synchronized, a green two-arrow icon appears in the Sync.

You can use the same procedure to assign wired switches or event groups to an MSE.

Related Topics

Data That is Synchronized With MSE, on page 780

View the History of MSE Database and product Database Synchronizations, on page 787
Change the MSE Assignment for a Wireless Controller, on page 782
Set Up Synchronization Between MSE Databases and Product Database, on page 785
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 799

Change the MSE Assignment for a Wireless Controller

You can assign an MSE to any wireless controller on a per-service (CAS or wIPS) basis.

To assign an MSE service to wireless controllers, follow these steps:

Step 1 In the synchronization page, choose Controllers.

Step 2 Choose the controllers to be assigned to the MSE.

Step 3 Click Change MSE Assignment.

Step 4 Choose the MSE to which the controllers must be synchronized.

Step 5 Click either of the following in the dialog box:

- Save—Saves the MSE assignment. The following message appears in the Messages column of the Controllers page:

"To be assigned - Please synchronize".

- Cancel—Discards the changes to the MSE assignment and returns to the Controllers page.
- You can also click Reset to undo the yellow button assignments.

Step 6 Click Synchronize to complete the synchronization process.

Step 7 Verify that the MSE is communicating with each of the controllers for only the chosen service. This can be done by clicking the NMSP status link in the status page. See Troubleshoot NMSP Connection Status, on page 783 for more information.

After Synchronizing a controller, verify that the timezone is set on the associated controller. Controller names must be unique for synchronizing with an MSE. If you have two controllers with the same name, only one is synchronized.

Step 8 If you want to unassign a network design, controller, wired switch, or event group from an MSE, do the following:

a) On the respective tabs, click one or more elements, and click Change MSE Assignment. The Choose MSE dialog box appears.
b) Unselect the Mobility Services Engine check box if you do not want the elements to be associated with that MSE.
c) Click Save to save the changes to the assignments.
d) Click Synchronize. A two-arrow icon appears in the Sync Status column.

Related Topics

Troubleshoot NMSP Connection Status, on page 783
View MSEs, on page 779
Data That is Synchronized With MSE, on page 780
View the History of MSE Database and product Database Synchronizations, on page 787
Set Up Synchronization Between MSE Databases and Product Database, on page 785

Troubleshoot NMSP Connection Status

If you recently upgraded a controller and NMSP status is inactive on the Services > Mobility Services > Synchronize Services > Controllers page, you need to trigger an inventory collection so receives the upgraded controller information:

Step 1 Choose Administration > Dashboards > Job Dashboard.

Step 2 Select System Jobs > Inventory, then select Wireless Controller Inventory.

Step 3 Click Run.

After the job completes, the NMSP Status will be updated.

Related Topics

Change the MSE Assignment for a Wireless Controller, on page 782

Synchronize Third Party NEs with MSE

When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.

To delete the elements or mark them as third-party elements, follow these steps:

SUMMARY STEPS

1. Choose Services > Mobility Services > Synchronize Services.
2. Select one or more elements.
3. Click one of the following buttons:

DETAILED STEPS

Step 1 Choose Services > Mobility Services > Synchronize Services.

The Network Design page appears.

In the Network Design page, choose Third Party Elements from the left sidebar menu.

The Third Party Elements page appears.

Step 2 Select one or more elements.

Step 3 Click one of the following buttons:

- Delete Event Groups—Deletes the selected event groups.
- Mark as 3rd Party Event Group(s)—Marks the selected event groups as third-party event groups.

Related Topics

View MSEs, on page 779
Data That is Synchronized With MSE, on page 780
View the History of MSE Database and product Database Synchronizations, on page 787

Set Up Synchronization Between MSE Databases and Product Database, on page 785
Change the MSE Assignment for a Wireless Controller, on page 782
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 799

Configure Controller Time Zones to Ensure Proper Synchronization with MSE

For controller Releases 4.2 and later, if an MSE (Release 5.1 or greater) is installed in your network, it is mandatory that the time zone be set on the controller to ensure proper synchronization between the two systems.

Greenwich Mean Time (GMT) is used as the standard for setting the time zone system time of the controller.

You can automatically set the time zone during initial system setup of the controller or manually set it on a controller already installed in your network.

To manually set the time and time zone on an existing controller in your network using the CLI, follow these steps:

Step 1 Configure the current local time in GMT on the controller by entering the following commands:

Example:

```
(Cisco Controller) >config time manual 09/07/07 16:00:00
(Cisco Controller) >config end
```

When setting the time, the current local time is entered in terms of GMT and as a value between 00:00 and 24:00. For example, if it is 8 AM Pacific Standard Time (PST) in the US, you enter 16:00 (4 PM PST) as the PST time zone is 8 hours behind GMT.

Step 2 Verify that the current local time is set in terms of GMT by entering the following command:

Example:

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 16:00:02 2007
Timezone delta........................... 0:0
```

Step 3 Set the local time zone for the system by entering the following commands:

When setting the time zone, you enter the time difference of the local current time zone with respect to GMT (+/-). For example, Pacific Standard Time (PST) in the United States (US) is 8 hours behind GMT (UTC) time. Therefore, it is entered as -8.

Example:

```
(Cisco Controller) >config time timezone -8
(Cisco Controller) >config end
```

Step 4 Verify that the controller shows the current local time with respect to the local time zone rather than in GMT by entering the following command:

Example:

```
(Cisco Controller) >show time
Time..................................... Fri Sep 7 08:00:26 2007
Timezone delta........................... -8:0
```

The time zone delta parameter in the show time command shows the difference in time between the local time zone and GMT (8 hours). Before configuration, the parameter setting is 0.0.

Related Topics

View MSEs, on page 779
Data That is Synchronized With MSE, on page 780
View the History of MSE Database and product Database Synchronizations, on page 787
Set Up Synchronization Between MSE Databases and Product Database, on page 785
Change the MSE Assignment for a Wireless Controller, on page 782
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 799
Synchronize Third Party NEs with MSE , on page 783

Set Up Synchronization Between MSE Databases and Product Database

Manual synchronization of and MSE databases provides immediate synchronization. However, future deployment changes (such as making changes to maps and access point positions), can yield incorrect location calculations and asset tracking until resynchronization reoccurs.

To prevent out-of-sync conditions, use to carry out synchronization. This policy ensures that synchronization between and MSE databases is triggered periodically and any related alarms are cleared.

Any change to one or more of any synchronized components is automatically synchronized with the MSE. For example, if a floor with access points is synchronized with a particular MSE and then one access point is moved to a new location on the same floor or another floor which is also synchronized with the MSE, then the changed location of the access point is automatically communicated.

To further ensure that and MSE are in sync, smart synchronization happens in the background.

To configure smart synchronization, follow these steps:

Step 1 Choose Administration > Settings > Background Tasks.

The Background Tasks summary page appears.

Step 2 Select the Mobility Service Synchronization check box.

Step 3 The Mobility Services Synchronization page appears.

Step 4 To set the MSE to send out-of-sync alerts, select the Enabled check box in the Out of Sync Alerts group box.

Step 5 To enable smart synchronization, select the Smart Synchronization Enabled check box.

Smart synchronization does not apply to elements (network designs, controllers, or event groups) that have not yet been assigned to an MSE. However, out-of-sync alarms are still generated for these unassigned elements. For smart synchronization to apply to these elements, you need to manually assign them to an MSE.

When an MSE is added to , the data in is always treated as the primary copy that is synchronized with the MSE. All synchronized network designs, controllers, event groups and wired switches that are present in the MSE and not in are removed automatically from MSE.

Step 6 Enter the time interval, in minutes, that the smart synchronization is to be performed.

By default, smart-sync is disabled.

Step 7 Click Submit.

Related Topics

Configure Controller Time Zones to Ensure Proper Synchronization with MSE, on page 784

Examples: How Smart Controllers are Selected When Synchronizing Product Data With MSEs

Scenario 1

If a floor having at least one access point from a controller is chosen to be synchronized with the MSE from the Network Designs section of the Synchronization page, then the controller to which that access point is connected is automatically selected to be assigned to the MSE for CAS service.

Scenario 2

When at least one access point from a controller is placed on a floor that is synchronized with MSE, the controller to which the access point is connected is automatically assigned to the same MSE for CAS service.

Scenario 3

An access point is added to a floor and is assigned to an MSE. If that access point is moved from controller A to controller B, then controller B is automatically synchronized to the MSE.

Scenario 4

If all access points placed on a floor which is synchronized to the MSE are deleted then that controller is automatically removed from MSE assignment or unsynchronized.

Related Topics

Data That is Synchronized With MSE, on page 780
View the History of MSE Database and product Database Synchronizations, on page 787
Change the MSE Assignment for a Wireless Controller, on page 782
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 799
Synchronize Third Party NEs with MSE , on page 783

View the Status of the MSE Database and product Database Synchronizations

You can use the Synchronize Servers command in to view the status of network design, controller, and event group synchronization with an MSE.

To view synchronization status, follow these steps:

Step 1 Choose Services > Mobility Services > Synchronize Services.

Step 2 From the left sidebar menu, choose Network Designs, Controllers, Event Groups, Wired Switches Third Party Elements, or Service Advertisements.

For each of the elements, the Sync. Status column shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the specified server such as an MSE. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a provided server.

A green two-arrow icon does not indicate the NMSP connection status for a controller.

You can also view the synchronization status at Monitor > Maps > System Campus >Building > Floor

where Building is the building within the campus and Floor is a specific floor in that campus building.

The MSE Assignment option on the left sidebar menu shows which MSE the floor is currently assigned to. You can also change MSE assignment from this page.

Related Topics

View MSEs, on page 779
Add MSEs to , on page 774
Data That is Synchronized With MSE, on page 780
View the History of MSE Database and product Database Synchronizations, on page 787
Change the MSE Assignment for a Wireless Controller, on page 782
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 799

View the History of MSE Database and product Database Synchronizations

You can view the synchronization history for the last 30 days for an MSE. This is especially useful when automatic synchronization is enabled as alarms are automatically cleared. Synchronization History provides a summary of those cleared alarms.

The Synchronization History page on the Services tab is available only in the root virtual domain in Release 7.3.

To view synchronization history, choose Services > Synchronization History, and click the column headers to sort the entries.

Related Topics

View MSEs, on page 779
Synchronize Third Party NEs with MSE , on page 783
Data That is Synchronized With MSE, on page 780
Change the MSE Assignment for a Wireless Controller, on page 782
Find and Troubleshoot MSE-Product Out-of-Sync Alarms, on page 799
Set Up Synchronization Between MSE Databases and Product Database, on page 785
View the Status of the MSE Database and product Database Synchronizations, on page 786

View the Notification Statistics for an MSE

You can view the notification statistics for a specific MSE. To view the Notification Statistics for a specific MSE:

Choose Services > Mobility Services > Mobility Services Engines > MSE-name Context Aware Service > Notification Statistics (where MSE-name is the name of an MSE).

The following table describes the fields in the Notification statistics page.

Table 78: Notification Statistics fields

Field	Description
Summary	
Destinations	
Total	Total destination count.
Unreachable	Unreachable destination count.
Notification Statistics Summary	
Destination Address	The destination address to which the notifications are sent.
Destination Port	The destination port to which the notifications are sent.
Destination Type	The type of the destination. Example: SOAP_XML
Destination Status	Status of the track definition. Track notification status can be either Enabled or Disabled.
Last Sent	The date and time at which the last notification was sent to the destination device.
Last Failed	The date and time at which the notification failed.
Track Definition (Status)	
Total Count	The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.

Change an MSE Server's Basic Properties

You can use to edit the general properties of an MSE registered in database. General properties include contact name, username, password, and HTTP.

To edit the general properties of an MSE, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines sto display the Mobility Services page.

Step 2 Click the name of the MSE that you want to edit. The General Properties page (with a General tab and Performance tab) appears.

Step 3 In the General Properties page, modify the following Server Details as necessary:

- Contact Name—Enter a contact name for the mobility service.
- Username—Enter the log in username for the server that manages the mobility service.
- Password—Enter the log in password for the server that manages the mobility service.
- HTTP—Select the HTTP enable check box to enable HTTP. When you have a non-default port or HTTPS turned on, you must pass the correct information along with the command. For example, getserverinfo must include

-port<<port>> -protocol<<HTTP/HTTPS>>. Similarly, for stopping the server, stoplocserver - port <<port>> -protocol <HTTP/HTTPS>>.

- Legacy Port—8001
- Legacy HTTPS—Select the check box to enable the legacy HTTPS.
- Delete synchronized service assignments and enable synchronization—Select the Delete synchronized service assignments check box if you want to permanently remove all service assignments from the MSE. This option shows up only if the delete synchronized service assignments check box was unselected while adding an MSE.

always uses HTTPS to communicate with an MSE.

The following tcp ports are in use on the MSE in Release 6.0: tcp 22: MSE SSH port, tcp 80: MSE HTTP port, tcp 443: MSE HTTPS port, tcp 1411: AeroScout, tcp 1999: AeroScout internal port, tcp 4096: AeroScout notifications port, tcp 5900X: AeroScout (X can vary from 1 to 10), and tcp 8001: Legacy port. Used for location APIs.

The following udp ports are in use on the MSE in Release 6.0: udp 123: NTPD port (open after NTP configuration), udp 162: AeroScout SNMP, udp/tcp 4000X: AeroScout proxy (X can vary from 1 to 5), udp 12091: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 12092: AeroScout devices (TDOA Wi-Fi Receivers, chokepoints), udp 32768: Location internal port, udp 32769: AeroScout internal port, and udp 37008: AeroScout internal port.

Step 4 In the Mobility Services dialog box, select the Admin Status check box to enable the applicable (Context Aware Service, WIPS, Mobile Concierge Service, Location Analytics Service, Billboard service) service.

If you select Context Aware Service, then you must select a location engine to perform location calculation.

Choose either of the following:

- Cisco Tag Engine

or

- Partner Tag Engine

Note With MSE 6.0, you can enable multiple services (CAS and wIPS) simultaneously. Before Version 6.0, MSEs can only supported one active service at a time.

The Mobility Services dialog box also shows the following:

- Service Name
- Service Version
- Service Status
- License Type

Use the Click here link to view MSE licensing details.

Step 5 Click Save to update and mobility service databases.

Step 6 Click the Performance tab to view a graph of CPU and memory utilization percentages.

Change the NMSP Protocol Properties for an MSE

Network Mobility Services Protocol (NMSP) manages communication between the mobility service and the controller. Transport of telemetry, emergency, and RSSI values between the mobility service and the controller is managed by this protocol.

Note The NMSP parameter is supported in mobility services installed with Release 3.0 through 7.0.105.0. It is not supported on releases later than 7.0.105.0.

- NMSP replaces the LOCP term introduced in Release 3.0.
- Telemetry and emergency information is only seen on controllers and installed with Release 4.1 software or greater and on mobility service engine running release 3.0 or later software.
- The TCP port (16113) that the controller and mobility service communicate over must be open (not blocked) on any firewall that exists between the controller and mobility service for NMSP to function.

The NMSP Parameters dialog box in enables you to modify NMSP parameters such as echo and neighbor dead intervals as well as response and retransmit periods.

To configure NMSP parameters, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the MSE whose properties you want to edit.

Step 3 From the left sidebar menu, choose Status > NMSP Parameters.

Step 4 Modify the NMSP parameters as appropriate.

Note We do not recommend you change the default parameter values unless the network is experiencing slow response or excessive latency.

NMSP parameters include the following:

- Echo Interval—Defines how frequently an echo request is sent from a mobility service to a controller. The default value is 15 seconds. Allowed values range from 1 to 120 seconds.
- If a network is experiencing slow response, you can increase the values of the echo interval, neighbor dead interval and the response timeout values to limit the number of failed echo acknowledgments.
- Neighbor Dead Interval—The number of seconds that the mobility service waits for a successful echo response from the controller before declaring the neighbor dead. This timer begins when the echo request is sent.
- The default values is 30 seconds. Allowed values range from 1 to 240 seconds. This value must be at least two times the echo interval value.
- Response Timeout—Indicates how long the mobility service waits before considering the pending request as timed out. The default value is one second. Minimum value is one (1). There is no maximum value.
- Retransmit Interval—Interval of time that the mobility service waits between notification of a response time out and initiation of a request retransmission. The default setting is 3 seconds. Allowed values range from 1 to 120 seconds.
- Maximum Retransmits—Defines the maximum number of retransmits that are done in the absence of a response to any request. The default setting is 5. Allowed minimum value is zero (0). There is no maximum value.

Step 5 Click Save to update and mobility service databases.

View MSE Active Sessions

The Active Sessions dialog box in enables you to view active user sessions on the MSE.

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the MSE.

Step 3 From the left sidebar menu, choose System > Active Sessions.

shows a list of active mobility service sessions. For every session, shows the following information:

- Session identifier
- IP address from which the mobility service is accessed
- Username of the connected user
- Date and time when the session started
- Date and time when the mobility service was last accessed
- How long the session was idle since the last access

View MSE Trap Destinations

The Trap Destinations dialog box of e enables you to specify which or Cisco Security Monitoring, Analysis, and Response System (CS-MARS) network management platform is the recipient of SNMP traps generated by the MSE.

To view a trap destination for an MSE, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the MSE.

Step 3 From the left sidebar menu, choose System > Trap Destinations.

shows a list of current trap destinations including the following information:

- IP address
- Port No.
- Community
- Destination type
- SNMP Version

Use the Select a command drop-down list to add or delete a trap destination.

Related Topics

Configure MSE Trap Destinations, on page 791

Configure MSE Trap Destinations

To add a trap destination, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the mobility service.

Step 3 From the left sidebar menu, choose System > Trap Destinations.

Step 4 Choose Add Trap Destination from the command drop-down list and click Go.

The New Trap Destination page appears.

Step 5 Enter the following details (see the following table).

Table 79: Add Trap Destination Page

Field	Description
IP Address	IP address for the trap destination.
Port No.	Port number for the trap destination. The default port number is 162.
Destination Type	This field is not editable and has a value of Other.
Snmp Version	Select either v2c or v3.
The following set of fields appear only if you select v3 as the SNMP version.	
User Name	Username for the SNMP Version 3.
Security Name	Security name for the SNMP Version 3.
Authentication Type	Select one of the following: HMAC-MD5 HMAC-SHA
Authentication Password	Authentication password for the SNMP Version 3.
Privacy Type	Select one of the following: CBC-DES CFB-AES-128 CFB-AES-192 CFB-AES-256
Privacy Password	Privacy password for the SNMP Version 3.

Step 6 Click Save to save the changes or Cancel to discard the changes.

Related Topics

View MSE Trap Destinations, on page 791

Configure Advanced MSE Server Settings

The Advanced Parameters dialog box in enables you to set the number of days events are kept, set session time out values, set an absent data interval cleanup interval, and enable or disable Advanced Debug. You can use to modify troubleshooting parameters for an MSE.

To edit advanced parameters for an MSE, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose System > Advanced Parameters.

Step 4 View or modify the advanced parameters as necessary.

- General Information
- Advanced Parameters

  Caution Because advanced debugging slows the mobility service down, enable advanced debugging only under the guidance of Cisco TAC personnel.

  - Number of Days to keep Events—Enter the number of days to keep logs. Change this value as required for monitoring and troubleshooting.
  - Session Timeout—Enter the number of minutes before a session times out. Change this value as required for monitoring and troubleshooting. Currently this option appears dimmed.

- Cisco UDI

  - Product Identifier (PID)—The Product ID of the MSE.
  - Version Identifier (VID)—The version number of the MSE.
  - Serial Number (SN)—Serial number of the MSE.

- Advanced Commands

  - Reboot Hardware—Click to reboot the mobility service hardware. See Reboot an MSE Server, on page 793 for more information.
  - Shutdown Hardware—Click to turn off the mobility service hardware. See Shut Down an MSE Server, on page 794Shut Down an MSE Server the for more information.
  - Clear Database—Click to clear the mobility services database. Unselect the Retain current service assignments in the Prime Infrastructure check box to remove all existing service assignments from and MSE. The resources have to be reassigned from Services > Synchronize Services page. This option is selected by default.

Step 5 Click Save to update and mobility service databases.

Reboot an MSE Server

If you need to restart an MSE, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines

Step 2 Click the name of the MSE that you want to reboot.

Step 3 Click System.

Step 4 Click Advanced Parameters.

Step 5 In the Advanced Commands dialog box, click Reboot Hardware.

Step 6 Click OK to confirm that you want to reboot the MSE hardware.

The rebooting process takes a few minutes to complete.

Shut Down an MSE Server

If you need to shut down an MSE, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the name of the MSE that you want to shut down.
Step 3 Click System.
Step 4 Click Advanced Parameters.
Step 5 In the Advanced Commands dialog box, click Shutdown Hardware.
Step 6 Click OK to confirm that you want to shut down the MSE.

Restore Factory Settings for the MSE Database (Clear)

To clear an MSE configuration and restore its factory defaults, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the name of the MSE you want to configure.
Step 3 Click System.
Step 4 Click Advanced Parameters.
Step 5 In the Advanced Commands dialog box, unselect the Retain current service assignments in the Prime Infrastructure check box to remove all existing service assignments from and MSE.

The resources have to be reassigned in the Services > > Mobility Services > Synchronize Services page. By default, this option is selected.

Step 6 In the Advanced Commands dialog box, click Clear Database.
Step 7 Click OK to clear the MSE database.

Configure MSE Logging Levels

You can use to specify the logging level and types of messages to log.

To configure logging options, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the name of the MSE that you want to configure.
Step 3 Choose System > Logs. The advanced parameters for the selected MSE appear.

Step 4 Choose the appropriate options from the Logging Level drop-down list.

There are four logging options: Off, Error, Information, and Trace.

All log records with a log level of Error or preceding are logged to a new error log file locserver-error-%u-%g.log. This is an additional log file maintained along with the location server locserver-%u-%g.log log file. The error log file consists of logs of Error level along with their context information. The contextual information consists of 25 log records prior to the error. You can maintain up to 10 error log files. The maximum size allowed for each log file is 10 MB.

Caution Use Error and Trace only when directed to do so by Cisco TAC personnel.

Step 5 Select the Enabled check box next to each element listed in that section to begin logging its events.

Step 6 Select the Enable check box in the Advanced Parameters dialog box to enable advanced debugging. By default, this option is disabled.

Step 7 To download log files from the server, click Download Logs. See Download MSE Log Files, on page 795for more information.

Step 8 In the Log File group box, enter the following:

- The number of log files to be maintained in the MSE. You can maintain a minimum of 5 log files and a maximum of 20 log files in the MSE.
- The maximum log file size in MB. The minimum log file size is 10 MB and the maximum is 50 MB.

Step 9 In the MAC Address Based Logging group box, do the following:

- Select the Enable check box to enable MAC address logging. By default, this option is disabled.
- Add one or more MAC addresses for which you want to enable logging. You can also remove MAC addresses that you have already added by selecting the MAC address from the list and clicking Remove.

See How MSE MAC Addressed-Based Logging Works How MSE MAC Addressed-Based Logging Works, on page 795 for more information on MAC Address-based logging.

Step 10 Click Save to apply your changes.

How MSE MAC Addressed-Based Logging Works

This feature allows you to create log files that are specific to an entity whose MAC address is specified. The log files are created in the locserver directory under the following path:

/opt/mse/logs/locserver

A maximum of 5 MAC addresses can be logged at a time. The Log file format for MAC address aa:bb:cc:dd:ee:ff is macaddress-debug-aa-bb-cc-dd-ee-ff.log

You can create a maximum of two log files for a MAC Address. The two log files might consist of one main and one backup or rollover log file.

The minimum size of a MAC log file is 10 MB. The maximum size allowed is 20 MB per MAC Address. The MAC log files that are not updated for more than 24 hours are pruned.

Download MSE Log Files

If you need to analyze MSE log files, you can use to download them to your system. downloads a zip file containing the log files.

To download a .zip file containing the log files, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the name of the MSE to view its status.
Step 3 From the left sidebar menu, choose Logs.
Step 4 Click Download Logs.
Step 5 Follow the instructions in the File Download dialog box to open the file or save the zip file to your system.

Configure MSE User Accounts

You can configure the MSE User Accounts using the following procedure.

SUMMARY STEPS

1. Choose Services > Mobility Services > Mobility Services Engines.
2. Click the device name of the MSE that you want to edit.
3. From the left sidebar menu, choose Systems > Accounts > Users.
4. If you want to add a user to an MSE, follow these steps:
5. If you want to delete a user from an MSE, follow these steps:
6. If you want to change user properties, follow these steps:

DETAILED STEPS

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the device name of the MSE that you want to edit.
Step 3 From the left sidebar menu, choose Systems > Accounts > Users.
Step 4 If you want to add a user to an MSE, follow these steps:
a) From the Select a command drop-down list, choose Add User.
b) Click Go.
c) Enter the username in the Username text box.
d) Enter a password in the Password text box.
e) Enter the name of the group to which the user belongs in the Group Name text box.
f) Choose a permission level from the Permission drop-down list.
g) There are three permission levels to choose from: Read Access, Write Access, and Full Access (required for to access an MSE).

Caution Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access, that user is unable to configure MSE settings.

h) Click Save to add the new user to the MSE.

Step 5 If you want to delete a user from an MSE, follow these steps:
a) From the left sidebar menu, choose Systems > Accounts > Users.
b) Select the check box(es) of the user(s) that you want to delete.
c) From the Select a command drop-down list, choose Delete User.

d) Click Go.
e) Click OK to confirm that you want to delete the selected users.

Step 6 If you want to change user properties, follow these steps:
a) Click the username of the user that you want to edit.
b) Make the required changes to the Password, Group Name, and Permission text boxes.
c) Click Save to apply your change.

Configure MSE User Groups to Control Read-Write Access

You can control the Read-Write access of the MSE User group using the following procedure.

Step 1 Choose Services > Mobility Services > Mobility Services Engines.
Step 2 Click the device name of the MSE that you want to edit.
Step 3 From the left sidebar menu, choose Systems > Accounts > Groups.
Step 4 If you want to add a user group to an MSE, do the following:
a) From the Select a command drop-down list, choose Add Group.
b) Click Go.
c) Enter the name of the group in the Group Name text box.
d) Choose a permission level from the Permission drop-down list.

There are three permissions levels to choose from:

- Read Access
- Write Access
- Full Access (required for to access mobility services engines)

e) Click Save to add the new group to the MSE.

Caution Group permissions override individual user permissions. For example, if you give a user full access and add that user to a group with read access permission, that user cannot configure MSE settings.

Step 5 If you want to delete a user group from an MSE, do the following:
a) Select the check box(es) of the group(s) that you want to delete.
b) From the Select a commanddrop-down list, choose Delete Group.
c) Click Go.
d) Click OK to confirm that you want to delete the selected users.

Step 6 If you want to change user group permissions, do the following:
a) Click the group name of the group that you want to edit.
b) Choose a permission level from the Permission drop-down list.
c) Click Save to apply your change.

Caution Group permissions override individual user permissions. For example, if you give a user permission for full access and add that user to a group with read access, that user is unable to configure MSE settings.

Monitor the MSE and Product Servers

The System > Status page enables you to monitor server events, alarms and events, and NMSP connection status for the MSE.

To view a list of server events, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the applicable MSE.

Step 3 From the left sidebar menu, choose System > Status > Server Events.

The Status > Server Events page provides the following information:

- Timestamp—Time of the server event.
- Severity—Severity of the server event.
- Event—Detailed description of the event.
- Facility—The facility in which the event took place.

View product-related MSE Alarms

You can view the audit logs for User-triggered operations using the Audit Logs option available in an MSE. To view the audit logs, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the applicable MSE.

Step 3 From the left sidebar menu, choose System > Status > Audit Logs.

The Status > Audit Logs page provides the following information:

- Username—The Username which has triggered the audit log.
- Operation—The operation that has been performed by the User.
- Operation Status—The status of the operation and it can be SUCCESSFUL or FAILED.
- Invocation Time—The date and time at which the audit log was recorded for the specified operation.

View MSE Alarms and Events

To view a list of alarms and events, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu:

- Choose System > Status > Prime Infrastructure Alarms, to view the alarms.
- Choose System > Status > Prime Infrastructure Events, to view the events.

Find and Troubleshoot MSE-Product Out-of-Sync Alarms

Out-of-sync alarms are of Minor severity (yellow) and are raised in response to the following conditions:

- Elements have been modified in (the auto-sync policy pushes these elements).
- Elements have been modified in the MSE.
- Elements except controllers exist in the MSE database but not in .
- Elements have not been assigned to any MSE (the auto-sync policy does not apply).

Out-of-sync alarms are cleared when the following occurs:

- The MSE is deleted

When you delete an MSE, the out-of-sync alarms for that system is also deleted. In addition, if you delete the last available MSE, the alarms for "elements not assigned to any server" are also deleted.

- Elements are synchronized manually or automatically
- User manually clears the alarms (although the alarms might reappear the future when the scheduled task is next executed)

By default, out-of-sync alarms are enabled. You can disable them in by choosing Administration > System Settings > Alarms and Events, and clicking Mobility Service Synchronization, unselecting the Auto Synchronization check box, and clicking Submit.

Monitor the Connection Status Between Controllers and MSEs

The NMSP Connection Status page allows you to verify the NMSP connection between the MSE and the Cisco controller to which the MSE is assigned.

Network Mobility Services Protocol (NMSP) is the protocol that manages communication between the mobility service and the controller.

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu, choose System > Status > NMSP Connection Status.

The NMSP Connection Status page shows the following information:

- Summary—The Summary section shows each device type, the total number of connections, and the number of inactive connections.
- NMSP Connection Status—This group box shows the following:

IP address—Click the device IP address to view NMSP connection status details for this device. See the Monitor the Connection Status Between a Specific Device and MSE, on page 800, for additional information.

- Target Type—Indicates the device to which the NMSP connection is intended.
- Version—Indicates the current software version for the device.
- NMSP Status—Indicates whether the connection is active or inactive.
- Echo Request Count—Indicates the number of echo requests that were sent.
- Echo Response Count—Indicates the number of echo responses that were received.
- Last Message Received—Indicates the date and time of the most recent message received.

Step 4 Verify that the NMSP Status is ACTIVE.

- If active, you can view details on wired switches, controllers, and wired clients.
- If not active, resynchronize device and the MSE.

You can launch an NMSP troubleshooting tool for an inactive connection.

Related Topics

Troubleshoot NMSP Connection Status, on page 783

Monitor the Connection Status Between a Specific Device and MSE

To view NMSP Connection Status details, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the applicable mobility service.

Step 3 From the left sidebar menu, choose System > Status > NMSP Connection Status.

Step 4 Click the device IP address to open the NMSP Connection Status Details page. The Details page shows the following information:

- Summary
  - IP Address
  - Version—The current software version for the device.
  - Target Type—The device to which the NMSP connection is intended.
  - NMSP Status—Indicates whether the connection is active or inactive.
  - Echo Request Count—The number of echo requests that were sent.
  - Echo Response Count—The number of echo responses that were received.
  - Last Activity Time—The date and time of the most recent message activity between the device and the MSE.
  - Last Echo Request Message Received At—The date and time the last echo request was received.
  - Last Echo Response Message Received At—The date and time the last echo response was received.
  - Model—The device model.
  - MAC Address—The MAC address of the device, if applicable.
  - Capable NMSP Services—Indicates the NMSP-capable services for this device such as ATTACHMENT or LOCATION.
- Subscribed Services—Indicates subservices for each subscribed NMSP service. For example, MOBILE_STATION_ATTACHMENT is a subservice of ATTACHMENT.
- Messages

- Message Type—Message types might include: ATTACHMENT_NOTIFICATION, ATTACHMENT_REQUEST, ATTACHMENT_RESPONSE, CAPABILITY_NOTIFICATION, ECHO_REQUEST, ECHO_RESPONSE, LOCATION_NOTIFICATION, LOCATION_REQUEST, SERVICE_SUBSCRIBE_REQUEST, SERVICE_SUBSCRIBE_RESPONSE.
- In/Out—Indicates whether the message was an incoming or outgoing message.
- Count—Indicates the number of incoming or outgoing messages.
- Last Activity Time—The date and time of the most recent activity or message.
- Bytes—Size of the message in Bytes.

Configure Settings for MSE Database Backups

To view or edit mobility service backup parameters, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose Maintenance > Backup.

- Backups located at—Indicates the location of the backup file.
- Enter a name for the Backup—Enter or edit the name of the backup file.
- Timeout (in secs)—Indicates the length of time (in seconds) before attempts to back up files times out.

Back Up MSE Historical Data to the product Server

contains functionality for backing up MSE data.

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the MSE that you want to back up.

Step 3 From the left sidebar menu, choose Maintenance > Backup.

Step 4 Enter the name of the backup.

Step 5 Enter the time in seconds after which the backup times out.

Step 6 Click Submit to back up the historical data to the hard drive of the server running .

Status of the backup can be seen on the page while the backup is in process. Three items are displayed on the page during the backup process: (1) Last Status field provides messages noting the status of the backup; (2) Progress field shows what percentage of the backup is complete; and (3) Started at field shows when the backup began noting date and time.

You can run the backup process in the background while working on other MSE operations in another page.

Backups are stored in the FTP directory that you specify during the installation. However, in the installation, the FTP directory is not specified. It might be necessary to provide the full path of the FTP root.

Restore MSE Historical Data from the Product Server

To restore a file back into the mobility service, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose Maintenance > Restore.

Step 4 Choose the file to restore from the drop-down list.

Step 5 Select the Delete synchronized service assignments check box if you want to permanently remove all service assignments from the MSE.

This option is applicable for network designs, wired switches, controllers and event definitions. The existing location history data is retained, however you must use manual service assignments to perform any future location calculations.

Step 6 Click Submit to start the restoration process.

Step 7 Click OK to confirm that you want to restore the data from the server hard drive.

When the restoration is complete, shows a message to that effect.

You can run the restore process in the background while working on other MSE operations in another page.

Download Software to MSEs

To download software to an MSE using , follow these steps:

Step 1 Verify that you can ping the location appliance from or an external FTP server, whichever you are going to use for the application code download.

Step 2 Choose Services > Mobility Services > Mobility Services Engines.

Step 3 Click the name of the MSE to which you want to download software.

Step 4 On the left sidebar menu, choose Maintenance.

Step 5 Click Download Software and do one of the following:

- To download software listed in directory, select the Select from uploaded images to transfer into the Server check box. Then, choose a binary image from the drop-down list.

  downloads the binary images listed in the drop-down list into the FTP server directory you specified during the installation.

  In the installation, FTP directory is not specified. It might be necessary to give the full path of the FTP root.

- To use downloaded software available locally or over the network, select the Browse a new software image to transfer into the Server check box and click Browse. Locate the file and click Open.

Step 6 Enter the time, in seconds (between 1 and 1800), after which the software download times out.

Step 7 Click Download to send the software to the /opt/installers directory on the MSE.

Configure MSE Partner Systems to Improve Navigation for Mobile Devices (Qualcomm PDS)

The System > Partner Systems page enables you to do MSE-Qualcomm PDS configuration. This configuration is aimed at providing better navigation capability for the mobile devices. The Partner Discovery Server (PDS) generates encrypted assistance data using the floor plan and AP data which is provided by the MSE. The PDS converts this information into an optimized format that will be used by Qualcomm smart phones.

Configure Qualcomm PDS to Work with MSE

To configure Qualcomm PDS for MSE, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the mobility services.

Step 3 From the left sidebar menu, choose System > Partner Systems.

The Qualcomm PDS Configuration for MSE page appears.

Step 4 If you want o enable MSE-Qualcomm communication, then select the Enable Qualcomm check box.

Step 5 In the Qualcomm PDS Endpoint text box, enter the Qualcomm PDS server URL. This is the URL of the PDS from where you can fetch data assistance. The default URL is http://207.114.133.174:8000/AssistanceDataMgr/AssistanceDataMgrSOAP?wsdl.

Step 6 In the MSE URL to request assistance data text box, enter the MSE URL. This is the URL at which the MSE is accessible by the devices at the venue.

Step 7 In the Cisco Mobile Concierge SSID text box, enter the Mobile Concierge SSID information of the venue to which mobile clients should connect. The Qualcomm smart phones will associate this SSID and communicate with MSE.

Step 8 Enter the venue description in the Venue Description text box.

Step 9 Enter refresh time period for assistance data for MSE in the Refresh time period for assistance data on MSE text box.

Step 10 Enter refresh time period for assistance data for mobile clients in the Refresh time period for assistance data on mobile clients text box.

Step 11 Select the Include Copyright Information check box if the messages/assistance data sent to Qualcomm PDS server and mobile clients should be copyrighted.

Step 12 In the Copyright Owner text box, enter the copyright owner information that has to be included.

Step 13 Enter the copyright year to be included in the Copyright Year text box.

Step 14 Click Save to save the configuration and Cancel to go back.

How Qualcomm PDS Works with MSE

The MSE-Qualcomm configuration involves the following steps:

- Generate Map Extraction Tool (MET) output from CAD file.
- Input MET Output into .
- Addition of GPS Markers.
- Synchronize the Floor to MSE.
- Provide Qualcomm QUIPS/PDS and Copyright Information.
- On MSE, perform F2 Interface request to Qualcomm PDS server.

Qualcomm's MET is an application that allows you to customize and select various layers from a map file (DXF file) and generates a zip file containing:

- Image file (.PNG format) to be used as floor map on .
- Span.xml file that contains the dimensions of the floor (horizontal and vertical) in meters.
- Qualcomm specific map XML file containing geometric feature information related to walls, doors, points of interest, and so on.

Note MET application is independent of and MSE and can reside an any host machine. Only the output of MET is used as MAP related input information on .

Step 1 Start Qualcomm MET tool by following the steps in ReadMe.txt within the MET Tool folder.

Step 2 Input the DXF File in the Map Extraction Tool.

Step 3 Select necessary layers from the left sidebar menu.

Step 4 Save the output of Map Extraction Tool to desired location on the Map Extraction Tool user interface.

Configure the MSE wIPS Service Administrative Settings

The wIPS Service page allows you to view or manage wIPS service administrative settings.

Note Cisco Adaptive wIPS functionality is not supported for non-root partition users.

To view or manage wIPS service administration settings, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Choose the device name of the applicable MSE.

Step 3 From the left sidebar menu, choose wIPS Service.

Step 4 View or edit the following parameters:

- Log level—Choose the applicable log level from the drop-down list. Log levels include Debug, Error, Important Event, Major Debug, None, and Warning.
- Forensic size limit (GB)—Enter the maximum allowable size of forensic files.
- Alarm ageout (hours)—Enter the age limit, in hours, for each alarm.
- Device ageout (days)—Enter the age limit, in days, for the device to send alarms.

Step 5 Click Save to confirm the changes or Cancel to close the page with no changes applied.

Improve Tracking with MSE Context-Aware Service (Location Services)

Context-Aware Service (CAS) software allows an MSE to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location, temperature and asset availability about a client or tag (Cisco CX version or later) from Cisco access points.

CAS relies on two engines for processing the contextual information it receives. The Context-Aware Engine for Clients processes data received from Wi-Fi clients and the Context-Aware Engine for Tags processes data received from Wi-Fi tags; these engines can be deployed together or separately depending on the business need.

Mobility services engines do not track or map non-Cisco CX tags.

CAS was previously referred to as Cisco location-based services.

You can modify Context-Aware Service Software properties as to the type and number of clients or tags that are tracked and whether or not locations are calculated for those clients or tags.

You can also modify parameters that affect the location calculation of clients and tags such as Received Signal Strength Indicator (RSSI) measurements.

After its installation and initial configuration are complete, the MSE can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated to communicate with each MSE to transfer and display selected data.

You can configure the MSE to collect data for clients, rogue access points, rogue clients, mobile stations, interferers, and active RFID asset tags.

Prerequisites for using MSE CAS, Improve Tracking with MSE Context-Aware Service (Location Services)

Before you can use to view contextual information, initial configuration for the MSE is required using a command-line interface (CLI) console session. See the Cisco 3355 Mobility Services Engine Getting Started Guide and the Cisco 3100 MSE Getting Started Guide at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html.

Licensing for Clients and Tags

You must purchase licenses from Cisco to retrieve contextual information on tags and clients from access points.

- Licenses for tags and clients are offered separately.
- The clients license also contains tracking of rogue clients and rogue access points, and interferers (if enabled).
- Licenses for tags and clients are offered in a variety of quantities, ranging from 1,000 to 12,000 units.

The AeroScout Context-Aware Engine for Tags support 100 permanent tag licenses; Context-Aware Services consists of permanent tag licenses.

Note See the Release Notes for Cisco 3300 Series Mobility Services Engine for Software Release 6.0 at the following URL: http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html for more information on tags and client licenses.

Context-Aware Service General Parameters

To access the Context Aware Service > General page,follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Choose General from the left sidebar menu.

This page provides the following information:

- Version
- Operational Status
- Number of Tracked Wireless Clients
- Number of Traced Tags
- Number of Tracked Rogue APs
- Number of Tracked Rogue Clients
- Number of Tracked Interferers
- Number of Tracked Wired Clients
- Total Elements Tracked
- Tracked Elements (Wireless Clients, Rogue APs, Rogue Clients, Interferers, and Wired Clients) Limit
- Tracked Tags Limit

Clients represent a snapshot of client count every 15 minutes. Peak Clients is the peak count during that15-minute time period. For example, in a 15-minute time period, the client count varies from 100 to 300. When polls MSE, MSE returns the client count as the count at that exact time, which could be any number between 100 to 300, and the Peak Client Count as 300.

Enable and Configure Context-Aware Service Settings on an MSE

The MSE can track up to 25,000 clients or up to 25,000 tags (with the proper license purchase). Updates on the locations of elements being tracked are provided to the MSE from the Cisco wireless LAN controller.

Only those elements designated for tracking by the controller are viewable in Prime Infrastructure maps, queries, and reports. No events and alarms are collected for non-tracked elements and none are used in calculating the 25,000 element limit for clients or tags.

You can modify the following tracking parameters using Prime Infrastructure:

- Enable and disable element locations (client stations, active asset tags, interferers, wired clients, rogue clients, and rogue access points) you actively track.
    - Wired client location tracking enables servers in a data center to more easily find wired clients in the network. Servers are associated with wired switch ports in the network.

- Set limits on how many of specific elements you want to track.

For example, given a client license of 12,000 trackable units, you can set a limit to track only 8,000 client stations (leaving 4,000 units available to track rogue clients and rogue access points). Once the tracking limit is met for a given element, the number of elements not being tracked is summarized in the Tracking Parameters page.

- Disable tracking and reporting of ad hoc rogue clients and access points.

To configure tracking parameters for an MSE, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines to open the Mobility Services page.

Step 2 Click the name of the MSE whose properties you want to edit. The General Properties page appears.

Step 3 Choose Context-Aware Software > Tracking Parameters from the Administration subheading to display the configuration options.

Step 4 Modify the following tracking parameters as appropriate (see the following table).

Table 80: Tracking Parameters

Field	Configuration Options
Tracking Parameters	
Wired Clients	a. Select the Enable check box to enable tracking of client stations by the MSE. In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers. The wired client limiting is supported from MSE 7.0 and Prime Infrastructure 1.0. In other words, you can limit wired clients to a fixed number, say 500. This limit is set to ensure that the licenses are not taken up completely by wired clients and some licenses are available for other devices. **Caution** When upgrading the MSE from 6.0 to 7.0, if any limits have been set on wireless clients or rogues, they reset because of the wired client limit change in 7.0. **Note** Active Value (Display only): Indicates the number of wired client stations currently being tracked. **Note** Not Tracked (Display only): Indicates the number of wired client stations beyond the limit.
Wireless Clients	a. Select the Enable check box to enable tracking of client stations by the MSE. b. Select the Enable Limiting check box to set a limit on the number of client stations to track. c. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of clients that can be tracked by an MSE. **Note** The actual number of tracked clients is determined by the license purchased. **Note** Active Value (Display only): Indicates the number of client stations currently being tracked. **Note** Not Tracked (Display only): Indicates the number of client stations beyond the limit.

Field	Configuration Options
Rogue Access Points	a. Select the Enable check box to enable tracking of rogue clients and asset points by the MSE. b. Select the Enable Limiting check box to set a limit on the number of rogue clients and asset tags stations to track. c. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of rogue clients and access points that can be tracked by an MSE. **Note** The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license. **Note** Active Value (Display only): Indicates the number of rogue clients and access points currently being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue clients and access points beyond the limit.
Exclude Ad-Hoc Rogues	Select the check box to turn off the tracking and reporting of ad hoc rogues in the network. As a result, ad hoc rogues are not displayed on Prime Infrastructure maps or its events and alarms reported.
Rogue Clients	a. Select the Enable check box to enable tracking of rogue clients by the MSE. b. Select the Enable Limiting check box to set a limit on the number of rogue clients to track. c. Enter a Limit Value, if limiting is enabled. The limit entered can be any positive value up to 25,000 which is the maximum number of rogue clients that can be tracked by an MSE. **Note** The actual number of tracked rogues (clients and access points) is driven by the client license purchased. The user must consider the number of clients that are being tracked in determining the available quantity to allocate to track rogue clients and access points because clients and rogue clients and access points are addressed by the same license. **Note** Active Value (Display only): Indicates the number of rogue clients being tracked. **Note** Not Tracked (Display only): Indicates the number of rogue clients beyond the limit.
Interferers	a. Select the Enable check box to enable tracking of the interferers by the MSE. In 7.0, the client license encompasses all network location service elements and is shared among wireless clients, wired clients, rogue clients, access points, and interferers. **Note** Active Value (Display only): Indicates the number of interferers currently being tracked. **Note** Not Tracked (Display only): Indicates the number of interferers beyond the limit.
Asset Tracking Elements	
Active RFID Tags	a. Select the Enable check box to enable tracking of active RFID tags by the MSE. **Note** The actual number of tracked active RFID tags is determined by the license purchased. **Note** Active Value (Display only): Indicates the number of active RFID tags currently being tracked. It also depends on the tag engine chosen. **Note** Not Tracked (Display only): Indicates the number of active RFID tags beyond the limit.

Field	Configuration Options
SNMP Parameters Not applicable to mobility services 7.0.105.0 and later.	
SNMP Retry Count	Enter the number of times to retry a polling cycle the default value is 3. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)
SNMP Timeout	Enter the number of seconds before a polling cycle times out, the default value is 5. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)
SNMP Polling Interval	
Client Stations	Select the Enable check box to enable client station polling and enter the polling interval in seconds. Default value is 300. Allowed values are from 1 to 99999. (Configurable in controller Release 4.1 and earlier only.)
Active RFID Tags	Select the Enable check box to enable active RFID tag polling and enter the polling interval in seconds. Allowed values are from 1 to 99999. **Note** Before the mobility service can collect asset tag data from controllers, you must enable the detection of active RFID tags using the config rfid status enable CLI command on the controllers.
Rogue Clients and Access Points	Select the Enable check box to enable rogue access point polling and enter the polling interval in seconds. Default value is 600. Allowed values are from 1 to 99999.(Configurable in controller Release 4.1 and earlier only.)
Statistics	Select the Enable check box to enable statistics polling for the mobility service, and enter the polling interval in seconds. Default value is 900. Allowed values are from 1 to 99999.(Configurable in controller Release 4.1 and earlier only.)

Step 5 Click Save to store the new settings in the MSE database.

Customize Which MSE Assets Are Tracked Using Context-Aware Service Filters

You can limit the number of asset tags, wired clients, rogue clients, interferers and access points whose location is tracked by filtering on the following:

- MAC addresses

Specific MAC addresses can be entered and labeled as allowed or disallowed from location tracking. You can import a file with the MAC addresses that are to be allowed or disallowed, or you can enter them individually in the GUI page.

The format for entering MAC addresses is xx:xx:xx:xx:xx:xx. If a file of MAC addresses is imported, the file must follow a specific format as follows:

- Each MAC address should be listed on a single line.

- Allowed MAC addresses must be listed first and preceded by an "[Allowed]" line item. Disallowed MAC addresses must be preceded by "[Disallowed]."
- Wildcard listings can be used to represent a range of MAC addresses. For example, the first entry "00:11:22:33:*" in the Allowed listing that follows is a wildcard.

Note Allowed MAC address formats are viewable in the Filtering Parameters configuration page. See the following table for details.

EXAMPLE file listing:

[Allowed]00:11:22:33:*22:cd:34:ae:56:4502:23:23:34:*[Disallowed]00:10:*ae:bc:de:ea:45:23

- Probing clients

Probing clients are clients that are associated to another controller but whose probing activity causes them to be seen by another controller and be counted as an element by the "probed" controller as well as its primary controller.

To configure filtering parameters for an MSE, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines. The Mobility Services page appears.

Step 2 Click the name of the MSE whose properties you want to edit. The General Properties page appears.

Step 3 From the Context-Aware Software menu, choose Filtering Parameters from the Administration subheading to display the configuration options.

Step 4 Modify the following filtering parameters as appropriate (see the following table).

Table 81: Filtering Parameters

Field	Configuration Options
Advanced Filtering Parameters	
Duty Cycle Cutoff Interferers	Enter the duty cycle cutoff value for interferers so that only those interferers whose duty cycle meets the specified limits are tracked and counted against the Base location license. The default value for the Duty Cycle Cutoff Interferers is 0% and the configurable range is from 0% to 100%. To better utilize the location license, you can choose to specify a filter for interferers based on the duty cycle of the interferer.
MAC Filtering Parameters	
Exclude Probing Clients	Select the check box to prevent location calculation of probing clients.

Field	Configuration Options
Enable Location MAC Filtering	a. Select the check box to enable MAC filtering of specific elements by their MAC address. b. To import a file of MAC addresses (Upload a file for Location MAC Filtering field), browse for the filename and click Save to load the file. The imported list of MAC addresses auto-populates the Allowed List and Disallowed List based on their designation in the file. **Note** To view allowed MAC address formats, click the red question mark next to the Upload a file for Location MAC Filtering field. a. To add an individual MAC address, enter the MAC addresses (format is xx:xx:xx:xx:xx:xx) and click either Allow or Disallow. The address appears in the appropriate column. **Note** To move an address between the Allow and Disallow columns, highlight the MAC address entry and click the button under the appropriate column. **Note** To move multiple addresses, click the first MAC address and press Ctrl to highlight additional MAC addresses. Click Allow or Disallow based on its desired destination. **Note** If a MAC address is not listed in the Allow or Disallow column, by default, it appears in the Blocked MACs column. If you click the Unblock button, the MAC address automatically moves to the Allow column. You can move it to the Disallow column by selecting the Disallow button under the Allow column.

Step 5 Click Saveto store the new settings in the MSE database.

Configure Settings for Saving Client Stations, Rogue Clients, and Asset Tags Historical Information

You can use to specify how long to store (archive) histories on client stations, rogue clients, and asset tags. These histories are received from those controllers that are associated with the mobility service.

You can also program the mobility service to periodically remove (prune) duplicate data from its historical files to reduce the amount of data stored on its hard drive.

To configure mobility service history settings, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose Context Aware Service > History Parameters.

Step 4 Modify the following history parameters as appropriate (see the following table).

Table 82: History Parameters

Field	Description
Archive for	Enter the number of days for the location appliance to retain a history of each enabled category. The default value is 30. Allowed values are from 1 to 99999.

Field	Description
Prune data starting at	Enter the number of hours and minutes at which the location appliance starts data pruning (between 0 and 23 hours, and between 1 and 59 minutes). Enter the interval, in minutes, after which data pruning starts again (between 0, which means never, and 99900000). The default start time is 23 hours and 50 minutes, and the default interval is 1440 minutes.
Enable History Logging of Location Transitions for	To enable history logging of Location transitions, choose one or more of the following: • Client Stations • Wired Stations • Asset Tags • Rogue Clients • Rogue Access Points • Interferers **Note** Before the mobility service can collect asset tag data from controllers, you must enable the detection of RFID tags using the config rfid status enable CLI command.

Step 5 Click Save to store your selections in the location appliance database.

Enable MSE Location Presence to Enhance Location Information

You can enable location presence on the MSE to provide expanded Civic (city, state, postal code, country) and GEO (longitude, latitude) location information beyond the Cisco default setting (campus, building, floor, and X, Y coordinates). This information can then be requested by wireless and wired clients on a demand basis for use by location-based services and applications.

You can also import advanced location information such as the MAC address of a wired client and the wired switch slot and port to which the wired client is attached.

Location Presence can be configured when a new Campus, Building, Floor or Outdoor Area is being added or configured at a later date.

Once enabled, the MSE is capable of providing any requesting Cisco CX v5 client its location.

Note Before enabling this feature, synchronize the MSE.

To enable and configure location presence on an MSE, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Select the MSE to which the campus or building or floor is assigned.

Step 3 From the left sidebar menu, choose Context Aware Services > Administration > Presence Parameters.

Step 4 Select the Service Type On Demand check box to enable location presence for Cisco CX clients v5.

Step 5 Select one of the following Location Resolution options:

a) When Building is selected, the MSE can provide any requesting client, its location by building.

For example, if a client requests its location and the client is located in Building A, the MSE returns the client address as Building A.

b) When AP is selected, the MSE can provide any requesting client, its location by its associated access point. The MAC address of the access point appears.

For example, if a client requests its location and the client is associated with an access point with a MAC address of 3034:00hh:0adg, the MSE returns the client address of 3034:00hh:0adg.

c) When X,Y is selected, the MSE can provide any requesting client, its location by its X and Y coordinates.

For example, if a client requests its location and the client is located at (50, 200) the MSE returns the client address of 50, 200.

Step 6 Select any or all of the location formats:

a) Select the Cisco check box to provide location by campus, building and floor and X and Y coordinates. Default setting.
b) Select the Civic check box to provide the name and address (street, city, state, postal code, country) of a campus, building, floor, or outdoor area.
c) Select the GEO check box to provide the longitude and latitude coordinates.

Step 7 By default, the Location Response Encoding check box is selected. It indicates the format of the information when received by the client. There is no need to change this setting.

Step 8 Select the Retransmission Rule check box to allow the receiving client to retransmit the received information to another party.

Step 9 Enter a Retention Expiration value in minutes. This determines how long the received information is stored by the client before it is overwritten. The default value is 24 hours (1440 minutes).

Step 10 Click Save.

Import and Export MSE Asset, Chokepoint, and TDOA Receiver Information to an MSE

To import asset, chokepoint, and TDOA receiver information for the MSE using follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 To import information for an MSE:

a) Click the name of the MSE for which you want to import information.
b) Choose Context Aware Service > Administration > Import Asset Information.
c) Enter the name of the text file or browse for the filename.

Specify information in the imported file in the following formats:

- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

d) When the import filename is located in the Browse text box, click Import.

Step 3 To export asset, chokepoint, and TDOA receiver information from the MSE to a file using :

a) Click the name of the MSE from which you want the export information.

b) Choose Context Aware Services > Administration > Export Asset Information.

Information in the exported file is in the following formats:

- tag format: #tag, 00:00:00:00:00:00, categoryname, groupname, assetname
- station format: #station, 00:00:00:00:00:00, categoryname, groupname, assetname

c) Click Export.

Click Open (display to screen), Save (to external PC or server), or Cancel (to cancel the request).

If you select Save, you are asked to select the asset file destination and name. The file is named assets.out by default. Click Close in the dialog box when the download is complete.

Import Civic Address Information to an MSE

To import civic information for the MSE using , follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the MSE for which you want to import asset information.

Step 3 From the left sidebar menu, choose Context Aware Software.

Step 4 From the Administration left sidebar menu, choose Import Civic Information.

Step 5 Enter the name of the text file or browse for the filename.

Information in the imported file should be one of the following formats:

Switch IP Address, Slot Number, Port Number, Extended Parent Civic Address, X, Y, Floor ID, Building ID, Network Design ID, ELIN:”ELIN”, PIDF-Lo-Tag:”Civic Address Element Value”

Each entry must appear on a separate line.

Step 6 Click Import.

View Details About the Wired Switches and Clients That Are Synchronized with an MSE

This section describes the Context Aware Service > Wired drop-down list parameters.

View Wired Switches That Are Synchronized with an MSE (CAS)

You can review details on the wired switch (IP address, MAC address, serial number, software version, and ELIN), its port, its wired clients (count and status), and its civic information.

Wired switch data is downloaded to the MSE through when the Ethernet switch and the MSE are synchronized (Services > Synchronize Services > Switches). Communication between a location-capable switch and the MSE is over NMSP. and the MSE communicate over XML.

To view details on wired switches, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the device name link of the appropriate wired location switch.

Step 3 Choose Context Aware Service > Wired > Wired Switches. A summary of wired switches that are synchronized with the MSE appears.

Step 4 Click the IP address link for the applicable wired switch. The Wired Switch Details page appears.

The Wired Switch Details page has four tabs: Switch Information, Switch Ports, Civic, and Advanced.

You can export civic information from the switch by choosing that option from the Select a command drop-down list. This option is available in all four dashlets of the Wired Switches page.

The Wired Switch Details tabs shows the following information:

- Switch Information—Displays a total count summary of wired clients connected to the switch along with the state of the client (connected, disconnected, and unknown).
  - Connected clients—Clients that are connected to the wired switch.
  - Disconnected clients—Clients that are disconnected from the wired switch.
  - Unknown clients—Clients are marked as unknown when the NMSP connection to the wired switch is lost.

You can view detailed wired client information by clicking in one of the client count links (total clients, connected, disconnected, and unknown). See View Wired Clients That Are Synchronized with an MSE (CAS), on page 815 for more information.

- Switch Ports—Displays a detailed list of the ports on the switch.

You can change the listing order (ascending, descending) of port IP addresses, slot numbers, module number, port type, and port number by clicking in the respective column heading.

- Civic—Displays a detailed list of the civic information for the wired switch.
- Advanced—Displays a detailed list of the additional civic information for the wired switch.

View Wired Clients That Are Synchronized with an MSE (CAS)

You can view details on a wired client (MAC address, IP address, username, serial number, UDI, model no., software version, VLAN ID, and VLAN ID), port association, and its civic information.

Wired client data is downloaded to the MSE through when the switch and the MSE are synchronized (Services > Synchronize Services > Switches).

and the MSE communicate over XML.

You can view the details of the wired client on either the wired switches page (Context Aware Service > Wired > Wired Switches) or wired clients page (Context Aware Service > Wired > Wired Clients).

- If you know the IP address, MAC address, VLAN ID, serial number, or username, you can use the search field on the wired clients page.
- If you want to examine wired clients as they relates to a specific switch, you can view that information on the wired switches page. See View Wired Switches That Are Synchronized with an MSE (CAS), on page 814 for more information.

To view details on a wired client, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the device name link of the appropriate MSE.

Step 3 Choose Context Aware Service > Wired > Wired Clients.

In the Wired Clients summary page, clients are grouped by their switch.

A client status is noted as connected, disconnected, or unknown:

- Connected clients—Clients that are active and connected to a wired switch.
- Disconnected clients—Clients that are disconnected from the wired switch.
- Unknown clients—Clients that are marked as unknown when the NMSP connection to the wired switch is lost. See Monitor the Connection Status Between Controllers and MSEs, on page 799 for more information about NMSP connections.

If you know the MAC address of the wired client, you can click that link to reach the detail page of the client or use the search field.

You can also search for a wired client by its IP address, username, or VLAN ID.

If you click the IP address of the switch, you are forwarded to the detail page of the switch. See View Wired Switches That Are Synchronized with an MSE (CAS), on page 814 for more information.

Step 4 Click the MAC address link for the applicable wired client. The Wired Client Details page appears.

The Wired Client Details page has four tabs: Device Information, Port Association, Civic Address, and Advanced.

The Wired Switch Details tabs show the following information:

- Device Information—Display MAC and IP address, username, serial and model number, UDI, software version, VLAN ID, and VLAN name.
- Port Association—Displays the physical location of the switch port/slot/module on which the wired client terminates, the client status (connected, disconnected, unknown), and the switch IP address.
- Civic Address—Displays any civic address information.
- Advanced—Displays extended physical address details for the wired clients, if applicable.

A client takes on the civic address and advanced location information that is configured for the port on which the client terminates. If no civic and advanced information is defined for the its port (port/slot/module) then no location data is displayed.

Configure MSE CAS to Send Tag Notifications to Third-Party (Northbound) Applications

Northbound notifications define which tag notifications the MSE sends to third-party applications.

To configure northbound parameters, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the MSE you want to configure.

Step 3 Choose Context Aware Service > Advanced > Notification Parameters to display the configuration options.

Step 4 Select the Enable Northbound Notifications check box to enable the function.

Step 5 Select the Notification Contents check box to send notifications to third-party applications (northbound).

Step 6 Select one or more of the Notification Contents check boxes.

Step 7 Select the Notification Triggers check box.

Step 8 Select one or more of the Notification Triggers check boxes.

Step 9 Enter the IP address or hostname and port for the system that is to receive the northbound notifications.

Step 10 Choose the transport type from the drop-down list.

Step 11 Select the HTTPS check box if you want to use HTTPS protocol for secure access to the destination system.

Step 12 To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of this page. See the following table.

Table 83: User-Configurable Conditional and Northbound Notifications Fields

Field	Configuration Options
Rate Limit	Enter the rate, in milliseconds, at which the MSE generates notifications. A value of 0 (default) means that the MSE generates notifications as fast as possible (Northbound notifications only).
Queue Limit	Enter the event queue limit for sending notifications. The MSE drops any event above this limit.
Retry Count	Enter the number of times to generate an event notification before the refresh time expires. This parameter can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification may be lost in transit. Default value is 1. **Note** The MSE does not store events in its database.
Refresh Time	Enter the wait time in minutes that must pass before a notification is resent. For example, if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time. Default value is 0 minutes.
Drop Oldest Entry on Queue Overflow	(Read-only). The number of event notifications dropped from the queue since startup.
Serialize Events per Mac address per Destination	Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner.

Step 13 Click Save.

Set MSE CAS Location Parameters

You can use to specify whether the mobility service retains its calculation times and how soon the mobility service deletes its collected Received Signal Strength Indicator (RSSI) measurement times. You can also apply varying smoothing rates to manage location movement of an element.

To configure location parameters, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the mobility service whose properties you want to edit.

Step 3 From the left sidebar menu, choose Context Aware Service > Location Parameters.

Step 4 Modify the location parameters as appropriate (See Cisco Prime Infrastructure 3.2 Reference Guide).

Step 5 Click Save to store your selections in Prime Infrastructure and mobility service databases.

Set MSE CAS Event Notifications

You can use to configure MSE event notification parameters that define such items as how often the notifications are generated or resent by the MSE.

Modify notification parameters only if you expect the MSE to send a large number of notifications or if notifications are not being received.

You can also enable forwarding of northbound notifications for tags to be sent to third-party applications.

The format of northbound notifications sent by the MSE is available on the Cisco developers support portal at the following URL:

http://www.cisco.com/en/US/products/svcs/ps3034/ps5408/ps5418/serv_home.html

To configure notification parameters, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click the name of the MSE you want to configure.

Step 3 From the Context Aware Software left sidebar menu, choose Notification Parameters from the Advanced sub-heading to display the configuration options.

Step 4 Select the Enable Northbound Notifications check box to enable the function.

Step 5 Select the Notification Contents check box to send notifications to third-party applications (northbound).

Step 6 Select one or more of the Notification content options.

Step 7 Select the Notification Triggers check box.

Step 8 Select one or more of the Notification trigger options.

Step 9 Enter the IP address and port for the system that is to receive the northbound notifications.

Step 10 Choose the transport type from the drop-down list.

Step 11 Select HTTPS if you want to use HTTPS protocol for secure access to the destination system.

Step 12 To modify the notification parameter settings, enter the new value in the appropriate text box in the Advanced tab of the page. (See Cisco Prime Infrastructure 3.2 Reference Guide).

Step 13 Click Save.

View Context Aware Partner and Tag Engine Status for MSE

To access the Partner Engine Status page, choose Services > Mobility Services > Mobility Services Engines > MSE Name > Context Aware Service > Partner Engine > Status.

If tag licenses are available, then Aeroscout Tag Engine is enabled. Otherwise, Cisco Partner Engine is enabled by default.

If only the evaluation license is available, then the Cisco Partner Engine is enabled by default. The Partner Engine status page shows status based on whether it is a Aeroscout Tag Engine or Cisco Tag Engine. See Cisco Prime Infrastructure 3.2 Reference Guide.

Note The Aeroscout engine fails to start on MSE if the map names have special characters such as '&'.

View the Notifications Sent By an MSE (CAS)

To view the Notification Summary, choose Services > Mobility Services > Context Aware Service > Notifications Summary.

The mobility service sends event notifications and does not store them (fire and forget). However, if is a destination of notification events, it stores the notifications it receives and groups them into the following seven categories:

- Absence (Missing)—Generated when the mobility service cannot see the asset in the WLAN for the specified time.
- Location Change Events—Generated when client stations, asset tags, rogue clients, and rogue access points move from their previous location.
- Chokepoint Notifications—Generated when a tag is seen (stimulated) by a chokepoint. This information is only reported and displayed for CCX v.1-compliant tags.
- Battery Level—Generated when a tracked asset tag hits the designated battery level.
- In/Out Area—Generated when an asset is moved inside or outside a designated area.

You define a containment area (campus, building, or floor) in the Maps section of . You can define a coverage area using the Map Editor.

- Movement from Marker—Generated when an asset is moved beyond a specified distance from a designated marker you define on a map.
- Emergency—Generated for a CCX v.1 compliant asset tag when the panic button of the tag is triggered or the tag becomes detached, tampered with, goes inactive or reports an unknown state. This information is only reported and displayed for CCX v.1 compliant tags.

The summary details include the following:

- All Notifications
- Client Stations
- Asset Tags
- Rogue Clients
- Rogue Access Points

To view details for each of the notifications, click the number under the Last Hour, Last 24 Hours, or Total Active column to open the details page for the applicable notification.

How MSE Notifications are Cleared (CAS)

A mobility service sends event notifications when it clears an event condition in one of the following scenarios:

- Missing (Absence)—Elements reappear.
- In/Out Area (Containment)—Elements move back in or out of the containment area.
- Distance—Elements move back within the specified distance from a marker.
- Location Changes—Clear state is not applicable to this condition.
- Battery Level—Tags are detected again operating with Normal battery level.
- Emergency

- Chokepoint

In , the Notifications Summary page reflects whether notifications for cleared event conditions have been received.

View the Current Definitions for MSE Notifications (CAS)

To view the Notification Definitions, choose Services > Mobility Services > Context Aware Notifications > Notifications Definition. You can add event groups and event definitions to a group in this page. Every groups help you organize your event notifications. An event definition must belong to a particular group.

For more information on adding event groups and event definitions, see Configure Event Groups for MSE Notifications, on page 822 and Add an MSE Event Definition to an Event Group, on page 825.

The Notification Definition page displays the following parameters only after adding event groups and event definitions:

The following table lists and describes the fields in the Notification Definition page.

Table 84: Notification Definition Page

Field	Description
Group Name	Name of the group to which the event definition is added.
Event Definitions	Existing event definitions for the event group.
Created On	Date on which the event groups are created.

View the Notification Statistics for a Specific MSE (CAS)

You can view the notification statistics for a specific MSE. To view the Notification Statistics for a specific MSE, choose Services > Mobility Services > MSE-name > Context Aware Service > Notification Statistics (where MSE-name is the name of an MSE).

The following table lists and describes the fields in the Notification statistics page.

Table 85: Notification Statistics Fields

Field	Description
Summary	
Destinations	
Total	Total count of the destinations.
Unreachable	Count of unreachable destinations.
Notification Statistics Summary	
Track Definition Status	Status of the track definition. Track notification status can be either Enabled or Disabled.
Track Definition	Track definition can be either Northbound or CAS event notification.

Field	Description
Destination IP Address	The destination IP address to which the notifications are sent.
Destination Port	The destination port to which the notifications are sent.
Destination Type	The type of the destination. For example, SOAP_XML.
Destination Status	Status of the destination device. The status is either Up or Down.
Last Sent	The date and time at which the last notification was sent to the destination device.
Last Failed	The date and time at which the notification had failed.
Total Count	The total count of notifications sent to the destination. Click the count link to view the notification statistics details of the destination device.

View MSE Mobile Concierge Advertisements

To view the configured service advertisements, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click Device Name to view its properties.

Step 3 Choose Mobile Concierge Service > Advertisements from the left sidebar menu.

The following information appears in the Mobile Concierge Service page:

- Icon—Displays an icon associated with the service provider.
- Provide Name—Displays the service providers name.
- Venue Name—Displays the venue name.
- Advertisements
  - Friendly Name—Friendly name that is displayed in the handset.
  - Advertisement Type—Type of advertisement that is displayed in the handset.

View MSE Mobile Concierge Statistics

To view Mobile Concierge service statistics, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Services Engines.

Step 2 Click Device Name to view its properties.

Step 3 Choose Mobile Concierge service > Statistics from the left sidebar menu.

The following information appears in the Mobile Concierge Service page:

- Top 5 Active Mobile MAC addresses—Displays information of the most active mobiles in a given venue.

- Top 5 Service URIs—Displays information of the usage of the services across a given venue or provider.

What are MSE Event Groups?

To manage events more efficiently, you can use to create event groups. Event groups help you organize your event definitions.

Configure Event Groups for MSE Notifications

To add an event group, follow these steps:

SUMMARY STEPS

1. Choose Services > Mobility Services > Context Aware Notifications.
2. Choose Notification Definitions from the left sidebar menu.
3. From the Select a command drop-down list, choose Add Event Group.
4. Click Go.
5. Enter the name of the group in the Group Name text box.
6. Click Save.

DETAILED STEPS

Step 1 Choose Services > Mobility Services > Context Aware Notifications.

Step 2 Choose Notification Definitions from the left sidebar menu.

Step 3 From the Select a command drop-down list, choose Add Event Group.

Step 4 Click Go.

Step 5 Enter the name of the group in the Group Name text box.

Step 6 Click Save.

The new event group appears in the Event Settings page.

Delete Event Groups for MSE Notifications

To delete an event group, follow these steps:

Step 1 Choose Services > Mobility Services > Context Aware Notifications.

Step 2 Choose Notification Definitions from the left sidebar menu.

Step 3 Select the check box of the event group you want to delete.

Step 4 From the Select a command drop-down list, choose Delete Event Group(s).

Step 5 Click Go.

Step 6 Click OK to confirm the deletion.

Step 7 Click Save.

Configure New MSE Events (Event Definitions)

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destinations. This section describes how to add, delete, and test event definitions.

enables you to add definitions on a per-group basis. Any new event definition must belong to a particular group.

To add an event definition, follow these steps:

Step 1 Choose Services > Mobility Services > Context Aware Notifications.

Step 2 From the left sidebar menu, choose Notification Definitions.

Step 3 Click the name of the group to which you want to add the event. An event definition summary page appears for the selected event group.

Step 4 From the Select a command drop-down list, choose Add Event Definition.

Step 5 Click Go.

Step 6 Enter the name of the event definition in the Event Definition Name text box.

The event definition name must be unique within the event group.

Step 7 Click Save.

Step 8 On the General tab, manage the following parameters:

- Admin Status—Enable event generation by selecting the Enabled check box (disabled by default).
- Priority—Set the event priority by choosing a number from the drop-down list. Zero is highest.
- An event definition with higher priority is serviced before event definitions with lower priority.
- Activate—To continuously report events, choose the All the Time check box. To indicate specific days and times for activation, unselect the All the Time check box and choose the applicable days and From/Until times. Click Save.

Step 9 On the Conditions tab, add one or more conditions. For each condition, specify the rules for triggering event notification. To add a condition, follow these steps:

a) Click Add to open the Add/Edit Condition page.

b) Choose a condition type from the Condition Type drop-down list and configure its associated Trigger If parameters see (See the following table).

Table 86: Condition Type/Trigger If Parameters

Condition Type	Trigger If
Missing	Missing for Time (mins)—Enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the MSE generates a missing asset event if the MSE has not located the asset for more than 10 minutes.

Condition Type	Trigger If
In/Out	Inside of or Outside of—Click Select Area and choose the area parameters from the Select page. Click Select. The area to monitor can be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor).
Distance	In the distance of x (feet) from Marker text box—Enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker. Click Select Marker and choose the marker parameters in the Select page. Click Select.
Battery Level	Battery Level Is—Low, Medium, Normal. Select the appropriate battery level that triggers an event.
Location Change	An event is triggered if the location of the asset changes.
Emergency	Select Any, Panic Button, Tampered, or Detached check box.
Chokepoint	In the range of Chokepoints—Click Select Chokepoint check box and choose the chokepoint parameters in the Select page. Click Select.

c) In the Apply To drop-down list, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients or Interferers) for which an event is generated if the trigger condition is met.
d) Emergency and chokepoint events are only applicable to tags (CCXv.1 compliant).
e) From the Match By drop-down list, choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category), the operator (Equals or Like), and enter the relevant text for the selected Match By element.
f) Click Add.

Step 10 On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and configure the transport settings:

a) Click Add to open the Add/Edit Destination and Transport page.
b) To add one or more new destinations, click Add New, enter the applicable IP address, and click OK.
c) The recipient system must have an event listener running to process notifications. By default, when you create an event definition, adds its IP address as the destination.
d) To select a destination to receive notifications, click to highlight one or more IP addresses in the box on the right and click Select to add the IP address(es) to the box on the left.
e) From the Message Format field drop-down list, select XML or Plain Text.
f) If you select as the destination, you must select XML format.
g) Choose one of the following transport types from the Transport Type drop-down list:

- SOAP—Simple Object Access Protocol. Use SOAP to send notifications over HTTP/HTTPS and to be processed by web services on the destination.
- Specify whether to send notifications over HTTPS by selecting its corresponding check box. Enter the destination port number in the Port Number text box.
- Mail—Use this option to send notifications through e-mail.
- Choose the protocol for sending the e-mail from the Mail Type drop-down list. Enter the following: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.
- SNMP—Simple Network Management Protocol. Use this option to send notifications to SNMP-capable devices.
- If you have selected SNMP version v2c then you are prompted to enter the SNMP community string in the SNMP Community text box and the applicable port number in the Port Number text box.

- If you have selected SNMP version v3 then you are prompted to enter the username, security name, choose the authentication type from the drop-down list, enter the authentication password, choose the privacy type from the drop-down list and enter the privacy password.
- SysLog—Specifies the system log on the destination system as the recipient of event notifications.
- Enter the notification priority in the Priority text box, the name of the facility, and the port number on the destination system.

h) Click Add.

Add an MSE Event Definition to an Event Group

An event definition contains information about the condition that caused the event, the assets to which the event applies, and the event notification destination.

enables you to add definitions for each group. An event definition must belong to a group. See the Cisco Content-Aware Software Configuration Guide for more information on deleting or testing event definitions.

To add an event definition, follow these steps:

SUMMARY STEPS

1. Choose Services > Mobility Services > Context Aware Notifications.
2. Choose Notification Definitions from the left sidebar menu.
3. Click the name of the group to which you want to add to the event. An event definition summary page appears for the selected event group.
4. From the Select a command drop-down list, choose Add Event Definition, and click Go.
5. On the Conditions tab, add one or more conditions. For each condition you add, specify the rules for triggering event notifications.
6. On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and to configure the transport settings:
7. On the General tab, follow these steps:
8. Verify that the new event notification is listed for the event group (Mobility > Notifications > Settings > Event Group Name).

DETAILED STEPS

Step 1 Choose Services > Mobility Services > Context Aware Notifications.

Step 2 Choose Notification Definitions from the left sidebar menu.

Step 3 Click the name of the group to which you want to add to the event. An event definition summary page appears for the selected event group.

Step 4 From the Select a command drop-down list, choose Add Event Definition, and click Go.

Step 5 On the Conditions tab, add one or more conditions. For each condition you add, specify the rules for triggering event notifications.

Tip For example, to keep track of heart monitors in a hospital, you can add rules to generate event notifications when a heart monitor is missing for one hour, a heart monitor moves off its assigned floor, or a heart monitor enters a specific coverage area within a floor.

To add a condition, follow these steps:

a) Click Add to add a condition that triggers this event.
b) In the Add/Edit Condition dialog box, follow these steps:

1. Choose a condition type from the Condition Type drop-down list.

If you chose Missing from the Condition Type drop-down list, enter the number of minutes after which a missing asset event is generated. For example, if you enter 10 in this text box, the mobility service engine generates a missing asset event if the mobility service engine has not found the asset for more than 10 minutes. Proceed to Step c.

If you chose In/Out from the Condition Type drop-down list, choose Inside of or Outside of, then select Select Area to select the area to monitor for assets going into it or out of it. In the Select dialog box, choose the area to monitor, then click Select. The area to monitor can be an entire campus, building within a campus, a floor in a building, or a coverage area (you can define a coverage area using the map editor). For example, to monitor part of a floor in a building, choose a campus from the Campus drop-down list, choose a building from the Building drop-down list, and choose the area to monitor from the Floor Area drop-down list. Then click Select. Proceed to Step c.

If you chose Distance from the Condition Type drop-down list, enter the distance in feet that triggers an event notification if the monitored asset moves beyond the specified distance from a designated marker, then click Select Marker. In the Select dialog box, choose the campus, building, floor, and marker from the corresponding drop-down list, and click Select. For example, if you add a marker to a floor plan and set the distance in the Trigger. If the text box is set to 60 feet, an event notification is generated if the monitored asset moves more than 60 feet away from the marker. Proceed to Step c.

You can create markers and coverage areas using the Map Editor. When you create marker names, make sure they are unique across the entire system.

If you chose Battery Level from the Condition Type drop-down list, select the check box next to the battery level (low, medium, normal) that triggers an event. Proceed to Step c.

If you chose Location Change from the Condition Type drop-down list, proceed to Step c.

If you chose Emergency from the Condition Type drop-down list, click the button next to the emergency (any, panic button, tampered, detached) that triggers an event. Proceed to Step c.

If you chose Chokepoint from the Condition Type drop-down list, proceed to Step c. There is only one trigger condition, and it is displayed by default. No configuration is required.

c) From the Apply To drop-down list, choose the type of asset (Any, Clients, Tags, Rogue APs, Rogue Clients, or Interferers) for which an event is generated if the trigger condition is met.

If you choose the any option from the Apply to drop-down list, the battery condition is applied to all tags, clients, and rogue access points and rogue clients.

Emergency and chokepoint events apply only to Cisco-compatible extension tags Version 1 (or later).

d) From the Match By drop-down list, choose the matching criteria (MAC Address, Asset Name, Asset Group, or Asset Category), the operator (Equals or Like) from the drop-down list, and enter the relevant text for the selected Match By element.

Some examples of asset matching criteria that you can specify:

- If you choose MAC Address from the Match By drop-down list, choose Equals from the Operator drop-down list, and enter a MAC address (for example, 12:12:12:12:12:12), the event condition applies to the element whose MAC address is 12:12:12:12:12:12 (exact match).
- If you choose MAC Address from the Match By drop-down list, choose Like from the Operator drop-down list, and enter 12:12, the event condition applies to elements whose MAC address starts with 12:12.

e) Click Add to add the condition you have just defined.

If you are defining a chokepoint, you must select the chokepoint after you add the condition.

To select a chokepoint, do the following:

1. Click Select Chokepoint. An entry page appears.
2. Choose Campus, Building, and Floor from the appropriate drop-down lists.
3. Choose a Chokepoint from the menu that appears.

You are returned to the Add/Edit Condition page, and the location path (Campus > Building > Floor) for the chokepoint auto-populates the text area next to the Select Checkpoint button.

Step 6 On the Destination and Transport tab, follow these steps to add one or more destinations to receive event notifications and to configure the transport settings:

a) To add a new destination, click Add. The Add/Edit Destination configuration page appears.
b) Click Add New.
c) Enter the IP address of the system that receives event notifications, and click OK.
d) The recipient system must have an event listener running to process notifications. By default, when you create an event definition, adds its IP address as the destination.
e) To select a destination to send event notifications to, highlight one or more IP addresses in the box on the right, and click Select to add the IP addresses to the box on the left.
f) Choose XML or Plain Text to specify the message format.
g) Choose one of the following transport types from the Transport Type drop-down list:

- SOAP—Specifies Simple Object Access Protocol, a simple XML protocol, as the transport type for sending event notifications. Use SOAP to send notifications over HTTP/HTTPS that are processed by web services on the destination.
- If you choose SOAP, specify whether to send notifications over HTTPS by selecting its corresponding check box. If you do not, HTTP is used. Also, enter the destination port number in the Port Number text box.
- Mail—Use this option to send notifications through e-mail.
- If you choose Mail, you need to choose the protocol for sending the e-mail from the Mail Type drop-down list. You also need to enter the following information: username and password (if Authentication is enabled), name of the sender, prefix to add to the subject line, e-mail address of recipient, and a port number if necessary.
- SNMP—Use Simple Network Management Protocol, a very common technology for network monitoring used to send notifications to SNMP-capable devices.
- If you choose SNMP, enter the SNMP community string in the SNMP Community text box and the port number to send notifications to in the Port Number text box.
- SysLog—Specifies the system log on the destination system as the recipient of event notifications.
- If you choose SysLog, enter the notification priority in the Priority text box, the name of the facility in the Facility text box, and the port number of the destination system in the Port Number text box.

h) To enable HTTPS, select the Enable check box next to it.

Port Number auto-populates.

i) Click Save.

Step 7 On the General tab, follow these steps:

a) Select the Enabled check box for Admin Status to enable event generation (disabled by default).
b) Set the event priority by choosing a number from the Priority drop-down list. Zero is the highest priority.
c) An event notification with high priority is serviced before event definitions with lower priority.
d) To select how often the event notifications are sent:

e) Select the All the Time check box to continuously report events. Proceed to Step g.
f) Unselect the All the Time check box to select the day and time of the week that you want event notifications sent. Days of the week and time fields appear for the selection. Proceed to Step d.
g) Select the check box next to each day you want the event notifications sent.
h) Select the time for starting the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply From heading.
i) Select the time for ending the event notification by selecting the appropriate hour, minute, and AM/PM options from the Apply Until heading.
j) Click Save.

Step 8 Verify that the new event notification is listed for the event group (Mobility > Notifications > Settings > Event Group Name).

Delete Event Definitions for MSE Notifications

To delete one or more event definitions from , follow these steps:

Step 1 Choose Services > Mobility Services > Context Aware Notifications.
Step 2 From the left sidebar menu, choose Settings.
Step 3 Click the name of the group from which you want to delete the event definitions.
Step 4 Select the event definition that you want to delete by selecting its corresponding check box.
Step 5 From the Select a command drop-down list, choose Delete Event Definition(s).
Step 6 Click Go.
Step 7 Click OK to confirm that you want to delete the selected event definitions.

Search for Specific MSE Wireless Clients (IPv6)

Note Only wireless clients have IPv6 addresses in this release.

To search for an MSE located clients using the Advanced search feature, follow these steps:

Step 1 Click Advanced Search.
Step 2 In the New Search dialog, choose Clients as the search category from the Search Category drop-down list.
Step 3 From the Media Type drop-down list, choose Wireless Clients.

The Wireless Type drop-down list appears only when you choose Wireless Clients as the media type.

Step 4 From the Wireless Type drop-down list, choose any of the following types: All, Lightweight or Autonomous Clients.
Step 5 From the Search By drop-down list, choose IP Address.

Searching a client by IP address can contain either full or partial IP address. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.

Step 6 From the Clients Detected By drop-down list, choose clients detected by as MSE.

This displays clients located by Context-Aware Service in the MSE by directly communicating with the controllers.

Step 7 From the Last detected within drop-down list, choose the time within which the client was detected.

Step 8 Enter the client IP address in the Client IP Address text box. You can enter wither a partial or full IPv6 address.

If you are searching for the client from on the MSE by IPv4 address, enter the IPv4 address in the Client IP address text box.

Step 9 From the Client States drop-down list, choose the client states. The possible values for wireless clients are All States, Idle, Authenticated, Associated, Probing, or Excused. The possible values for wired clients are All States, Authenticated, and Associated.

Step 10 From the Posture Status drop-down list, choose the posture status to know if the devices are clean or not. The possible values are All, unknown, Passed, and Failed.

Step 11 Select the CCX Compatible check box to search for clients that are compatible with Cisco Client Extensions. The possible values are All Versions, V1, V2, V3, V4, V5, and V6.

Step 12 Select the E2E Compatible check box to search for clients that are end-to-end compatible. The possible values are All Versions, V1, and V2.

Step 13 Select the NAC State check box to search for clients identified by a certain Network Admission Control (NAC) state. The possible values are Quarantine, Access, Invalid, and Not Applicable.

Step 14 Select the Include Disassociated check box to include clients that are no longer on the network but for which has historical records.

Step 15 From the Items per page drop-down list, choose the number of records to be displayed in the search results page.

Step 16 Select the Save Search check box to save the selected search option.

Step 17 Click Go.

The Clients and Users page appears with all the clients detected by the MSE.

View All MSE Clients

You can see the clients in probing state on 2.4 GHz on Cisco WLC but in probing state only on “a” radio (in the Monitor > Clients and Users > Client detected by MSE page). None of the clients shows up in probing state on “b/g” radio. This is because when clients are in the probing state, does not get details on the protocol and by default these are shown to be on 5 GHz channel. After they are associated, the INFO messages are received from the controller which contain details on the protocol and the channel. But when they are probing with Measurement messages, does not have this information and defaults it to 5 GHz.

To view all the clients detected by the MSE, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Clients and Users to view both wired and wireless clients information.

The Clients and Users table displays a few column by default. If you want to display the additional columns that are available, click 330159 image, and then click Columns. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

Step 2 Filter the current list to choose all the clients that are detected by the MSE by choosing Clients detected by MSE from the Show drop-down list.

All the clients detected by MSE including wired and wireless appear.

See Cisco Prime Infrastructure 3.2 Reference Guide, for the details of different parameters are available in the Clients Detected by MSE table.

Step 3 Select the radio button next to MAC Address in the Client and User page to view the associated client information.

Step 4 If you want to access the alarm details for a particular MSE, do the following:

a) Choose Monitor > Monitoring Tools > Alarms and Events, and click an MSE item under Failure Source column.

or

b) Choose Services > Mobility Services Engines> MSE Name > System > Status > Prime Infrastructure Alarms, and click a particular MSE item under Failure Source column.

See Cisco Prime Infrastructure 3.2 Reference Guide, for the descriptions of fields in the Alarm Detail page.

Configure Mobile Concierge Using MSE

The Mobile Concierge service allows the venue owners and service providers to monitor their WLAN. This solution delivers a unique in-store experience to customers who are using smart phones.

Mobile Concierge service uses wireless smart phones that have been configured with a set of policies for establishing network connectivity. Mobile Concierge service facilitates smartphones to discover network-based services available. Once you are connected to the stores Wi-Fi network, you can join the stores wireless guest network and can access variety of different services including electronic coupons, promotional offers, customer loyalty data, product suggestions, allow you to organize shopping lists, receive unique digital signature based on shopping preferences.

Related Topics

Configure Venues for Mobile Concierge (MSE), on page 830
Configure Providers for Mobile Concierge (MSE), on page 832
Configure Mobile Concierge Policies (MSE), on page 832

Configure Venues for Mobile Concierge (MSE)

To define a venue, follow these steps:

Step 1 Choose Services > Mobility Services > Mobile Concierge.

Step 2 Choose Mobile Concierge Services > Venues from the left sidebar menu.

The Venues page appears.

Step 3 From the Select a command drop-down list, choose Define New Venue and click Go.

The Venue Wizard page appears.

Step 4 Enter the venue name in the Venue Name text box and click Next.

Step 5 In the Floor/Outdoor Association group box, you can configure the following:

- From the Area Type drop-down list, choose the area type where you want to display the service advertisement. The possible values are Floor Area and Outdoor Area.

Note The Building, Floor Area, andCoverage Area drop-down lists are displayed only if you select Floor Area as the area type.

- From the Campus drop-down list, choose the campus name where you want to display the service advertisements.
- From the Building drop-down list, choose the building name where you want the advertisements to appear.
- From the Floor drop-down list, choose the floor type.
- From the Coverage Area drop-down list, choose the coverage area within the floor.
- From the Outdoor Area drop-down list, choose the outdoor area where you want to display the service advertisements. This field is displayed only if you select Outdoor Area as the Area Type.

Step 6 Click Next. The Audio group box appears.

Step 7 From the Audio group box, click Choose File to browse and select the audio file to play the audio notification.

Step 8 Click Next. The Icons group box appears.

Step 9 From the Icons group box, click Choose File to browse and select the icon that you want to display on the clients handset.

Step 10 Click Next. The Venue Apps group box appears.

Step 11 From the Venue Apps group box, choose the venue app on which you want to display the service advertisement from the Web App drop-down list.

Step 12 Click Next. The Additional Venue Information group box appears.

Step 13 From the Additional Information group box, you can provide any additional information that the venue would like to provide to the mobile application. You can configure the following:

- Enter the location detail in the Location Detail text box. This provides details such as store address, zip code, or street address of the venue.
- Enter the GPS latitude and longitude of the venue in the Latitude and Longitude text box. This helps the applications to identify the venue accurately.
- Enter any other additional information that the venue would like to provide to the mobile application in the Additional Information text box.

Step 14 Click Save. This information is applied to the MSE and the synchronization happens automatically.

Step 15 If you want to delete any venue, do the following in the Venue page:

a) Select the check box of the venue that you want to delete.
b) From the Select a command drop-down list, choose Delete Venue, and click Go.
c) Click OK to confirm the deletion.

Related Topics

Configure Mobile Concierge Using MSE, on page 830
Configure Providers for Mobile Concierge (MSE), on page 832
Configure Mobile Concierge Policies (MSE), on page 832

Configure Providers for Mobile Concierge (MSE)

Step 1 Choose Services > Mobility Services > Mobile Concierge.

Step 2 Choose Mobile Concierge Services > Providers from the left sidebar menu.

The Providers page appears.

Step 3 From the Select a command drop-down list, choose Define New Provider and click Go.

The Provider Wizard page appears.

Step 4 Enter the providers venue name in the Provider Name text box.

Step 5 Click Next. The Icons group box appears.

Step 6 From the Icons group box, click Choose File to browse and select the icon that you want to display on the clients handset.

Step 7 Click Next. The Local Services group box appears.

Step 8 From the Local Services group box, do the following:

- Click the inverted triangle icon location at the left side of the Local Service # name to expand the Local Service and configure the following:
  - Choose the service type from the Service Type drop-down list. The possible options are: Directory Info, Sign Up, Discount Coupon, Network Help, and Other.
  - Enter the display name in the Display Name text box.
  - Enter the description in the Description text box.
  - Choose the service URIs from the Service URIs drop-down list.
  - Enter the recommended application for the venue in the Recommended Apps text box.

Step 9 Click Save.

Step 10 If you want to delete a provider, do the following in the Providers page:

a) Select the check box of the venue that you want to delete.
b) From the Select a command drop-down list, choose Delete Provider, and click Go.
c) Click OK to confirm the deletion.

Related Topics

Configure Venues for Mobile Concierge (MSE), on page 830
Configure Mobile Concierge Using MSE, on page 830
Configure Mobile Concierge Policies (MSE), on page 832

Configure Mobile Concierge Policies (MSE)

To configure policies, follow these steps:

Step 1 Choose Services > Mobility Services > Mobile Concierge.

Step 2 Choose Mobile Concierge Services > Policies from the left sidebar menu.

The Policies page appears.

Step 3 From the Select a command drop-down list, choose Define New Policy and click Go.

The Policy Wizard page appears.

Step 4 Choose the venue on which you want the policy to be applied from the Venue drop-down list.

Step 5 Click Next. The Provider group box appears.

Step 6 Choose the provider from the Provider drop-down list.

Step 7 Click Next. The SSID group box appears.

Step 8 From the drop-down list, choose the SSIDs on which you want to broadcast the service advertisements and click OK. You can choose multiple SSIDs.

Step 9 Click Next. The Display Rule group box appears.

Step 10 From the Display Rule group box, you can do the following:

- Select the Display Rule radio button. You can select either Everywhere or Near selected APs radio button. By default, Display everywhere is selected.

If you select Display everywhere, then it searches for all the Mobile Concierge-supported controllers that provide these SSIDs and assigns these controllers to the MSE.

If you select Display near selected APs, then you can configure the following parameters:

- AP—Select those APs on which you want the advertisements to broadcast.
- Radio—Select the radio frequency on which you want the advertisements to be broadcasted. The service advertisement is displayed when the mobile device is near the radio band that you have selected. The possible values are 2.4 GHz or 5 GHz.
    - min RSSI—Enter a value for RSSI at which you want the service advertisemfm
    - ents to be displayed on the user interface.

Step 11 Click Finish.

Step 12 If you want to delete a policy, do the following in the Policy page:

a) Select the check box of the policy that you want to delete.
b) From the Select a command drop-down list, choose Delete Provider, and click Go.
c) Click OK to confirm the deletion.

Related Topics

Configure Mobile Concierge Using MSE, on page 830
Configure Venues for Mobile Concierge (MSE), on page 830
Configure Providers for Mobile Concierge (MSE), on page 832

Configure wIPS Using the MSE Wireless Security Configuration Wizard

The Wireless Security wizard page appears and allows you to perform the following wIPS related configurations:

- Allows rogue policy to detect and report ad hoc networks.
- Allows rogue rules to define rules to automatically classify rogue access points.

- Allows you to add new wIPS profiles.

Step 1 Choose Services > Mobility Services > Wireless Security.

By default, the Before You Begin tab opens. The Before You Begin wizard page displays information about how to use the Wireless Security wizard and includes the following information:

- Rogue Policy—The Rogue Policy page enables you to configure the rogue policy. It has three pre-configured rogue policy settings for rogue detection and containment.
- Rogue Rules—The Rogue Rules page allows you to automatically classify rogue access points based on criteria such as authentication type, matching configured SSIDs, client count, and RSSI values. Rogue rules can be created to classify rogues as Malicious and Friendly.
- wIPS Profile—The wIPS Profile page provides several pre-defined profiles from which to choose. These profiles allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. The profile can be further customized by selecting the awIPS signatures to be detected and contained.
- Devices—The Devices page allows you to apply rogue policy, rogue rules, and wIPS profiles to controllers.

Step 2 Click Next to configure the Rogue Policy to detect and report ad hoc networks. This page enables you to configure the rogue policy (for access points and clients) applied to the controller.

- You can either set the policy settings to Low, High, or Critical by moving the Configure the rogue policy settings sliding bar with the mouse or select the Custom check box to configure the policy settings.s
- In the General group box, configure the following fields:
  - Rogue Location Discovery Protocol—Determines whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network. Choose one of the following from the drop-down list:
  - Disable—Disables RLDP on all access points.
  - All APs—Enables RLDP on all access points.
  - Monitor Mode APs—Enables RLDP only on access points in monitor mode.
- Expiration Timeout for Rogue AP and Rogue Client Entries—Set the expiration timeout (in seconds) for rogue access point entries. The valid range is 240 to 3600 seconds.
- Validate rogue clients against AAA—Select the Validate rogue clients against AAA check box to enable the AAA validation of rogue clients.
- Detect and report Adhoc networks—Select the Detect and report Adhoc networks check box to enable detection and reporting of rogue clients participating in ad hoc networking.
- Rogue Detection Report Interval—In the Rogue Detection Report Interval text box, enter the time interval in seconds at which the APs should send the rogue detection report to the controller. A valid range is 10 seconds to 300 seconds, and the default value is 10 seconds. This feature is applicable to APs that are in monitor mode only.
- Rogue Detection Minimum RSSI—In the Rogue Detection Minimum RSSI text box, enter the minimum RSSI value that a rogue should have for the APs to detect and for the rogue entry to be created in the controller. A valid range is -70 dBM to -128 dBm. This feature is applicable to all the AP modes.
- Rogue Detection Transient Interval—In the Rogue Detection Transient Interval text box, enter the time interval at which a rogue has to be consistently scanned for by the AP after the first time the rogue is scanned. By entering the transient interval, you can control the time interval at which the AP should scan for rogues. The APs can filter the rogues based on their transient interval values. Valid range is between 120 seconds to 1800 seconds, and the default value is 0. This feature is applicable to APs that are in monitor mode only.
- In the Auto Contain group box, configure the following fields:
  - Rogue on Wire—Select the Rogue on Wire check box to auto contain those APs that are detected on the wired network.
  - Using our SSID—Select the Using our SSID check box.

- Valid client on Rogue AP—Select the Valid client on Rogue AP check box to auto contain the valid clients from connecting to the rogue APs.
- AdHoc Rogue—Select the AdHoc Rogue checkbox to auto contain adhoc rogue APs.

- Click Apply to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click Apply to Controllers.

Step 3 Click Next to configure the rogue rules. This page enables you to define rules to automatically classify rogue access points. applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time).

Step 4 Click Create New to create new rogue rules.The Add/Edit Rogue Rule window appears.

- In the General group box, configure the following fields:
  - Rule Name—Enter a name for the rule in the text box.
  - Rule Type—Choose Malicious or Friendly from the drop-down list.

Note Malicious Rogue—A detected access point that matches the user-defined Malicious rules or has been manually moved from the Friendly AP category. Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined Friendly rules.

- Match Type—Choose Match All Conditions or Match Any Condition from the drop-down list.
- In the Rogue Classification Rule group box, configure the following fields:
  - Open Authentication—Select the Open Authentication check box to enable Open Authentication.
  - Match Managed AP SSID—Select the Match Managed AP SSID check box to enable the matching of managed AP SSID rule condition.

    Note Managed SSID are the SSIDs configured for the WLAN and is known to the system.

  - Match User Configured SSID (Enter one per line)—Select the Match User Configured SSID check box to enable the matching of user configured SSID rule condition.

    Note User Configured SSID are the SSIDs that are manually added. Enter the User Configured SSIDs (one per line) in the Match User Configured SSID text box.

  - Minimum RSSI—Select the Minimum RSSI check box to enable the Minimum RSSI threshold limit.

    Note Enter the minimum RSSI threshold level (dB) in the text box. The detected access point is classified as malicious if it is detected above the indicated RSSI threshold.

  - Time Duration—Select the Time Duration check box to enable the Time Duration limit.

    Note Enter the time duration limit (in seconds) in the text box. The detected access point is classified as malicious if it is viewed for a longer period of time than the indicated time limit.

  - Minimum Number Rogue Clients—Select the Minimum Number Rogue Clients check box to enable the Minimum Number Rogue Clients limit.

    Note Enter the minimum number of rogue clients allowed. The detected access point is classified as malicious if the number of clients associated to the detected access point is greater than or equal to the indicated value.

- Click Ok to save the rule or Cancel to cancel the creation or changes made to the current rule. You are returned to the Rogue Rules page and the newly added rogue rule is listed.

- Click Apply to apply the current rule to controllers. In the Devices wizard page, select the applicable controllers and click Apply to Controllers.

Step 5 Click Next to configure the wIPS profiles. provides several pre-defined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile 'as is' or customize it to better meet your needs.

Step 6 For more information on configuring the wIPS profile, see the Configuring wIPS and Profiles section.

Step 7 After configuring wIPS profile, click Next to open the Devices page where you can select the controllers to apply the settings.

Configure Connected Mobile Experiences

Cisco Connected Mobile Experiences (CMX) is a smart Wi-Fi solution that uses the wireless infrastructure to detect and locate users mobile devices. With it, you can directly deliver content to smartphones and tablets that is personalized to user preferences. Cisco CMX is a software solution that integrates with other components, such as the Cisco Mobility Services Engine (MSE) for location identification and the Cisco Enterprise Mobility Services Platform (EMSP) for mobile app development, distribution, and management.

Important

- Prime Infrastructure 3.2 supports integration with CMX 10.3. It uses the below queries to query CMX:
  - /api/config/v1/version/image (to get CMX version)
  - /api/config/v1/campuses/import (to import map file into CMX)
- Prime Infrstructure 3.5 does not support CMX versions 10.3 and 10.4. So, when upgrading Prime Infrastructure to version 3.5, you also need to upgrade CMX to 10.5.
- The file storage limit for Import Map to CMX is ten map export files. If you try to import additional files, a message asking you to remove one of the existing files will be displayed.
- CMX should be configured in location mode and loaded with maps from Prime Infrastructure before viewing the CMX clients in Prime Infrastructure
- If Prime Infrastructure has both MSE and CMX added, the floor map can be synchronized only to either of them. So the corresponding clients in this floor can be tracked only by any one of them.
- Changes done to maps in Prime Infrastructure are not synchronised with CMX, as there is no periodic task to update the information. Maps have to be re-imported to CMX to retrieve the updated information.
- Prime Infrastructure does an API query on CMX when the map page is open and it refreshes based on the configured map refresh interval.

Related Topics

Manage CMX in , on page 837

Manage CMX in

To add, edit, and delete a CMX device and to import site maps from to CMX:

Step 1 To add a device, choose Services > Mobility Services > Connected Mobile Experiences.

Alternately, you can click the Manage CMX link in the Services > Mobility Services > Mobility Service Engine page.

Step 2 Click Add.

Step 3 Enter the following details:

- IP address
- Device Name
- CMX Username (GUI Credentials)
- CMX password (GUI Credentials)
- SSH User (optional)
- SSH Password (optional)
- Name of the Owner (optional)

Step 4 Click Save to add the device.

Step 5 To edit the device parameters, choose Services > Mobility Services > Connected Mobile Experiences.

Step 6 Click Edit.

Step 7 Edit any or all of the following parameters:

- CMX Username (GUI Credentials)
- CMX password (GUI Credentials)
- SSH User (optional)
- SSH Password (optional)
- Name of the Owner (not mandatory)

Step 8 Click Update to save the new parameters or Cancel to go back to the previous parameters.

Step 9 To delete any device, choose Services > Mobility Services > Connected Mobile Experiences.

Step 10 Click Delete.

Step 11 Select the devices you want to delete and click Delete > Ok.

Step 12 To import the site maps into CMX, choose Services > Mobility Services > Connected Mobile Experiences. select a CMX and click Import Map to CMX

Note If the CMX is in Presence mode, map will not be visible in CMX, but will be visible in Location mode.

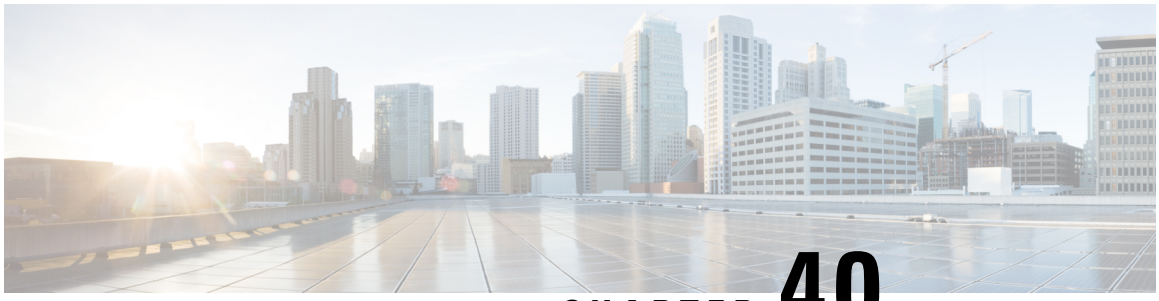
Step 13 Choose a map and click Import Map to CMX

Note You can also add map files to with the Export Map from PI button in the List CMX page.

Step 14 To create a new map file, click Export From PI in the Import Map to CMX window.

Step 15 In the Maps page, select the map and save it to .
On syncing, CMX can track the following parameters:

- Clients
- Interferers
- Rogue APs
- Rogue Clients
- RFID Tags



CHAPTER 40

Optimize WANs Using Cisco AppNav

What is Cisco AppNav

Cisco AppNav is a hardware and software solution that simplifies network integration of WAN optimization. It also overcomes the challenges related to provisioning, visibility, scalability, asymmetry, and high availability.

The Cisco AppNav solution reduces the dependency on the intercepting switch or router by distributing the traffic among Cisco WAAS devices for optimization by using a powerful class and policy mechanism. You can use ISR-WAAS to optimize traffic based on sites or applications. This includes device-level and template-based configurations.

An intelligent load-balancing mechanism in the Cisco IOS-XE software allows the diversion of TCP traffic to various products, including Cisco WAAS and OneFirewall, where Cisco WAAS is the initial target. Router management is performed through the network management application.

The Cisco AppNav solution, is made up of a distribution unit called the Cisco AppNav Controller (AC), WAAS Service Nodes (SNs). The Cisco AppNav Controller distributes the flow, and the service nodes process the flows. You can group up to four Cisco AppNav-XE (routers) together to form a Cisco AppNav Controller Group (ACG) to support asymmetric flows and high availability. However, must ensure that all of the routers in the ACG are on the same platform and have the same memory capacity.

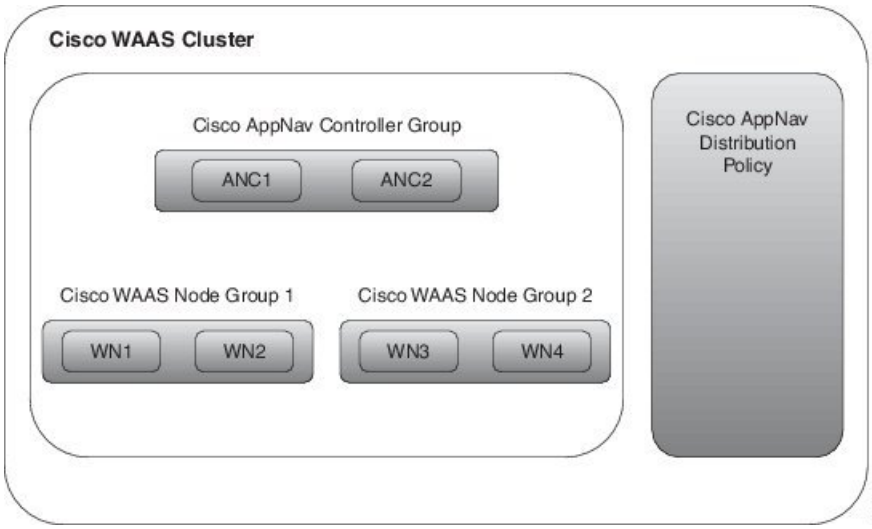
The Cisco AppNav solution's components perform the following functions:

- AppNav Controller—This is component that intelligently distributes traffic from a router to service nodes. The Cisco AppNav Controller is a part of Cisco IOS-XE Release 3.10 on the Cisco ISR-4400, Cisco CSR, and Cisco ASR 1K platforms.
- Cisco WAAS Service Nodes—These optimize traffic flows and are available in different form factors, for example, standalone appliances and virtualized ISR-WAAS running in a Cisco IOS-XE container.
- Cisco WAAS Central Manager—This is used to monitor and configure the ISR-WAAS.

- This chapter describes the configuration of the Cisco AppNav Controller functions on routers.

The following figure describes the components of Cisco AppNav

Figure 27: Components of Cisco AppNav



The advantages of using the Cisco AppNav components are:

- They can intelligently redirect new flows based on the load on each service node. This includes loads of individual application accelerators.
- If the flows do not require any optimization, service nodes can inform the Cisco AppNav Controller to directly pass the packets, thereby minimizing latency and resource utilization.
- There is minimal impact to traffic when adding or removing service nodes.
- The Cisco AppNav components support VRF. The VRF information is preserved when traffic returns from a service node. However, does not support VRF.
- For specific applications, such as Messaging Application Programming Interface (MAPI) and Virtual desktop infrastructure (VDI), the components ensure that a family of flow is redirected to the same service node.
- Asymmetric flows can be optimized in situations where traffic in one direction goes through one Cisco AppNav Controller and the return traffic goes through a different Cisco AppNav Controller. But both redirect the traffic to the same ISR-WAAS. This is achieved using the Cisco AppNav Controller Group.

The Cisco AppNav technology allows IP flows to be intercepted on routers and sent to a set of Cisco WAAS Service Node for processing. The initial application of Cisco AppNav which is supported in Cisco IOS-XE Release 3.10, is in Cisco WAAS.

Related Topics

- Prerequisites for Configuring Cisco AppNav
- Ways to Configure Cisco AppNav

Prerequisites for Configuring Cisco AppNav

The following are the prerequisites for configuring Cisco AppNav:

- The platform must be Cisco 4451-X ISR, Cisco ASR 1000 Series Aggregation Services Routers, or Cisco Cloud Services Router.
- The software version of above mentioned platforms must be Version 3.10 and later.
- A valid appxk9 license must be enabled on the routers.
- A Cisco WAAS Service Node must be available.

Ways to Configure Cisco AppNav

You must configure some parameters on the router before redirecting the traffic to the Cisco WAAS Service Node. If the Cisco AppNav configuration is generated as a part of installing the Cisco WAAS virtual appliance, it is transparent to the corresponding user. If it is configured using a template or through the Device Work Center, the user is more directly involved.

The Cisco AppNav can be configured in three ways:

- Configure Cisco AppNav on a Single Device , on page 842
- Configure Cisco AppNav on Multiple Devices Using Templates, on page 843
- How Cisco AppNav Configured When Created with ISR-WAAS Container, on page 845

The Cisco AppNav configuration involves the use of the following:

- Controllers—A list of routers that cooperate to redirect traffic. This is a list of IP addresses, exactly one of which must belong to the router on which Cisco AppNav is being configured.
- Cisco WAAS Service Node Groups (SNGs)—There must be one or more SNGs that are the target of redirected traffic and are defined as a set of IP addresses.
- Class Maps—A set of class maps that classify incoming and outgoing traffic. Class maps consist of a set of match conditions that together specify traffic of interest. They can match traffic based on three types of conditions:
  - An access control list (ACL) that selects traffic based on a source and destination IP address and port.
  - A protocol that is used to select traffic that uses the Microsoft port mapper service rather than depending on fixed port numbers. This includes MAPI and a host of other Microsoft protocols.
  - A remote device that matches the traffic that has traversed a particular Cisco WAAS Service Node on the remote end. The remote device is identified by a MAC address.
- Policy maps—A Cisco AppNav policy map is an ordered list of rules, each of which specify what is to be done with some type of traffic. A rule thus consists of a class map and an action. The action is to either redirect to a service node group or to pass through.
- Clusters—A Cisco WAAS cluster is the combination of a policy map, controller group, and a set of service node groups used by the policy map. A cluster can be enabled or disabled. allows several clusters to be defined but only one can be enabled at a time. An authentication key is used to secure communication between the controllers and the nodes in a cluster.
- Cisco WAAS interfaces—Traffic can be optimized only on interfaces where Cisco WAAS is enabled.

The WAN optimization template and the Device Work Center both have a default policy. The default policy consists of a number of class maps that match different types of traffic (HTTP, CIFS, TCP, and so on) that is optimized by Cisco ISR-WAAS. The template also includes a policy map containing a rule for each of those class maps. By default, all the matched traffic is redirected to a single service node group.

Configure Cisco AppNav on a Single Device

The Device Work Center allows an administrator to view and modify the configuration of individual devices. The Device Work Center can be used to configure Cisco AppNav when a user has a single or few devices. You can individually edit the configurations that are deployed using a template on the devices.

To configure the Cisco AppNav from the Device Work Center:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Select the device to be configured.

Step 3 On the Configuration tab in the bottom pane, and click WAN Optimization.

The Cisco AppNav configuration is divided into the following sections:

- AppNav controllers—The Controllers page shows the IP addresses of routers belonging to the same cluster as the router. You must assign one of the addresses to one of the currently selected router's interfaces. Each router's own IP address is shown in a drop-down list. The IP addresses of other routers in the same cluster are listed in a separate table.
- Cisco WAAS clusters—The Cisco WAAS Clusters page is the main Cisco AppNav page. It lists the Cisco WAAS clusters configured on the device and allows new ones to be created. To view the detailed configuration for a cluster, including the policy map, select the cluster, and click Edit.
  - In this page, cluster settings and policies can be edited. Expand individual rules by clicking the arrow in the third column. This enables the corresponding rule to be edited as well as the class maps and Cisco WAAS service node groups to be viewed, modified, and created. New rules can be added by clicking Add Policy. The order of the rules within a policy map is significant and the table allows the order to modified by dragging rows or selecting a contiguous list of rows and using the Up or Down arrows in the menu bar.
  - To create a new cluster, select Add WAAS Cluster on the Cisco WAAS Cluster Overview tab. This launches a wizard that prompts for controllers, Cisco WAAS Service Node, interception interfaces, and some general cluster parameters. After providing the necessary information, click Finish for the configuration to take effect. The wizard creates the cluster with a default policy that works for most small installations. All the TCP flows are redirected to a single node group, with the node group being monitored for overload conditions.

Note does not support VRFs; therefore, only one Cisco WAAS cluster can be enabled at a time.

- Interception—The Interception page lets the administrator select interfaces on which incoming and outgoing traffic should be redirected (subject to policies). All the WAN interfaces on the router should have Cisco WAAS enabled.
- Advanced Settings—The Advanced Settings folder contains pages for Cisco WAAS service node groups, class maps, and policy maps. Most of this information is also available in the Cisco WAAS Clusters page, but it is helpful to be able to view the definition of these objects directly.
  - Cisco WAAS Node Groups—The Cisco WAAS Node Groups page allows the existing Cisco WAAS node groups to be edited and new ones to be created.
  - Class maps and Policy maps—The Class Maps and Policy Maps page does the same.

Interface Roles and the Cisco AppNav Solution

The Cisco AppNav solution reroutes traffic only on the interfaces for which it has been explicitly enabled. Interface roles are logical objects that allow you to define policies to specific interfaces on multiple devices without having to manually define the names of each interface. When a template is deployed to a device, the interface role is resolved to a set of actual interfaces.

You can override the set of interfaces on which Cisco WAAS is enabled, during template deployment on a per-device basis. However, we recommend that you must define one or more interface roles and save them as part of the template to simplify the template deployment process. You can also define interface roles inConfiguration > Templates > Shared Policy Objects > Interface Role.

Configure Cisco AppNav on Multiple Devices Using Templates

templates contain reusable chunks of configuration that can be deployed to any number of devices. WAN Optimization templates define a policy and other information that can be applied across AppNav routers.

Templates are defined in design view and can later be deployed to one or more devices. As part of the deployment process, you can fill in the device-specific parameters and preview the final CLIs before the configuration is pushed to the device. When a template is modified, it is necessary to re- to devices for the changes to take effect.

This method of configuring Cisco AppNav is used when a user needs similar Cisco AppNav configurations on multiple devices. A single template, with similar configurations, and some minor customized values can be deployed to multiple devices at the same type using the deploy option.

To configure the Cisco AppNav using templates:

Step 1 Choose Configuration > Templates > Features & Technologies > WAN Optimization.

Step 2 Select an AppNav Cluster.

Step 3 Enter the configuration details on the following tabs:

- Controller IP addresses—A list of controllers can be configured here or during deployment. For example, if the template is used for multiple sites, such as branches, this field must be left empty. However, values can be provided during deployment.
- Service nodes—The Cisco WAAS service node groups are used by the policy map. By default, there is a single service node group called WNG-Default. If the template is used for multiple sites, leave the service node groups empty and add the actual IP addresses during deployment. Enter the following details:
  - Name of the Service Node
  - Description
  - IP address of the Cisco WAAS Service Node
- Interception—Interface roles for which Cisco WAAS should be enabled. During deployment, an actual list of interfaces is presented. You can make a selection of the actual interfaces belonging to the device, for each device. The purpose of the interface roles is to initialize the selection with a default. Therefore, the list of enabled interface roles can be left empty in the template design view. Here you can do the following:
  - Select or unselect the Enable WAAS check box.

- General—A valid cluster ID range is between 1 to 32. Select the check box to enable or disable a cluster. Enter the following details:
  - Cluster ID
  - Authentication Key
  - After this, select or unselect the Enable Distribution check box.
- Traffic redirection—This is a policy-related configuration, policy-map, class-maps and their relationships with ISR-WAAS groups. A simple setting results in a default policy that redirects all the TCP traffic to one node group. Select the Expert Mode to create custom policies and to redirect different types of TCP traffic to a different ISR-WAAS.

Step 4 Click Save as Template.

Step 5 Click Finish.

You can view the configured template by choosing Configuration > Templates > Features & Technologies > My Templates.

Deploy Cisco AppNav Templates

After a Cisco AppNav template is created, you can apply the template to begin traffic distribution.

To deploy a Cisco AppNav template:

Step 1 Choose Configuration > Templates > Features and Technologies.

Step 2 Select the My Templates folder in the left window pane.

Step 3 Select the Cisco WAAS template to be deployed and click Deploy.

You can choose a single device or multiple devices and change the required configurations.

Step 4 In the Value Assignment panel select each target device, one at a time and complete all the fields for that router:

- Basic Parameters—Includes an indication about whether the cluster is enabled.
- Controllers—The list of controller IP addresses. This must include an IP address assigned to the device itself.
- Node Groups—Enter IP addresses belonging to each of the ISR-WAAS groups used in the policy.
- Interception—A set of WAN interfaces on which Cisco WAAS interception is enabled.

Step 5 Click Apply.

Step 6 Click OK.

The Cisco AppNav is deployed on multiple devices.

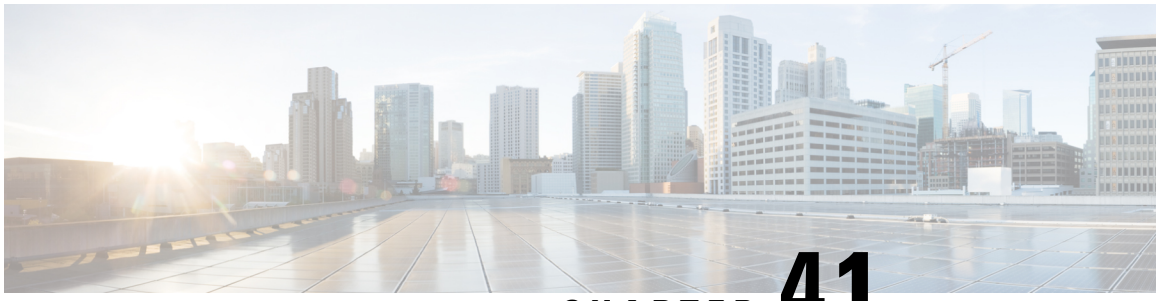
Note When a template is deployed to one or more devices, a job is created. Choose Administration > Dashboards > Job Dashboard, to verify the status of the template deployment and to view detailed status information about failures, success, or warnings, After you create a template, it can be edited multiple times depending on the requirements.

How Cisco AppNav Configured When Created with ISR-WAAS Container

Cisco AppNav can be configured only on Cisco 4451-X ISR devices or platform. Also, the software version required for ISR-WAAS activation must be Version 3.10 or later. In this method, the configuration occurs automatically as part of the installation of the Cisco WAAS virtual appliance node, ISR4451X-WAAS.

- A single service node group contains the new ISR-WAAS is created.
- Class maps are created for different types of traffic optimized by the Cisco WAAS service node.
- A default policy map, that redirects all TCP traffic to the Cisco WAAS service node, is generated.
- A Cisco WAAS cluster is created.
- Cisco WAAS is enabled on interfaces denoted by an interface role (specified at the time of container activation).

For more information on how to configure Cisco AppNav using this method, see the Create a Cisco WAAS Container .



CHAPTER 41

Optimize WANs Using Cisco WAAS Containers

Ways to Optimize WANs Using Cisco WAAS Containers

The Cisco Wide Area Application Services (Cisco WAAS) container is a powerful WAN optimization acceleration solution.

Note In this chapter, Cisco WAAS device refers to the router and Cisco WAAS container refers to the container.

Prerequisites for Installing Cisco WAAS Containers

Before you install a Cisco WAAS container, you must configure the following in :

- Integrate with Cisco WAAS Central Manager
- Import an OVA Image for Cisco WAAS Containers

Note Ensure that the name of the Cisco WAAS container does not exceed 22 characters.

Integrate with Cisco WAAS Central Manager

To manage thee Cisco-WAAS with the Cisco WAAS Central Manager, you must register with the Cisco WAAS Central Manager. Registration of Cisco WAAS with Cisco WAAS Central Manager can be done either from the Cisco WAAS CLI, or from the Cisco WAAS Central Manager GUI, or while activating the Cisco WAAS through . The WCM periodically polls the Cisco 4451-X Integrated Services Router (ISR) to retrieve the current status information and perform configuration synchronization.

A typical Cisco WAAS deployment consists of both and Cisco WAAS Central Manager applications. Cisco WAAS Central Manager IP is used during Cisco WAAS activation. After Cisco WAAS is activated, it registers with Cisco WAAS Central Manager. needs the IP address and the server name of WCM for the following reasons:

- To inform Cisco WAAS Central Manager of the new Cisco WAAS
- For cross-launching Cisco WAAS Central Manager GUI for monitoring purposes

Note Cisco WAAS Central Manager configuration is a one-time configuration. The Cisco WAAS Central Manager IP address is required for to authenticate itself to Cisco WAAS Central Manager, and is configured in using the Settings menu.

Note If Cisco WAAS Central Manager IP is not configured in , the newly activated Cisco WAAS will not be registered with Cisco WAAS Central Manager.

To configure the Cisco WAAS Central Manager IP address and server name in :

Step 1 Choose Administration > Settings > System Settings.

Step 2 Click Service Container Management.

Step 3 Enter the WCM IP address and the WCM server name.

Step 4 Click Save.

WCM can be deployed under the following condition:

works only with the active Cisco WAAS Central Manager that is configured in .

After a Cisco WAAS Central Manager failover, one of the following must take place for -Cisco WAAS Central Manager interworking to operate properly again:

- is reconfigured with the IP address of the new Cisco WAAS Central Manager.
- The failed Cisco WAAS Central Manager must become active.

Configure Single Sign-On for Launching Cisco WAAS Central Manager from

Configuring the Single Sign-On (SSO) feature provides a seamless method to launch Cisco WAAS Central Manager from using the existing Single Sign-On functionality.

To configure SSO:

Step 1 ChooseAdministration > User, Roles & AAA > SSO Servers.

Step 2 Choose Add SSO Server from the Select a command drop-down list.

Step 3 Select the type of SSL/TLS certificate being used by the SSO server. Select from either Self-Signed Certificate or Certificate Authority (CA) certificate type.

Step 4 If using Self-Signed Certificate type enter the IP address of the acting as the SSO server. If using CA certificate enter either the IP address or the FQDN of the server of the server that will be the SSO server.

Note The browser cookies that provide the Single Sign-On functionality are stored in the browser according to either the IP address or the FQDN given here. So, you must be consistent in entering either the IP address or the FQDN across all of the clients to the SSO server.

Step 5 Click GO.

Step 6 Click Save.

Step 7 Select AAA Mode Settings.

Step 8 Select the SSO radio button.

Step 9 Click Save.

Step 10 Configure the WCM IP address. For information on how to configure the WCM IP address, see the Integrate with Cisco WAAS Central Manager

Step 11 After you configure the IP address, log out of and log in to WCM and create a username.

Create Cisco WAAS Central Manager Users

Step 1 Log in to WCM.

Step 2 Choose Home > Admin > AAA > Users.

Step 3 Click Create.

Step 4 Enter a username that matches the username.

Step 5 Choose Role Management and click admin to assign a RBAC role to create a user account.

Step 6 Choose Domain Management and assign a role and domain.

Step 7 Click Submit.

Step 8 Choose Devices > Configure > AAA > NCS Single Sign-On.

Step 9 Select the Enable NCS Single Sign-On check box and enter the CAS/SSO server URL.

Step 10 Click Submit to create the certificate.

Step 11 Click Submit after the certificate is created.

Ways to Launch Cisco WAAS Central Manager from

You can cross-launch Cisco WAAS Central Manager in the following ways:

- Launch Cisco WAAS Central Manager from Single Device
- Launch Cisco WAAS Central Manager from Multiple Devices

Launch Cisco WAAS Central Manager from Single Device

To cross-launch the Cisco WAAS Central Manager from the Device Work Center:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Select the Cisco WAAS device.

The device details are displayed in the pane below.

Step 3 Click the Service Container tab.

Step 4 Select the corresponding Cisco WAAS container and click Launch WCM.

Launch Cisco WAAS Central Manager from Multiple Devices

To cross-launch from the Deployed Services:

Step 1 Choose Operate > Deployed Services.

Step 2 Select the corresponding Cisco WAAS container and click Launch WCM.

Note Note The Cisco WAAS Container Lifecycle enables a user to install, uninstall, activate, or deactivate the service container.

Import an OVA Image for Cisco WAAS Containers

To import an OVA image for an Cisco WAAS container:

Step 1 ChooseServices > Router Virtual Containers > WAAS-XE .

Step 2 Select an OVA image from one of the following locations:

- Device
- URL
- Protocol
- File

Step 3 Click Submit to import the image into .

Step 4 Click Refresh to view the imported image in the Services > Router Virtual Containers > WAAS-XE > Services Catalogue folder.

Configure Cisco WAAS Containers Automatically During Activation

A Cisco WAAS container can be configured in two different ways depending on whether you want to configure it on a single router (Install a Cisco WAAS Container on a Single Device) or multiple routers (Install a Cisco WAAS Container on Multiple Devices).

Installation of the Cisco WAAS container can be done in two ways. You can either install the container and activate it later, or you can install and activate the container at the same instance.

Note Ensure that the name of the Cisco WAAS container does not exceed 22 characters.

Create a Cisco WAAS Container

To install Cisco WAAS container:

Before you begin

- To install and activate a Cisco WAAS, make sure there is enough memory for each resource profile. You will need:
  - 4194304 KB memory and two CPUs for Cisco WAAS -750
  - 6291456 KB memory and four CPUs for Cisco WAAS -1300
  - 8388608 KB memory with six CPUs for Cisco WAAS -2500
- To install and activate a Cisco WAAS, you need 8 GB RAM in the router for the 750 resource profile.
- Once the Cisco WAAS is installed and activated, the Cisco AppNav is automatically configured.

Step 1 Choose Services > Router Virtual Containers > WAAS-XE > Services Catalogue to import an OVA image. For information on how to import an OVA image, see Import an OVA Image for Cisco WAAS Containers.

Step 2 After importing, click Refresh to view the imported image.

Step 3 Click Deploy.

Step 4 In the Network Wizard page, select the Cisco WAAS device on which you want to configure the container.

Step 5 Choose the Install option or Install and Activate option to select a Resource Profile from the drop-down list.

Step 6 Click OK to install the Cisco WAAS container.

Step 7 Select the Redirect Traffic to WAAS-XE with AppNav-XE check box to install and activate

Step 8 Click OK to install and activate the Cisco WAAS container.

Install a Cisco WAAS Container on a Single Device

To install an Cisco WAAS container on a single router:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 From the list that is displayed, choose the router on which you want to install the Cisco WAAS container.

Step 3 Click the Service Container tab.

Step 4 Click Add and enter the configuration details in each field.

Step 5 Click OK.

Install a Cisco WAAS Container on Multiple Devices

To install an Cisco WAAS container on multiple routers:

Step 1 Choose Services > Router Virtual Containers

Step 2 Select the Cisco WAAS folder that contains the imported OVA image.

Step 3 Click Deploy.

From the list that is displayed, select the routers on which you want to install the Cisco WAAS container.

After you deploy, you can either click Install or Install and Activate (Create a Cisco WAAS Container)

Step 4 If you choose Install and Activate, enter the following details in the Value Assignment area:

- Enter the Cisco WAAS IP Address/Mask
- Enter the Router IP/ Mask
- Enter a Service Container name
- Select a Resource Profile

Step 5 Click OK.

Ways to Uninstall and Deactivate Cisco WAAS Containers

You can deactivate a Cisco WAAS Container either from the Device Work Center or from the Deployed Services. From the Device Work Center, you can deactivate a single Cisco WAAS container, but from the Deployed Services, you can deactivate multiple Cisco WAAS containers.

Uninstall Cisco WAAS Container on a Single Device

To uninstall a single Cisco WAAS container from the Device Work Center:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 From the list that is displayed, select the router from which you want to uninstall the Cisco WAAS container by clicking it.

Step 3 Click the Service Container tab in the bottom pane.

Step 4 Click Uninstall.

Step 5 Click OK.

Uninstall Cisco WAAS Container on Multiple Devices

To uninstall multiple Cisco WAAS containers from the Deployed Services:

Step 1 Choose Services > Router Virtual Containers > WAAS-XE > Deployed Services.

Step 2 From the list that is displayed, select the routers from which you want to uninstall the Cisco WAAS containers by clicking them.

Step 3 Click Uninstall.

Step 4 Click OK.

Note When a Cisco WAAS virtual appliance is uninstalled through , the corresponding Cisco AppNav configuration is removed.

Ways to Deactivate Cisco WAAS Containers

You can deactivate a Cisco WAAS container in the following two ways:

- Deactivate a Single Cisco WAAS Container
- Deactivate Multiple Cisco WAAS Containers

Deactivate a Single Cisco WAAS Container

To deactivate a single Cisco WAAS container from the Device Work Center:

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 Select a Cisco WAAS device name from the device group list.

Step 3 Click the Service Container tab.

Step 4 Click Deactivate.

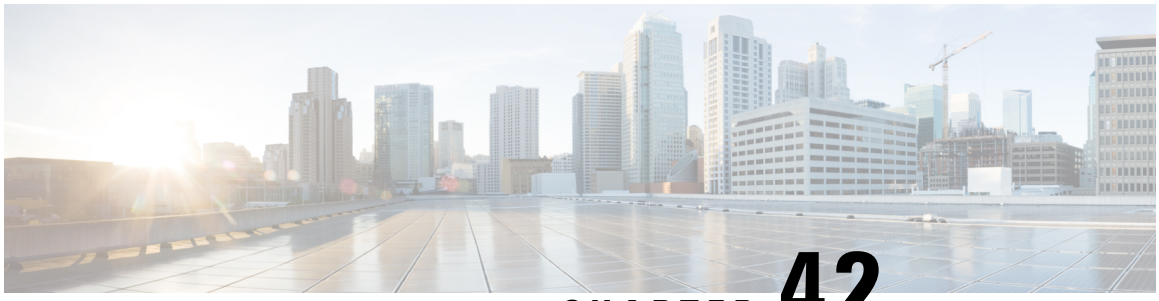
Deactivate Multiple Cisco WAAS Containers

To deactivate multiple Cisco WAAS containers from the Deployed Services:

Step 1 Choose Services > Router Virtual Containers > WAAS-XE > Deployed Services.

Step 2 Choose multiple Cisco WAAS device names from the list.

Step 3 Click Deactivate.



CHAPTER 42

Work With Wireless Mobility

What Is Mobility?

Mobility, or roaming, is an ability of a wireless client to maintain its association seamlessly from one access point to another securely and with as little latency as possible. To allow more flexible roaming and to minimize the need for tunnel encapsulation of traffic, provides a robust mobility architecture that distributes mobility functionality across the network devices.

The following are the key elements of the mobility architecture:

- Mobility Controller (MC)—The MC (for example, Cisco 5700 Series Wireless Controller) is responsible for one or more MAs or switch peer groups, handling roaming within its span of control, and transiting traffic between MAs and/or MCs when co-located with MTE.
- Mobility Agent (MA)—The MA (for example, Catalyst 3650 or Catalyst 3850 Switch) resides in the access switch or edge switch that the WAP is directly connected to, and terminates at the CAPWAP tunnel for communications with the WAP.
- Mobility Oracle (MO)—The MO is a top-level control entity responsible for connecting multiple MCs or mobility subdomains in deployments of the largest scale, to enable roaming across very large physical areas.
- Mobility Domain—A roaming domain: a mobile user may roam across all of the devices in this domain (the set of WAPs and all of the control entities associated with it). This typically includes MAs and MCs, and may include a MO (to join multiple subdomains).
- Mobility Sub-Domain—The set of WAPs and associated MAs and one MC, representing a portion of a larger mobility domain (where a MO serves to coordinate roaming between multiple sub-domains).
- Switch Peer Group (SPG)—A group of switches (acting as MAs). An SPG establishes a full mesh of mobility tunnels among the group members to support efficient roaming across the WAPs associated

with the switches in the group. An SPG is also intended to limit the scope of interactions between switches during handoffs. An SPG is configured by the Mobility Controller, and every switch in the switch peer group has the same view of the membership. The switches in an SPG might be interconnected by a set of direct tunnels. When a station roams from one switch to another within the same switch peer group, if the point of presence stays at the original or anchor switch, the traffic can be directly tunneled back to the anchor switch without involving the MTE. This direct tunneling mechanism is a data path optimization and is optional.

- Mobility Group—A mobility group is a set of MCs (and their associated MAs / switch peer groups)
- Mobility Tunnel Endpoint—The Mobility Tunnel Endpoint (MTE) provides data plane services for mobile devices through the use of tunneling. This minimizes the impact of roaming events on the network by keeping the user's point of presence on the network a constant. If the VLAN or subnet of the roamed client is available at the MTE, the MTE could become the point of presence; otherwise it merely functions as a tunnel switching entity that connects the roamed client to access switch or MTE that is the point of presence.

Related Topics

View Mobility Domains Using the Mobility Work Center, on page 856
Create a Mobility Domain from a Group of Controllers, on page 857

What is WLAN Hierarchical Mobility

Hierarchical Mobility is referred to as New Mobility in the wireless LAN controller configuration. 2.0 supports the new mobility functionality for Cisco 5508 and WiSM2 platforms that run Cisco WLC 7.6.

The key features of the New Mobility functionality in are:

- Mobility Work Center discovers Cisco 5508 and WiSM 2 platforms that run Cisco WLC 7.6 and provide necessary operations related to building hierarchical mobility architecture that involves two device types (Cisco 5508 and WiSM2) and Cisco 3650//3850 deployed as Mobility Agent.
- When deploying the hierarchical mobility architecture, the wireless features such as WLAN, VLAN, security, guest anchor can be configured on Cisco 5508 and WiSM2 using the LifeCycle view.
- Deploying the flat mobility architecture on Cisco 5508 and WiSM2 would be supported only in classic view and entire wireless configuration would be left as it is in classic and LifeCycle view.
- As in 2.0, the IOS based devices 3850 and 5760 continue to be configured using CLI templates for some of the wireless features such as creating VLAN interfaces.

For more information about the new mobility functionality, see the Hierarchical Mobility (New Mobility) section in the Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.3.112.0.

View Mobility Domains Using the Mobility Work Center

The Mobility Work Center is available by choosing Services > Mobility Services > Mobility Domains.

The following information is displayed:

- Device Name—Name of the MC.

- Management IP—Management IP address of the MC.
- Wireless Interface IP—IP address on the MC which is used for mobility protocol.
- Mobility Group—Name of the mobility group the MC belongs to.
- Mobility Role—Shows administrative and operational mobility mode. If Admin and Operational values are different, the device needs reboot for the administrative mode to be effective. It shows MO in addition to mobility mode if Mobility Oracle is enabled on it.

In this page, you can perform the following tasks:

- Create Mobility Domain.
- Create Switch Peer Group—To create switch peer groups in MC.
- Change Mobility Role—To change the controllers from MA to MC.
- Delete Domain—Deletes only the domain; it does not delete the controllers from .
- Delete Members—To remove selected MCs from a selected domain.
- Set as Mobility Oracle—To enable MO on a selected MC, if the MC must act as the MO for the entire domain. There can be only one MO per domain. Only Cisco 5760 series controllers support the MO feature.
- Add members to switch peer group—To add members to switch peer group.
- Delete members from switch peer group—To delete members from switch peer group.

Note By default, the Mobility Work Center page displays all of the mobility domains configured in the managed network. To see a list of mobility devices, choose All Mobility Devices from the left sidebar.

Related Topics

What Is Mobility?, on page 855
Create a Mobility Domain from a Group of Controllers, on page 857

Create a Mobility Domain from a Group of Controllers

A mobility domain is a collection of controllers that have all been configured with each other's IP addresses, allowing clients to roam between the controllers in the mobility domain.

The Mobility Work Center displays all mobility domains configured in the managed network using .

When a node is selected from the left sidebar, the right pane shows more details. When a domain node is selected from the left sidebar, the right pane displays the MCs in the domain.

To create a mobility domain:

Step 1 Choose Services > Mobility Services > Mobility Domains.

Step 2 Click on the left sidebar menu.

Step 3 Enter a name for the mobility domain for the set of MCs that you want to group together.

If a selected MC exists in another domain, it is removed from that domain and added to the new domain.

Step 4 Select mobility domain member devices.

A device can belong to one domain or SPG only.

Step 5 Click Apply.

Create a Mobility Switch Peer Group from a Group of Switches

An MC can have switch peer groups (SPGs), and a switch peer group can have MAs. The MAs in a managed network are listed on the Switch Peer Group page. If you create a switch peer group when you already have one, MAs are moved from the old switch peer group to the new one, and the MC wireless interface IP address is set on all of the MAs.

To create a switch peer group, follow these steps:

Step 1 Choose Services > Mobility Services > Mobility Domains.

Step 2 Choose an MC from the left sidebar.

Step 3 Click Create Switch Peer Group.

Step 4 Enter a name for the switch peer group that will contain the set of MAs that you want to group together on the selected MC.

If a selected MA exists in another switch peer group, it is removed from that group and added to the new group. You can create multiple switch peer groups on an MC.

Step 5 Select mobility agents.

A device can belong to one domain or SPG only.

Step 6 Click Apply.

The SPG that you created appears in the left sidebar. You can navigate to it to see the mobility agents on the selected switch peer group.

Change a Device's Mobility Role

By default, Cisco 3850 controllers act as MAs. These controllers can be converted to MCs if MCs are needed in the network.

To change a mobility role:

Step 1 Choose Services > Mobility Services > Mobility Domains.

Step 2 Choose All Mobility Devices.

Step 3 Select a device and the role that you want to change to:

- Change Role To Mobility Controller—Enables the mobility controller feature on the selected controller.
- Change Role To Mobility Agent—Enables the Mobility Agent feature on the selected controller. When you do this, the MC feature is disabled.
- Converting MAs to MCs (and vice versa) is limited to 3850 devices. For a changed role to take effect, you must reboot the device.
- Assign Mobility Group—Allows you to enter new mobility group name for the selected device.

Step 4 Click Apply.

What are Mobility Anchors

Mobility anchors are a subset of a mobility group specified as the anchor controllers for a WLAN. This feature can be used to restrict a WLAN to a single subnet, regardless of the entry point of a client into the network. In this way, users can access a public or guest WLAN throughout an enterprise but still be restricted to a specific subnet. Guest WLAN can also be used to provide geographic load balancing because WLANs can represent a particular section of a building (such as a lobby, a restaurant, and so on).

When a client first associates to a controller of a mobility group that has been preconfigured as a mobility anchor for a WLAN, the client associates to the controller locally, and a local session is created for the client. Clients can be anchored only to preconfigured anchor controllers of the WLAN. For a given WLAN, you should configure the same set of anchor controllers on all controllers in the mobility group.

When a client first associates to a controller of a mobility group that has not been configured as a mobility anchor for a WLAN, the client associates to the controller locally, a local session is created for the client, and the controller is announced to the other controllers in the same mobility group. If the announcement is not answered, the controller contacts one of the anchor controllers configured for the WLAN and creates a foreign session for the client on the local switch. Packets from the client are encapsulated through a mobility tunnel using EtherIP and sent to the anchor controller, where they are decapsulated and delivered to the wired network. Packets to the client are received by the anchor controller and forwarded to the foreign controller through a mobility tunnel using EtherIP. The foreign controller decapsulates the packets and forwards them to the client.

Configure a Mobility Guest Anchor Controller for a WLAN

The guest anchor controller is a controller dedicated to guest traffic, and is located in an unsecured network area, often called the demilitarized zone (DMZ). Other internal WLAN controllers from where the traffic originates are located in the enterprise LAN.

Note The Cisco 5760 controller can be a guest anchor whereas the Catalyst 3850 switch cannot be a guest anchor but it can be a foreign controller.

You can configure a guest controller as a mobility anchor for a WLAN for load balancing.

Before You Begin

- Ensure that wireless devices are set up in . For more information about setting up wireless devices, see Configuring Wireless Features.

- Ensure that the wireless devices that you want to configure as mobility anchors for a WLAN are in the same mobility domain.

To configure a guest anchor controller for a WLAN:

SUMMARY STEPS

1. Choose Inventory > Device Management > Network Devices.
2. In the Device Group area, expand Device Type, then expand Wireless Controller.
3. Select the controller that you want to designate as a guest mobility anchor. The details of the device appear in the lower part of the page.
4. Click the Configuration tab.
5. From the left sidebar menu, choose WLANs > WLAN Configuration. The WLAN Configuration page appears.
6. Select the URL of the desired WLAN ID. A tabbed page appears.
7. Click the Advanced tab, and then click the Mobility Anchors link at the bottom of the page. The Mobility Anchors page appears.
8. Select the IP address check box of the controller to be designated a mobility anchor, and click Save.

DETAILED STEPS

Step 1 Choose Inventory > Device Management > Network Devices.

Step 2 In the Device Group area, expand Device Type, then expand Wireless Controller.

Step 3 Select the controller that you want to designate as a guest mobility anchor. The details of the device appear in the lower part of the page.

Step 4 Click the Configuration tab.

Step 5 From the left sidebar menu, choose WLANs > WLAN Configuration. The WLAN Configuration page appears.

Note If you are in the Classic view, choose Configure > Controllers > Ctrl IP addr > WLANs > WLAN Configuration to access the WLAN Configuration page.

Step 6 Select the URL of the desired WLAN ID. A tabbed page appears.

Step 7 Click the Advanced tab, and then click the Mobility Anchors link at the bottom of the page. The Mobility Anchors page appears.

Note You can also access the Mobility Anchors page from the WLAN Configuration page. Select the check box of the desired WLAN ID. From the Select a command drop-down list, choose Mobility Anchors, and then click Go. The Mobility Anchors page appears.

Step 8 Select the IP address check box of the controller to be designated a mobility anchor, and click Save.

What is a Spectrum Expert

A Spectrum Expert client acts as a remote interference sensor and sends dynamic interference data to . This feature allows to collect, monitor, and archive detailed interferer data from Spectrum Experts in the network.

To configure spectrum experts, choose Services > Mobility Services > Spectrum Experts. This page provides a list of all Spectrum Experts including:

- Hostname—The hostname or IP address of the Spectrum Expert laptop.
- MAC Address—The MAC address of the spectrum sensor card in the laptop.
- Reachability Status—Specifies whether the Spectrum Expert is successfully running and sending information to . The status appears as reachable or unreachable.

See Mobility Services section in Cisco Prime Infrastructure Reference Guide for the Descriptions of fields in the Spectrum Expert page.

Configure a Mobility Spectrum Expert to Collect Interferer Data

To add a Spectrum Expert, follow these steps:

SUMMARY STEPS

1. Choose Services > Mobility Services > Spectrum Experts.
2. From the Select a command drop-down list, choose Add Spectrum Expert. This link only appears when no spectrum experts are added. You can also access the Add Spectrum Expert page by choosing Add Spectrum Expert from the Select a command drop-down list.
3. Enter the hostname or IP address of the Spectrum Expert. If you use hostname, your spectrum expert must be registered with DNS to be added to Prime Infrastructure.

DETAILED STEPS

Step 1 Choose Services > Mobility Services > Spectrum Experts.

Step 2 From the Select a command drop-down list, choose Add Spectrum Expert. This link only appears when no spectrum experts are added. You can also access the Add Spectrum Expert page by choosing Add Spectrum Expert from the Select a command drop-down list.

Step 3 Enter the hostname or IP address of the Spectrum Expert. If you use hostname, your spectrum expert must be registered with DNS to be added to Prime Infrastructure.

To be correctly added as a spectrum expert, the spectrum expert client must be running and configured to communicate to Prime Infrastructure.

See Mobility Services section in Cisco Prime Infrastructure Reference Guide for more information.

Use Cisco Adaptive wIPS Profiles for Threat Protection in Mobility Networks

provides several predefined profiles from which to choose. These profiles (based on customer types, building types, industry types, and so on) allow you to quickly activate the additional wireless threat protection available through Cisco Adaptive wIPS. You can use a profile ‘as is’ or customize it to better meet your needs.

Predefined profiles include:

- Education
- EnterpriseBest
- EnterpriseRogue
- Financial
- HealthCare
- HotSpotOpen
- Hotspot8021x
- Military
- Retail
- Tradeshow
- Warehouse

The wIPS Profiles > Profile List page allows you to view, edit, apply, or delete current wIPS profiles and to add new profiles. The Profile List provides the following information for each profile:

- Profile Name—Indicates the user-defined name for the current profile. Click the profile name to view or edit profile details.

Hover your mouse cursor over the profile name to view the Profile ID and version.

- MSE(s) Applied To—Indicates the number of mobility services engines (MSEs) to which this profile is applied. Click the MSE number to view profile assignment details.
- Controller(s) Applied To—Indicates the number of controllers to which this profile is applied. Click the controller number to view profile assignment details.

To create a wIPS profile, follow these steps:

SUMMARY STEPS

1. Choose Services > Mobility Services > wIPS Profiles.
2. From the Select a command drop-down list, choose Add Profile, then click Go.
3. Enter a profile name in the Profile Name text box of the Profile Parameters page.
4. Select the applicable predefined profile, or choose Default from the drop-down list.
5. Choose Save > Next.
6. To edit and delete current groups or add a new group:
7. To determine which policies are included in the current profile, choose Profile Configuration. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. Using this page, you can:
8. When the profile configuration is complete, select Next to proceed to the MSE/Controller(s) page.
9. In the Apply Profile page, select the mobility services engine and controller(s) to which you want to apply the current profile, then click Apply to apply the current profile to the selected mobility services engine/controller(s).

DETAILED STEPS

Step 1 Choose Services > Mobility Services > wIPS Profiles.

Step 2 From the Select a command drop-down list, choose Add Profile, then click Go.

Step 3 Enter a profile name in the Profile Name text box of the Profile Parameters page.

Step 4 Select the applicable predefined profile, or choose Default from the drop-down list.

Step 5 Choose Save > Next.

When you select Save, the profile is saved to the database with no changes and no mobility services engine or controller assignments. The profile appears in the profile list.

Step 6 To edit and delete current groups or add a new group:

a) From the Select a command drop-down list on the SSID Group List page, choose Add Group or Add Groups from Global List, then click Go.

b) Enter the group name and one or more SSID groups, then click Save.

Step 7 To determine which policies are included in the current profile, choose Profile Configuration. The check boxes in the policy tree (located in the left Select Policy pane) indicate which policies are enabled or disabled in the current profile. Using this page, you can:

- Enable or disable an entire branch or an individual policy by selecting or unselecting the check box for the applicable branch or policy.

By default, all policies are selected.

- Click an individual policy to display the policy description. Use the Policy Rules page add, edit, delete, and reorder the current policy rule settings.

Note There must be at least one policy rule in place. You cannot delete a policy rule if it is the only one in the list.

Note If the profile is already applied to a controller, it cannot be deleted.

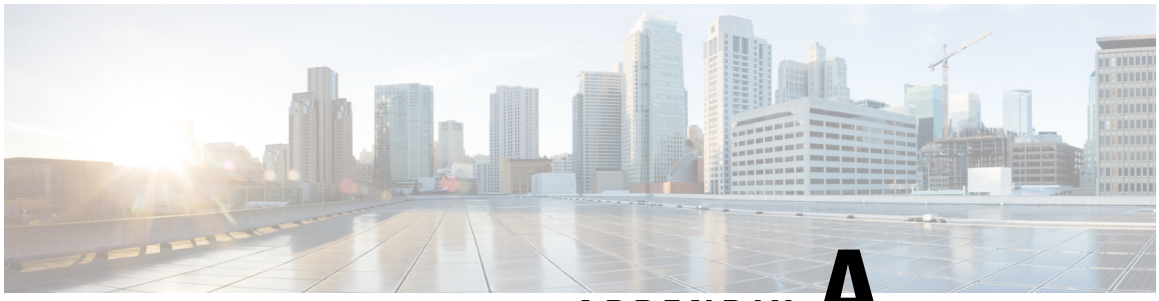
- Configure the following settings:
  - Threshold (not applicable to all policies)—Indicates the threshold or upper limit associated with the selected policy. Because every policy must contain at least one threshold, default thresholds are defined for each based on standard wireless network issues. Threshold options vary based on the selected policy.
  - When the threshold is reached for a policy, an alarm is triggered. Alarms from Cisco Adaptive wIPS DoS and security penetration attacks are classified as security alarms. A summary of these attacks is located in the Security Summary page; choose Monitor > Security to access this page. The wIPS attacks are located in the Threats and Attacks section.
  - Severity—Indicates the level of severity of the selected policy. Parameters include critical, major, info, and warning. The value of this field might vary depending on the wireless network.
  - Notification—Indicates the type of notification associated with the threshold.
  - ACL/SSID Group—Indicates the ACL or SSID Group(s) to which this threshold is be applied.

Note Only selected groups trigger the policy.

Step 8 When the profile configuration is complete, select Next to proceed to the MSE/Controller(s) page.

Step 9 In the Apply Profile page, select the mobility services engine and controller(s) to which you want to apply the current profile, then click Apply to apply the current profile to the selected mobility services engine/controller(s).

You can also apply a profile directly from the profile list. From the Profile List page, select the profile that you want to apply and click Apply Profile from the Select a command drop-down list. Then click Go to access the Apply Profile page.



APPENDIX A

User Interface Reference

User Interface Reference

is a web-based application.

If any of your installed Cisco Prime products are not yet enabled through licensing, the menu items or options for those features are not displayed in the web interface.

- About the User Interface
- Common UI Tasks
- Search Methods

About the User Interface

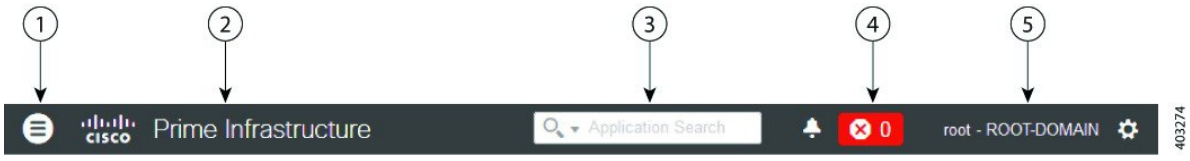
is a web-based application.

If any of your installed Cisco Prime products are not yet enabled through licensing, the menu items or options for those features are not displayed in the web interface.

When you first log in to , an overlay window shows you the major components of the graphical interface. To view this overlay window again, click your login name at the top-right of the screen, then choose Help > Getting Started.

The toolbar shown in Figure 58-1 is at the top of every page

Figure 28: Toolbar



1	Click to open the menu.
2	Click to go to the product page on cisco.com.

3	Type to search for data within . You can enter any text string such as a partial or complete IP address, a user name, an application name, or configuration archives. The search results display information such as Access Points, Alarms, Change Audit, Configuration Archives, Devices, etc. You can export the search results in CSV and PDF formats by clicking the export icon in the right corner.
4	Displays the number of alarms, and the color corresponds to the highest severity level alarm in your network. Click to display the alarm summary window, displaying all alarms and the number of critical, major, and minor alarms.
5	Displays login name and the virtual domain to which you are assigned. Click to change your user preferences, change your password, log out, access help, and submit product feedback.

Related Topics

Search Methods, on page 877

Dock Window

If you typically visit a small subsection of pages in , the Dock window provides a quick way to navigate quickly to those pages. From any page in , you can click the Dock icon (in the upper right corner) to quickly view:

- Links to videos relevant to the current page
- Links to pages you recently visited (up to a maximum of 15)
- Links to pages you marked as favorites (up to a maximum of 15)
- Pinned items

The Dock window stays open until you close it.

Related Topics

Pin Devices to a Dock Window, on page 866

Pin Devices to a Dock Window

If there are specific devices that you want to watch closely, you can pin the devices to the Dock window. You can have a maximum of 15 pinned items.

Step 1 From the Device 360° view, click the Add to Doc icon.

The device appears under the Pinned Items section of the Dock window.

Step 2 Click on the device link in the Dock window from anywhere in , and the Device 360° view appears with updated information.

Step 3 To remove an item from the Dock window, click the Trash icon next to the item. It is removed from Pinned Items.

Filters

You can use the Filter feature to display specific information about the interface. The Filter icon is provided wherever the data is displayed in a tabular format. The following types of filters are available:

- Quick Filter—See Quick Filters.
- Advanced Filter—See Advanced Filters.

- Dashboard Filter—See Dashboard Filters.

Quick Filters

This filter allows you to narrow down the data inside a table by applying a filter to a specific table column or columns. To apply different operators, use the Advanced Filter option (see Advanced Filters).

To launch the quick filter, choose Quick Filter from the Filter drop-down list.

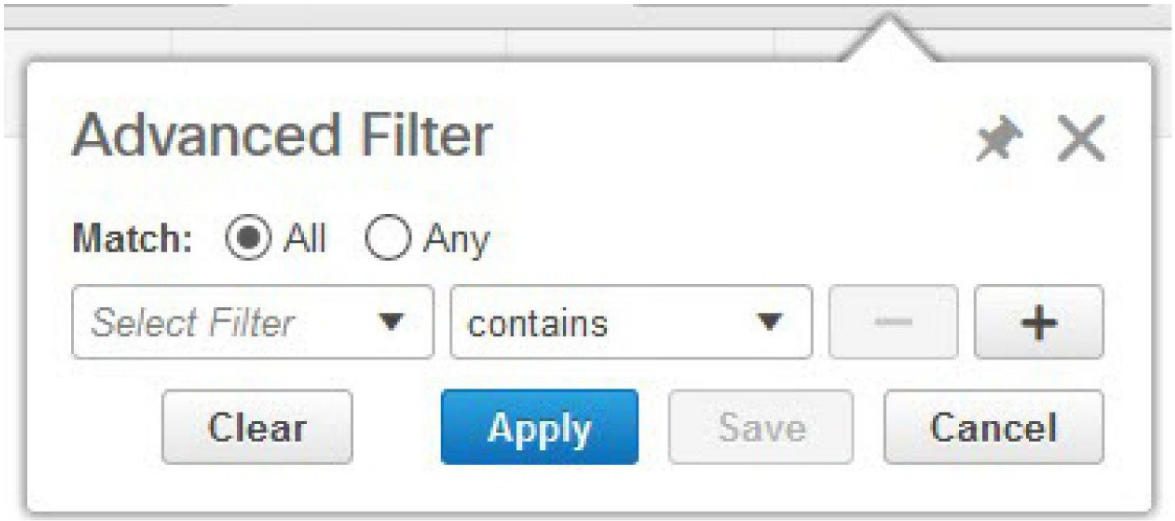
To clear the Quick Filter, click Filter.

Advanced Filters

This filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. For example, you can choose the filter pattern by table column names and the operator from the drop-down list. In addition, you must enter filter criteria based on the data available in the database.

To launch advanced filtering, choose Advanced Filters from the Filter drop-down list.

Figure 29: Advanced Filter



To save the filter criteria used in the Advanced filter, follow these steps:

Step 1 Enter the advanced filter criteria, then click Go. The data is filtered based on the filter criteria.

Step 2 After the data is filtered, click the Save icon.

Step 3 In the Save Preset Filter dialog box, enter a name for the preset filter and click Save.

Dashboard Filters

The Filters toolbar allows you to narrow down the data that is displayed in all of the dashlets in a dashboard. Use this toolbar to filter the dashlets data by:

- Time frame—Select one of the preset options or create a custom time frame.
- Client —Select or enter the client atttribute.

Note Client username field supports special characters except " (double quotes).

You can also use special characters except " (double quote).

- Applications—Select a service, up to 10 individual applications, or all applications.
- Network Aware—Select wired, wireless, or all networks.
- Site—Select a site, unassigned sites, or all sites.

Figure 30: Dashboard Filters Toolbar

To filter the data for all dashlets in a dashboard, follow these steps:

Step 1 Open a dashboard (for example, choose Dashboard Overview > Overview > General).

Step 2 Change the settings in any of the Filters toolbar options, then click Go.

Data Entry Features

In addition to the check boxes, drop-down lists and data entry fields common in most user interfaces, uses some specialized data-entry features. These features are designed to keep your view of the network as uncluttered as possible, while still making it possible for you to add, update, and save your settings when needed. These specialized data-entry features include:

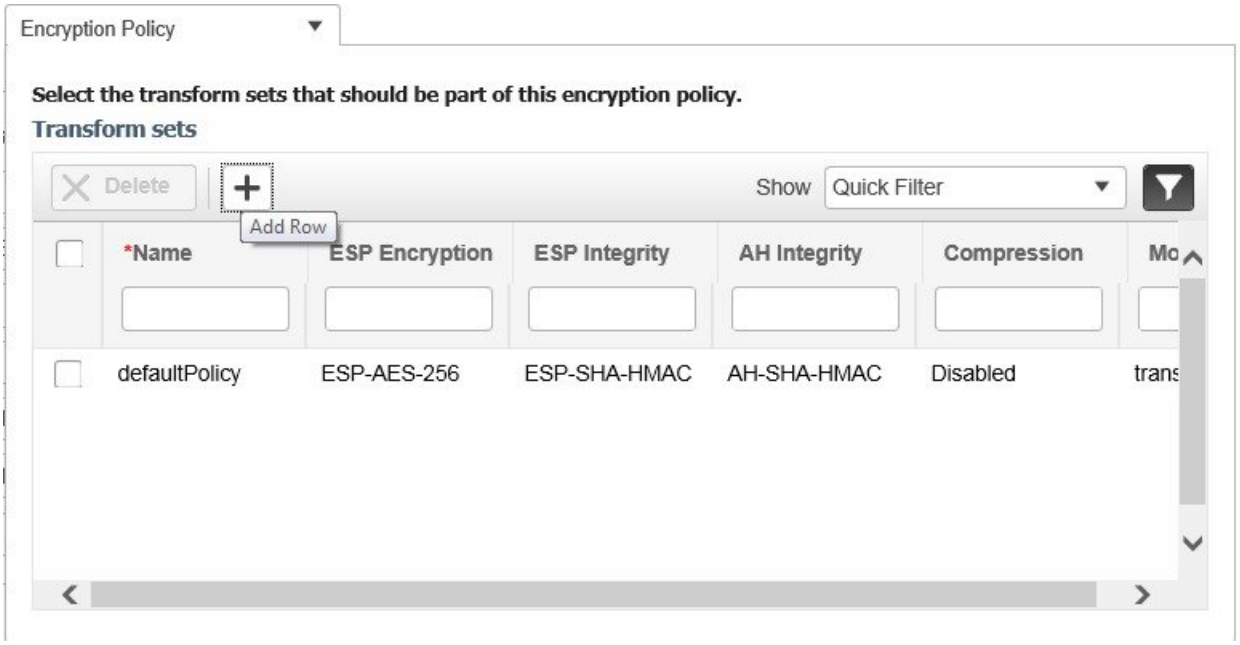
- Edit Tables
- Data Popups

Edit Tables

uses tables to display many kind of data, including lists of sites, devices, and events. The data is arranged in rows and columns, much like a spreadsheet.

An edit table differs from other tables in that you can add, edit, or delete the data it contains. Some edit tables also give you access to filters (see Filters). Edit tables are often displayed in data popups that are triggered by check boxes.

Figure 31: Edit Table



To use edit tables:

- To add a new row in the edit table:

Click the (+) icon, complete the fields in the new row, and click Save.

- To delete one or more existing rows in an edit table:

Select the row header check box (at the extreme left of each row), then click Delete.

- To update an entry in any field in any edit table row:

Click the row header or on the field itself, edit the contents, then click Save.

Data Pop-ups

A data popup is a window associated with a check box, anchored field, or other data-entry feature. It is displayed automatically when you select a feature, so that you can view or update the data associated with that feature. In addition to containing check boxes, drop-down lists, and data-entry fields, data popups can also contain edit tables.

To use a data popup:

1. Select the feature that triggers the data popup, such as an anchored field or a check box.
2. With the associated popup displayed, view or update the fields as needed.
3. When you are finished, click anywhere outside the data popup. If you entered new information or changed existing information, your changes are saved automatically.

Interactive Graphs

provides interactive line, area, pie, and stacked bar graphs of both time-based and non time-based data. Interactive graph features include the following:

- Support for automatic refresh—The graphs refresh automatically within a predetermined time interval.
- Two graph views:
  - Graph (Chart) view (this is the default)
  - Table (Grid) view
- Graph enlargement

Related Topics

- How to Use Interactive Graphs
- Time-based Graphs

How to Use Interactive Graphs

The following table summarizes how to use interactive graphs.

Table 87: Using Interactive Graphs

To do this:	Do this:
Get help with the graph buttons	Hover your mouse cursor over the button. displays a popup tooltip describing the button.
View the data as a graph or chart.	Click View in Chart.
View the data in grid or table form	Click View in Grid.
Enlarge the graph	Click the button located at the bottom right side of the graph. displays an enlarged version of the graph in a separate page. The View in Chart and View in Grid toggle buttons are available in the new page, so you can change the type of enlarged graph displayed.

Related Topics

- Interactive Graphs
- Time-based Graphs

Time-based Graphs

Some graphs display time-based data. For these time-based graphs, provides a link bar at the top of the graph. The link bar contains a set of links representing standard time-frames (such as the last six hours, one day, and so on) appropriate for the type of data in the chart. When you select one of these time-frame links, the data for that time frame is retrieved and the graph is refreshed to show only the data for that time-frame.

The time-frame links displayed in time-based graphs include the following:

- 6h—Denotes the last six hours of data from the current time. The data is gathered from the current database table.
- 1d—Denotes the last day (24 hours) of data from the current time. The data is gathered from the current database table.
- 1w—Denotes the last week (seven days) of data from the current time. The data is gathered from the hourly aggregated table.

- 2w—Denotes the last two weeks of data from the current time. The data is gathered from the hourly aggregated table.
- 4w—Denotes the last four weeks of data from the current time. The data is gathered from the hourly aggregated table.
- 3m—Denotes the last three months of data from the current time. The data is gathered from the daily aggregated table.
- 6m—Denotes the last six months of data from the current time. The data is gathered from the weekly aggregated table.
- 1y—Denotes the past year (12 months) of data from the current time. The data is gathered from the weekly aggregated table.
- Custom—User-selected time period. You can set the day and time for the start and end dates. The use of a current or hourly, daily, or weekly aggregated source for data depends upon the selected start date.

The default, maximum and minimum retention periods for the aggregated data displayed in time-based graphs are controlled by administrators. For details, see "About Historical Data Retention" in Related Topics.

Related Topics

- Interactive Graphs
- How to Use Interactive Graphs
- About Historical Data Retention

Common UI Tasks

You can perform the following actions from nearly any window:

- Get Device Details from Device 360° View, on page 871
- Get User Details from the User 360° View
- Get VRF Details from Router 360° View

Get Device Details from Device 360° View

The Device 360° View provides detailed device information including device status, interface status, and associated device information. You can see the device 360° view from nearly all pages in which device IP addresses are displayed.

To launch the 360° view of any device, click the info icon next to the device IP address.

Note In the 360° View dialog, navigate to the Neighbors tab and click the info icon beside the IP address to view the 360 views of the looped devices.

Figure 58-5 shows a sample of the Device 360° View.

Note The features that appear in the Device 360° View differ depending on the device type.

User Interface Reference

Figure 32: Sample Device 360° View

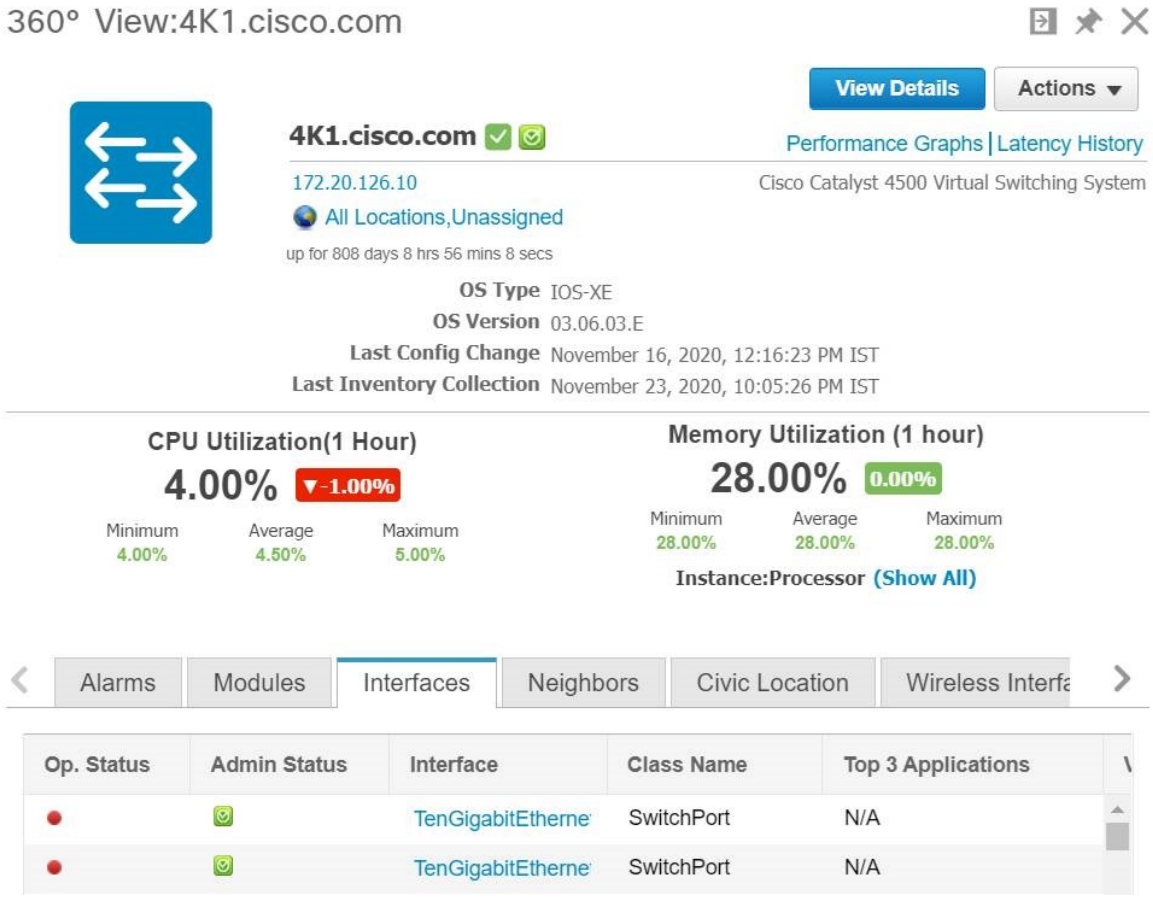


Table 88: Device 360° View Features

Device 360° View Feature	Description
Device status	Indicates whether the device is reachable, is being managed, and is synchronized with the .

Device 360° View Feature	Description
Action drop-down list	Choose one of the following options from the Action drop-down list at the top right of the device 360° view. • Alarm Browser—Launches the Alarm Browser. See -Monitor Alarms and Events for more information. • Device Details—Displays device details. • Support Community—Launches the Cisco Support Community. See Get Help from the Cisco Support Community and Technical Assistance Center (TAC)-. • Support Request—Allows you to open a support case. See Open a Cisco Support Case for more information. • Ping—Allows you to ping the device. • Traceroute—Allows you to perform a traceroute on the device. • Connect to Device—Allows you to connect to the device using Telnet, SSH, HTTP, and HTTPS protocols. • Sync Now—Allows you to synchronize the device with the configuration stored in the database. • Routing Table Info—Shows the VRF details for routers and nexus devices. **Note** There are some prerequisites for 360° view Telnet and SSH to work in client browser. • Firefox: Use external applications such as Putty for Telnet, and FireSSH add-on for SSH. • Internet Explorer (IE) and Google Chrome: Add Regedit entries for Telnet and SSH. See Related Topics
Alarms	Lists alarms on the device, including the alarm status, time stamp, and category.
Modules	Lists the device modules and their name, type, state, and ports.
Interfaces	Lists the device interfaces and the top three applications for each interface. Shows the configured VRFs (only for routers and nexus devices).
Neighbors	Lists the device neighbors, including their index, port, duplex status, and IP address. If the neighbor devices are managed in , the device name will have link to the device details page and the info icon allows to lauch the device 360° view.
Civic Location	Lists the Network Mobility Services Protocol (NMSP) status, civic address and location details of the device.
Wireless Interfaces	Lists the interface names, associated WLANs, VLAN IDs and IP addresses.
WLAN	Lists the WLAN names, SSIDs, security policies, and number of clients.
Recent Changes	Lists the last five audit changes made by user on the selected device. These changes are categorized as: • Inventory • Configuration • Software Image Management

Related Topics

- Connect to Devices Using Telnet and SSH With Internet Explorer and Google Chrome

Connect to Devices Using Telnet and SSH With Internet Explorer and Google Chrome

Before You Begin

Ensure that you have the Telnet and SSH browser plug-ins installed in Internet Explorer and Chrome.

Enable Telnet Client Functionality in Internet Explorer

To enable Telnet client functionality in 64 bit Windows operating System with 32 bit Internet Explorer, follow these steps:

Step 1 Open the Telnet client in control panel.

- Go to Control Panel.
- Click Programs And Features.
- Click Turn Windows features on or off in the left pane.
- Check the Telnet Client check box.
- Click OK.

Step 2 Copy the 64 bit version of telnet.exe from System32 in Windows directory to SysWOW64 in the same directory.

Step 3 Add the following registry key for the 32 bit version of Internet Explorer.

- Open regedit.exe and navigate to the following registry key:

Example:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_DISABLE_TELNET_PROTOCOL
```

- For backing up the key, right- click FEATURE_DISABLE_TELNET_PROTOCOL and select export. Save the key to a location where you can easily locate it when it needs to be restored.

  Note If this key does not exist, please add the key as named above.

- Right-click FEATURE_DISABLE_TELNET_PROTOCOL again and select New and select DWORD (32-bit) Value from the drop-down list.
- In the right pane, rename the New Value as iexplore.exe.
- Verify that the value for iexplore.exe is 0x00000000 and close regedit.exe.

Step 4 Copy the file System32\en-US\telnet.exe.mui to the folder SysWOW64\en-US.

Enable SSH

Follow these steps to start SSH session in Internet Explorer.

Step 1 Create a file called ssh.reg with the following content:

Example:

```
REGEDIT4
[HKEY_CLASSES_ROOT\ssh]
@="URL:ssh Protocol"
"URL Protocol"=""
[HKEY_CLASSES_ROOT\ssh\shell]
[HKEY_CLASSES_ROOT\ssh\shell\open]
[HKEY_CLASSES_ROOT\ssh\shell\open\command]
@="\"C:\\Program Files\\putty\\putty.exe\" \"%1\""
```

Step 2 Run this file to add the information to the Windows Registry.

Note If you perform Enable Telnet Client Functionality in Internet Explorer and Enable SSH, the changes will also be reflected in your Google chrome.

Related Topics

Get Device Details from Device 360° View, on page 871

Get User Details from the User 360° View

The User 360° View provides detailed information about an end user, including:

- End user network connection and association
- Authentication and authorization
- Possible problems with the network devices associated with the user's network attachment
- Application-related issues
- Other issues in the broader network

To access the 360° view for a user, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Clients and Users.

Step 2 Click the expand icon next to a user name under the UserName column. You can view the User 360° View.

The following figure shows a sample of the User 360° View.

User Interface Reference

Figure 33: Sample User 360° View

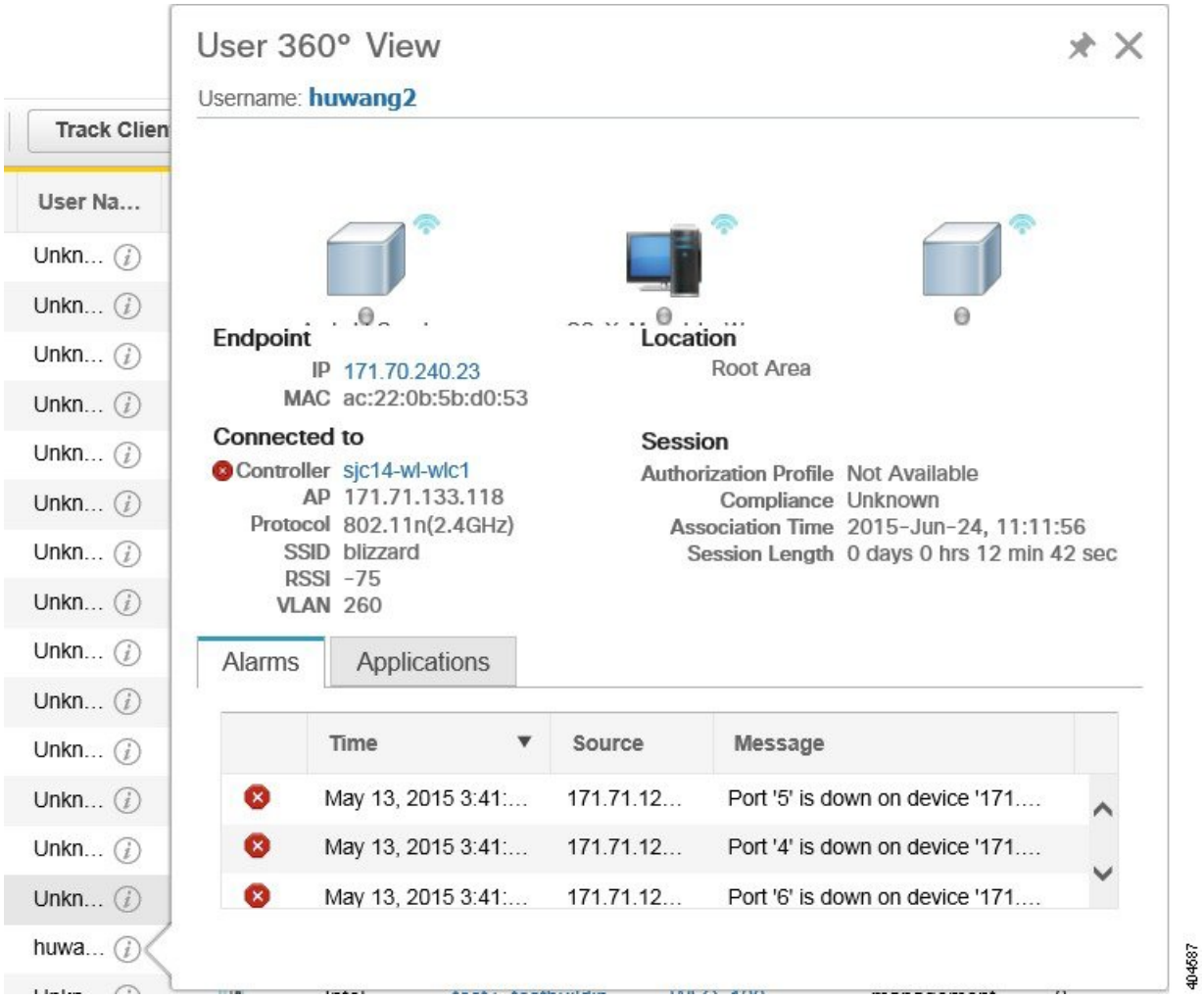


Table 89: User 360° View Features

User 360° View Feature	Description
User information	Displays key information about the end user.
Endpoint	Displays endpoint information. This feature requires integration with an ISE server.
Connected To	Displays network attachment information. • Network device (access switch or AP + Controller): Visible indication of existence and severity of any active alarms associated with the device • Attachment port: Visible indication of existence and severity of any active alarms associated with the port

User 360° View Feature	Description
LocationSession	Displays network session information. • The location is the hierarchy location. • Authorization Profile—Visible indication of the existence of any errors associated with authentication. This feature requires integration with an ISE server. • Endpoint compliance status. This feature requires integration with an ISE server. • Session start time and end time.
Alarms	Click the Alarms tab to view a list of alarms and statistics associated with the network session.
Applications	Click the Applications tab to view a list of applications and statistics associated with the network session. Session information (Netflow/NAM data, Assurance licenses) must be available.

Get VRF Details from Router 360° View

The router 360° view provides the VRF details for the following routing protocols:

- BGP Routes
- BGP Neighbors
- EIGRP Routes
- EIGRP Neighbors

To view the VRF details using the router 360° view, follow these steps:

Step 1 Choose Inventory Device Management > Network Devices.

Step 2 Choose Device Type > Routers in the Device Groups pane.

Step 3 Choose the router that you want to view the details.

The router details are displayed in a tabular form in the right pane.

Step 4 Click the info icon next to the router IP address.

Step 5 Choose Actions > Routing Table Info in the 360° view of the router.

Step 6 Choose the VRF from the Select a VRF drop-down list and choose the protocol that you want to view the routing details.

Search Methods

provides the following search methods:

- Application Search—See Use Application Search
- Advanced Search—See Use Application Search.
- Saved Search—See Use Saved Search

You can access the search options from any page within .

Use Application Search

To quickly search for data within , you can enter any text string such as a partial or complete IP address or a username if you are searching for a client.

Step 1 Click the Search icon at the top-right of the screen.

Step 2 In the Search text box, enter a search string and click Search .

Entering multiple strings in the Application Search text box will return all the results matching every keyword provided. You can also search for Managed Devices, Clients, Alarms, Config Archive, Change Audit, and Maps apart from applications.

Note The search will not return exact results if the search text contains special characters. Entering plain text in the search text box will return all the relevant results including the one with special characters.

Step 3 Click View List to view the matching devices from the Monitor or Configuration page.

Use Advanced Search

Step 1 Click the Search icon at the top-right of the screen.

Step 2 From the Search pulldown menu, select Advanced Search.

Step 3 In the Advanced Search dialog box, choose a category from the Search Category drop-down list.

Step 4 Choose all applicable filters or parameters for your search.

Note Search parameters change depending on the category that you selected.

Step 5 To save this search, select the Save Search check box, enter a unique name for the search in the text box, and click Go.

Note You can decide what information appears on the search results page.

The Search categories include the following:

- Access Points—See Find Access Points
- Alarms—See Find Alarms.
- Clients—See Find Alarms.
- Chokepoints—See Find Chokepoints
- Configuration Versions—See Find Configuration Versions
- Controller Licenses—See Find Controller Licenses.
- Controllers—See Find Controllers.
- Device Type—See Find Device Types.
- Events—See Find Events.
- Interferers—See Find Interferers.
- Jobs—See Find Jobs.

- Maps—See Find Maps.
- Rogue Client—See Find Rogue Clients.
- Shunned Client—See Find Shunned Clients.
- Switches—See Find Switches.
- Tags—See Find Tags.
- Wi-Fi TDOA Receivers—See Find Wi-Fi TDOA Receivers.

Find Alarms

You can configure the following parameters when performing an advanced search for alarms.

Table 90: Find Alarms Fields

Field	Options
Severity	Choose All Severities, CriticalMajor, Major, Minor, Warningor Clear.
Alarm Category	Choose All Types, System, Access Points,Controllers, Coverage Hole, , Config Audit, Mobility Service,Context Aware Notifications, SE Detected Interferers, Mesh Links, Rogue AP, Adhoc Rogue, Security, Performance, Application Performance, Routers, Switches and Hubs, or Cisco Interfaces and Modules.
Condition	Use the drop-down list to choose a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you have selected an alarm category, this drop-down list would contain the conditions available in that category.
Time Period	Choose a time increment from Any Time to Last 7 days. The default is Any Time.
Acknowledged State	Select this check box to search for alarms with an Acknowledged or Unacknowledged state. If this check box is not selected, the acknowledged state is not taken into search criteria consideration.
Assigned State	Select this check box to search for alarms with an Assigned or Unassigned state or by Owner Name. If this check box is not selected, the assigned state is not part of the search criteria. **Note** If you choose Assigned State > Owner Name, type the owner name in the available text box.

Find Jobs

You can configure the following parameters when performing an advanced search for jobs (see Table 58-5).

Table 91: Find Jobs Fields

Field	Options
Job Name	Type the name of the job that you want to search.
Job Type	Type the job type that you want to search.

Field	Options
Job Status	Choose All Status, Power, or Scheduled.

Note You can use wildcards such as *,? in the Job Name and Job Type text box to narrow or broaden your search.

Find Access Points

You can configure the following parameters when performing an advanced search for access points (see the following table).

Table 92: Find Access Points Fields

Field	Options
Search By	Choose All APs, Base Radio MAC, Ethernet MAC, AP Name, AP Model, AP Location, IP Address, Device Name, Controller IP, All Unassociated APs, Floor Area, Outdoor Area, Unassigned APs or Alarms. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select Floor Area, you also must identify its campus and building. Or, if you select Alarms, you can search for access points based on the severity of the alarm.
AP Type	Choose All Types, LWAPP, or Autonomous.
AP Mode	Choose All Modes, Local, Monitor, FlexConnect, Rogue Detector, Sniffer, , Bridge, or SE-Connect.
Radio Type	Choose All Radios, 802.11a, or 802.11b/g.
802.11n Support	Select this check box to search for access points with 802.11n support.
OfficeExtend AP Enabled	Select this check box to search for Office Extend access points.
CleanAir Support	Select this check box to search for access points which support CleanAir.
CleanAir Enabled	Select this check box to search for access points which support CleanAir and which are enabled.
Items per page	Configure the number of records to be displayed in the search results page.

Find Controller Licenses

You can configure the following parameters when performing an advanced search for controller licenses.

Table 93: Find Controller Licenses Fields

Field	Options
Controller Name	Type the controller name associated with the license search.
Feature Name	Choose All, Plus or Base depending on the license tier.

Field	Options
Type	Choose All, Evaluation, Extension, Grace Period, or Permanent.
% Used or Greater	Choose the percentage of the license use from this drop-down list. The percentages range from 0 to 100.
Items per page	Configure the number of records to be displayed in the search results page.

Find Controllers

You can configure the following parameters when performing an advanced search for controllers.

Table 94: Find Controllers Fields

Field	Options
Search for controller by	Choose All Controllers, IP Address, and Controller Name. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Enter Controller IP Address	This text box appears only if you choose IP Address from the Search for controller by drop-down list.
Enter Controller Name	This text box appears only if you choose Controller Name from the Search for controller by drop-down list.
Audit Status	Choose one of the following from the drop-down list: • All Status • Mismatch—Config differences were found between and controller during the last audit. • Identical—No configuration differences were found during the last audit. • Not Available—Audit status is unavailable.
Items per page	Configure the number of records to be displayed in the search results page.

Find Switches

You can configure the following parameters when performing an advanced search for switches.

Table 95: Find Switches Fields

Field	Options
Search for Switches by	Choose All Switches, IP Address, or Switch Name. You can use wildcards (*). For example, if you select IP Address and enter 172*, returns all switches that begin with IP address 172.
Items per page	Configure the number of records to be displayed in the search results page.

Find Clients

You can configure the following parameters when performing an advanced search for clients (see Table 58-10).

Table 96: Find Clients Fields

Field	Options
Media Type	Choose All, Wireless Clients or Wired Clients.
Wireless Type	Choose All, Lightweight, or Autonomous Clients if you chose Wireless Clients from the Media Type list.
Search By	Choose All Clients, All Excluded Clients, All Wired Clients, All Logged in Guests, IP Address,, User Name, MAC Address, Asset Name, Asset Category, Asset Group, AP Name, Controller Name, Controller IP, MSE IP, Floor Area, Outdoor Area, Switch Name, or Switch Type. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select IP address, you must enter the specific IP address for this search.
Clients Detected By	Choose Prime Infrastructure or MSEs. Clients detected by —Clients stored in databases. Clients detected by MSE—Clients located by Context Aware service in the MSE directly communicating with the controllers.
Client States	Choose All States, Idle, Authenticated, Associated, Probing, or Excluded.
Posture Status	Choose All, Unknown, Passed, Failed if you want to know if the devices are clean or not.
Restrict By Radio Band	Select the check box to indicate a specific radio band. Choose 5 GHz or 2.4 GHz from the drop-down list.
Restrict By Protocol	Select the check box to indicate a specific protocol. Choose 802.11a, 802.11b, 802.11g, 802.11n, or Mobile from the drop-down list.
SSID	Select the check box and choose the applicable SSID from the drop-down list.
Profile	Select the check box to list all of the clients associated to the selected profile. **Note** Once the check box is selected, choose the applicable profile from the drop-down list.

Field	Options
CCX Compatible	Select the check box to search for clients that are compatible with Cisco Client Extensions. **Note** Once the check box is selected, choose the applicable version, All Versions, or Not Supported from the drop-down list.
E2E Compatible	Select the check box to search for clients that are end–to–end compatible. **Note** Once the check box is selected, choose the applicable version, All Versions, or Not Supported from the drop-down list.
NAC State	Select the check box to search for clients identified by a certain Network Admission Control (NAC) state. **Note** Once the check box is selected, choose the applicable state from the drop-down list: Quarantine, Access, Invalid, and Not Applicable.
Include Disassociated	Select this check box to include clients that are no longer on the network but for which has historical records.
Items per page	Configure the number of records to be displayed in the search results page.

Find Chokepoints

You can configure the following parameters when performing an advanced search for chokepoints.

Table 97: Find Chokepoint Fields

Field	Options
Search By	Choose MAC Address or Chokepoint Name. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category. For example, when you select MAC address, you must enter the specific MAC address for this search.

Find Events

You can configure the following parameters when performing an advanced search for events .

Table 98: Find Events Fields

Field	Options
Severity	Choose All Severities, Critical, Major, Minor, Warning, Clear, or Info. Color coded.

Field	Options
Event Category	Choose All Types, Access Points, Controller, Security, Coverage Hole, Rogue AP, Adhoc Rogue, Interference, Mesh Links,Client, Mobility Service, Mobility Service, Location Notifications, re Coverage Hole, or Prime Infrastructure.
Condition	Use the drop-down list to choose a condition. Also, you can enter a condition by typing it in this drop-down list. **Note** If you selected an event category, this drop-down list contains the conditions available in that category.
Search All Events	Configure the number of records to be displayed in the search results page.

Find Interferers

You can configure the following parameters when performing an advanced search for interferers detected by access points.

Table 99: Find SE-Detected Interferers Fields

Field	Options
Search By	Choose All Interferers, Interferer ID, Interferer Category, Interferer Type, Affected Channel, Affected AP, Severity, Power, or Duty Cycle. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Detected By	Choose All Spectrum Experts or a specific spectrum expert from the drop-down list.
Detected within the last	Choose the time range for the interferer detections. The times range from 5 minutes to 24 hours to All History.
Interferer Status	From this drop-down list, choose All, Active, or Inactive.
Restrict by Radio Bands/Channels	Configure the search by radio bands or channels.
Items per page	Configure the number of records to be displayed in the search results page.

Find Wi-Fi TDOA Receivers

You can configure the following parameters when performing an advanced search for Wi-Fi TDOA receivers.

Table 100: Find Wi-Fi TDOA Receivers Fields

Field	Options
Search By	Choose MAC Address or Wi-Fi TDOA Receivers Name. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Find Maps

You can configure the following parameters when performing an advanced search for maps.

Table 101: Find Map Fields

Field	Options
Search for	Choose All Maps, Campuses, Buildings, Floor Areas, or Outdoor Areas.
Map Name	Search by Map Name. Enter the map name in the text box.
Items per page	Configure the number of records to be displayed in the search results page.

Find Rogue Clients

You can configure the following parameters when performing an advanced search for rogue clients.

Table 102: Find Rogue Client Fields

Field	Options
Search for clients by	Choose All Rogue Clients, , MAC Address, Controller, MSE, Floor Area, or Outdoor Area.
Search In	Choose MSEs or Prime Infrastructure Controllers.
Status	Select the check box and choose Alert, Contained, or Threat from the drop-down list to include status in the search criteria.

Find Shunned Clients

Note When a Cisco IPS sensor on the wired network detects a suspicious or threatening client, it alerts the controller to shun this client.

You can configure the following parameters when performing an advanced search for shunned clients.

Table 103: Find Shunned Client Fields

Field	Options
Search By	Choose All Shunned Clients, Controller, or IP Address. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.

Find Tags

You can configure the following parameters when performing an advanced search for tags.

Table 104: Find Tags Fields

Field	Options
Search for tags by	Choose All Tags,Asset Name, Asset Category, Asset Group, MAC Address, Controller, MSE, Floor Area, or Outdoor Area. **Note** Search parameters might change depending on the selected category. When applicable, enter the additional parameter or filter information to help identify the Search By category.
Search In	Choose MSEsor Prime Infrastructure Controllers.
Last detected within	Choose a time increment from 5 minutes to 24 hours. The default is 15 minutes.
Tag Vendor	Select the check box and choose Aeroscout, G2, PanGo, or WhereNet.
Telemetry Tags only	Select the Telemetry Tags only check box to search tags accordingly.
Items per page	Configure the number of records to be displayed in the search results page.

Find Device Types

You can configure the following parameters when performing an advanced search for device type.

Table 105: Find Device Type Fields

Field	Options
Select Device Type	Choose All Switches and Hubs, Wireless Controller, Unified AP, Autonomous AP, Unmanaged AP, or Routers.
Enter Device IP	Enter the IP address of the device selected in the Select Device Type field.

Find Configuration Versions

You can configure the following parameter when performing an advanced search for configuration versions.

Table 106: Find Configuration Versions Fields

Field	Options
Enter Tag	Enter the tag name.

Use Saved Search

Note Saved searches apply only to the current partition.

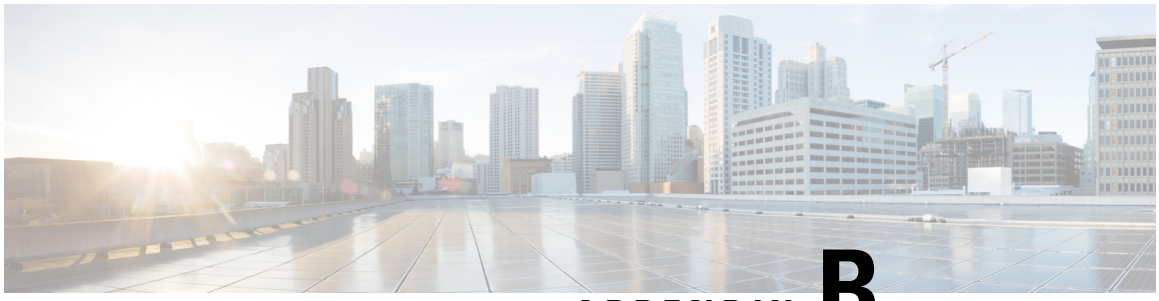
To access and run a previously saved search, follow these steps:

Step 1 Click the icon in the Application Search box, then click Saved Search.

Step 2 Choose a category from the Search Category drop-down list, then choose a saved search from the Saved Search List drop-down list.

Step 3 If necessary, change the current parameters for the saved search, then click Go.

User Interface Reference



APPENDIX B

Icon and State Reference

This section contains the following topics:

Device Reachability and Admin States

Device Reachability State—Indicates whether can communicate with the device using all configured protocols.

Table 107: Device Reachability State

Icon	Device Reachability State	Description	Troubleshooting
	Reachable	can reach the device using SNMP, or the NCS 2K device using ICMP.	—
	Ping reachable	can reach the device using Ping, but not via SNMP.	Although ICMP ping is successful, check for all possible reasons why SNMP communication is failing. Check that device SNMP credentials are the same in both the device and in , whether SNMP is enabled on the device, or whether the transport network is dropping SNMP packets due to reasons such as mis-configuration, etc. .
	Unreachable	cannot reach the device using Ping.	Verify that the physical device is operational and connected to the network.
	Unknown	cannot connect to the device.	Check the device.

Device Admin State—Indicates the configured state of the device (for example, if an administrator has manually shut down a device, as opposed to a device being down because it is not reachable by Ping).

Table 108: Device Admin State

Device Admin State	Description	Troubleshooting
Managed	is actively monitoring the device.	Not Applicable.
Maintenance	is checking the device for reachability but is not processing traps, syslogs, or TL1 messages.	To move a device back to Managed state, see Move a Device To and From Maintenance State, on page 41.
Unmanaged	is not monitoring the device.	In the Network Devices table, locate the device and click the "i" icon next to the data in the Last Inventory Collection Status column. The popup window will provide details and troubleshooting tips. Typical reasons for collection problems are: • Device SNMP credentials are incorrect. • The deployment has exceeded the number of devices allowed by its license. • A device is enabled for switch path tracing only. If a device type is not supported, its Device Type will be Unknown. You can check if support for that device type is available from Cisco.com by choosing Administration > Licenses and Software Updates > Software Update and then clicking Check for Updates.
Unknown	cannot connect to the device.	Check the device.

Port or Interface States

Port or Interface Primary States—Conveys the most important state information for a port or interface by combining the admin and operational states. The Multilayer Trace displays either a port's primary state or alarm status. For the Chassis View, if an element does not support the changing of color to indicate a state change, you can still get the state change information from the alarm that is generated.

Note If there is an alarm associated with a port/interface, alarm icon will show up, port icon will not show. The alarm is shown only in case the port is not in test or admin down state.

Port or Interface Primary State	Icon	Admin Status	Operational State

Unknown		Unknown	Unknown
Down		Up	Down
Test		Test	—
Admin Down		Admin Down	—
Up		Up	Up
Auto Up		Up	Auto Up

Port or Interface Admin Status—Represents the configured state of the port or interface (for example, if an administrator has manually shut down a port).

Port or Interface Admin Status	Icon	Description
Unknown		Port or interface admin status is unknown. There is no response (or insufficient response) from the device.
Admin Down		Port or interface was manually shut down by the administrator.
Up		Port or interface is enabled by the administrator.
Test		Port or interface is being tested by the administrator.

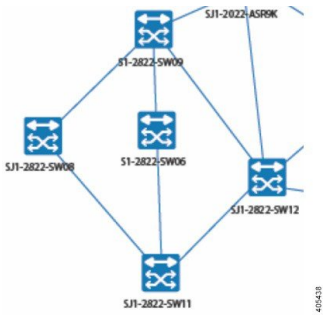
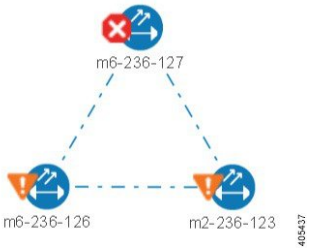
Port or Interface Operational State—Conveys the port or interface's running state and whether it is working properly.

Port or Interface Operational State	Icon	Description
Unknown		Port or interface operational state is unknown. There is no response (or insufficient response) from the device.
Down		Port or interface is not working properly.
Up		Port or interface is receiving and transmitting data.
Auto Up		Port or interface is receiving and transmitting data (only certain devices support this state; other devices use "Up").

Link Serviceability States

Link Characteristics

The following table describes the different types of links used to represent the connection between devices in the Topology Map view of .

Link Type	Description
	Solid Line-—Indicates a physical, topological, or service link, such as a link between two devices.
	Dashed Line—Indicates an association or business link between elements such as EVCs, VPLS service instances, or VPN components.

Equipment Operational States (Chassis View)

The equipment operational states represent the running state of the network element.

Equipment Operational State	Icon	Description
In Service	(none)	Equipment is operating properly.
Pre-provisioned		(Cisco NCS 2000 and Cisco ONS devices only) Equipment has been configured but is not physical present in the chassis.
Failed/Disabled/Down/Out of Service/Out of Service Maintenance		Equipment is not operating properly.
Unknown		Equipment operational state is unknown. No response (or insufficient response) from the device.

Alarm Severity Icons

The table below lists the alarm colors and their respective severity levels for the icons displayed in various parts of the web GUI.

Severity Icon	Description	Color
	Critical alarm	Red
	Major alarm	Orange
	Minor alarm	Yellow
	Warning alarm	Light Blue
	Alarm cleared; normal, OK	Green
	Informational alarm	Medium Blue
	Indeterminate alarm	Dark Blue

Device Type Icons

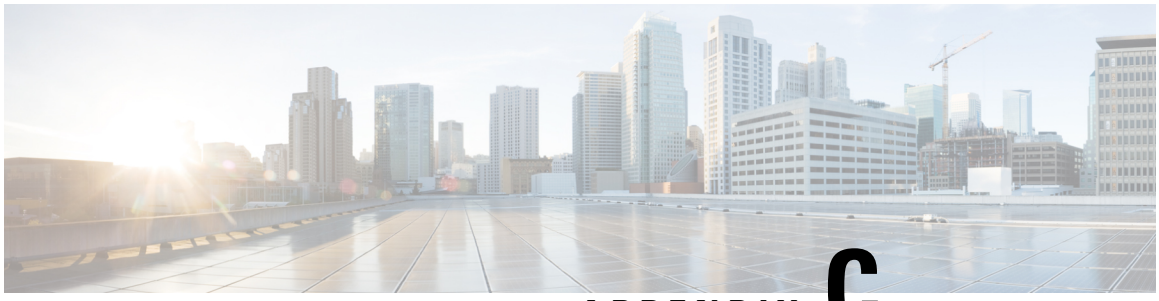
Table below defines the icons used to represent different device types in the Topology and the Multi-layer Trace views in .

Icon	Definition
	Switch
	Router
	Router Aggregated

Icon	Definition
	Cisco NCS 6000 device on which a Secure Domain Router (SDR) resides. The SDR's name is listed directly above the device's icon. **Note** There may be cases where the SDR label for a device that belongs to a cluster or user-defined group is not displayed (since auto-clustering is applied to devices based on their proximity).
	Router configured with an L3VPN service.
	Switch Aggregated
	Access Point
	Service Module
	UCS C-Series
	NAM Blade
	Group
	Generic Device

Icon	Definition
	Virtual Server
	Wireless LAN Controller
	Unknown
	DWDM ROADM Regeneration/NCS 2000

Icon and State Reference



APPENDIX C

Time Zones Supported by

Time Zones Supported by

This table lists the available values for the system time zone.

Africa/Abidjan	America/St_Johns	Etc/GMT+6
Africa/Accra	America/St_Kitts	Etc/GMT+7
Africa/Addis_Ababa	America/St_Lucia	Etc/GMT+8
Africa/Algiers	America/St_Thomas	Etc/GMT+9
Africa/Asmara	America/St_Vincent	Etc/GMT0
Africa/Asmera	America/Swift_Current	Etc/GMT-0
Africa/Bamako	America/Tegucigalpa	Etc/GMT-1
Africa/Bangui	America/Thule	Etc/GMT-10
Africa/Banjul	America/Thunder_Bay	Etc/GMT-11
Africa/Bissau	America/Tijuana	Etc/GMT-12
Africa/Blantyre	America/Toronto	Etc/GMT-13
Africa/Brazzaville	America/Tortola	Etc/GMT-14
Africa/Bujumbura	America/Vancouver	Etc/GMT-2
Africa/Cairo	America/Virgin	Etc/GMT-3
Africa/Casablanca	America/Whitehorse	Etc/GMT-4
Africa/Ceuta	America/Winnipeg	Etc/GMT-5
Africa/Conakry	America/Yakutat	Etc/GMT-6

Time Zones Supported by

Africa/Dakar	America/Yellowknife	Etc/GMT-7
Africa/Dar_es_Salaam	Antarctica/Casey	Etc/GMT-8
Africa/Djibouti	Antarctica/Davis	Etc/GMT-9
Africa/Douala	Antarctica/DumontDUrville	Etc/Greenwich
Africa/El_Aaiun	Antarctica/Mawson	Etc/UCT
Africa/Freetown	Antarctica/McMurdo	Etc/Universal
Africa/Gaborone	Antarctica/Palmer	Etc/UTC
Africa/Harare	Antarctica/Rothera	Etc/Zulu
Africa/Johannesburg	Antarctica/South_Pole	Europe/Amsterdam
Africa/Kampala	Antarctica/Syowa	Europe/Andorra
Africa/Khartoum	Antarctica/Vostok	Europe/Athens
Africa/Kigali	Arctic/Longyearbyen	Europe/Belfast
Africa/Kinshasa	Asia/Aden	Europe/Belgrade
Africa/Lagos	Asia/Almaty	Europe/Berlin
Africa/Libreville	Asia/Amman	Europe/Bratislava
Africa/Lome	Asia/Anadyr	Europe/Brussels
Africa/Luanda	Asia/Aqtau	Europe/Bucharest
Africa/Lubumbashi	Asia/Aqtobe	Europe/Budapest
Africa/Lusaka	Asia/Ashgabat	Europe/Chisinau
Africa/Malabo	Asia/Ashkhabad	Europe/Copenhagen
Africa/Maputo	Asia/Baghdad	Europe/Dublin
Africa/Maseru	Asia/Bahrain	Europe/Gibraltar
Africa/Mbabane	Asia/Baku	Europe/Guernsey
Africa/Mogadishu	Asia/Bangkok	Europe/Helsinki
Africa/Monrovia	Asia/Beirut	Europe/Isle_of_Man
Africa/Nairobi	Asia/Bishkek	Europe/Istanbul
Africa/Ndjamena	Asia/Brunei	Europe/Jersey
Africa/Niamey	Asia/Calcutta	Europe/Kaliningrad
Africa/Nouakchott	Asia/Choibalsan	Europe/Kiev

Africa/Ouagadougou	Asia/Chongqing	Europe/Lisbon
Africa/Porto-Novo	Asia/Chungking	Europe/Ljubljana
Africa/Sao_Tome	Asia/Colombo	Europe/London
Africa/Timbuktu	Asia/Dacca	Europe/Luxembourg
Africa/Tripoli	Asia/Damascus	Europe/Madrid
Africa/Tunis	Asia/Dhaka	Europe/Malta
Africa/Windhoek	Asia/Dili	Europe/Mariehamn
America/Adak	Asia/Dubai	Europe/Minsk
America/Anchorage	Asia/Dushanbe	Europe/Monaco
America/Anguilla	Asia/Gaza	Europe/Moscow
America/Antigua	Asia/Harbin	Europe/Nicosia
America/Araguaina	Asia/Ho_Chi_Minh	Europe/Oslo
America/Argentina/	Asia/Hong_Kong	Europe/Paris
America/Argentina/	Asia/Hovd	Europe/Podgorica
America/Argentina/Catamarca	Asia/Irkutsk	Europe/Prague
America/Argentina/Cordoba	Asia/Istanbul	Europe/Riga
America/Argentina/Jujuy	Asia/Jakarta	Europe/Rome
America/Argentina/La_Rioja	Asia/Jayapura	Europe/Samara
America/Argentina/Mendoza	Asia/Jerusalem	Europe/San_Marino
America/Argentina/Rio_Gallegos	Asia/Kabul	Europe/Sarajevo
America/Argentina/Salta	Asia/Kamchatka	Europe/Simferopol
America/Argentina/San_Juan	Asia/Karachi	Europe/Skopje
America/Argentina/San_Luis	Asia/Kashgar	Europe/Sofia
America/Argentina/Tucuman	Asia/Kathmandu	Europe/Stockholm
America/Argentina/Ushuaia	Asia/Katmandu	Europe/Tallinn
America/Aruba	Asia/Kolkata	Europe/Tirane
America/Asuncion	Asia/Krasnoyarsk	Europe/Tiraspol
America/Atikokan	Asia/Kuala_Lumpur	Europe/Uzhgorod
America/Atka	Asia/Kuching	Europe/Vaduz

Time Zones Supported by

America/Bahia	Asia/Kuwait	Europe/Vatican
America/Barbados	Asia/Macao	Europe/Vienna
America/Belem	Asia/Macau	Europe/Vilnius
America/Belize	Asia/Magadan	Europe/Volgograd
America/Blanc-Sablon	Asia/Makassar	Europe/Warsaw
America/Boa_Vista	Asia/Manila	Europe/Zagreb
America/Bogota	Asia/Muscat	Europe/Zaporozhye
America/Boise	Asia/Nicosia	Europe/Zurich
America/Buenos_Aires	Asia/Novosibirsk	Factory
America/Cambridge_Bay	Asia/Omsk	GB
America/Campo_Grande	Asia/Oral	GB-Eire
America/Cancun	Asia/Phnom_Penh	GMT
America/Caracas	Asia/Pontianak	GMT+0
America/Catamarca	Asia/Pyongyang	GMT0
America/Cayenne	Asia/Qatar	GMT-0
America/Cayman	Asia/Qyzylorda	Greenwich
America/Chicago	Asia/Rangoon	Hongkong
America/Chihuahua	Asia/Riyadh	HST
America/Coral_Harbour	Asia/Riyadh87	Iceland
America/Cordoba	Asia/Riyadh88	Indian/Antananarivo
America/Costa_Rica	Asia/Riyadh89	Indian/Chagos
America/Cuiaba	Asia/Saigon	Indian/Christmas
America/Curacao	Asia/Sakhalin	Indian/Cocos
America/Danmarkshavn	Asia/Samarkand	Indian/Comoro
America/Dawson	Asia/Seoul	Indian/Kerguelen
America/Dawson_Creek	Asia/Shanghai	Indian/Mahe
America/Denver	Asia/Singapore	Indian/Maldives
America/Detroit	Asia/Taipei	Indian/Mauritius
America/Dominica	Asia/Tashkent	Indian/Mayotte

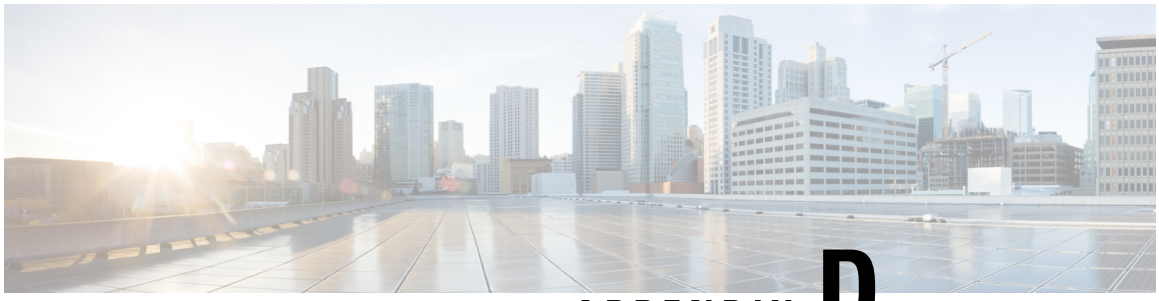
America/Edmonton	Asia/Tbilisi	Indian/Reunion
America/Eirunepe	Asia/Tehran	Iran
America/El_Salvador	Asia/Tel_Aviv	Israel
America/Ensenada	Asia/Thimbu	Jamaica
America/Fort_Wayne	Asia/Thimphu	Japan
America/Fortaleza	Asia/Tokyo	Kwajalein
America/Glace_Bay	Asia/Ujung_Pandang	Libya
America/Godthab	Asia/Ulaanbaatar	MET
America/Goose_Bay	Asia/Ulan_Bator	Mexico/BajaNorte
America/Grand_Turk	Asia/Urumqi	Mexico/BajaSur
America/Grenada	Asia/Vientiane	Mexico/General
America/Guadeloupe	Asia/Vladivostok	Mideast/Riyadh87
America/Guatemala	Asia/Yakutsk	Mideast/Riyadh88
America/Guayaquil	Asia/Yekaterinburg	Mideast/Riyadh89
America/Guyana	Asia/Yerevan	MST
America/Halifax	Atlantic/Azores	MST7MDT
America/Havana	Atlantic/Bermuda	Navajo
America/Hermosillo	Atlantic/Canary	New_Salem
America/Indiana/Indianapolis	Atlantic/Cape_Verde	NZ
America/Indiana/Knox	Atlantic/Faeroe	NZ-CHAT
America/Indiana/Marengo	Atlantic/Faroe	Pacific/Apia
America/Indiana/Petersburg	Atlantic/Jan_Mayen	Pacific/Auckland
America/Indiana/Tell_City	Atlantic/Madeira	Pacific/Chatham
America/Indiana/Vevay	Atlantic/Reykjavik	Pacific/Easter
America/Indiana/Vincennes	Atlantic/South_Georgia	Pacific/Efate
America/Indiana/Winamac	Atlantic/St_Helena	Pacific/Enderbury
America/Indianapolis	Atlantic/Stanley	Pacific/Fakaofo
America/Inuvik	Australia/ACT	Pacific/Fiji
America/Iqaluit	Australia/Adelaide	Pacific/Funafuti

Time Zones Supported by

America/Jamaica	Australia/Brisbane	Pacific/Galapagos
America/Jujuy	Australia/Broken_Hill	Pacific/Gambier
America/Juneau	Australia/Canberra	Pacific/Guadalcanal
America/Kentucky/Louisville	Australia/Currie	Pacific/Guam
America/Kentucky/Monticello	Australia/Darwin	Pacific/Honolulu
America/Knox_IN	Australia/Eucla	Pacific/Johnston
America/La_Paz	Australia/Hobart	Pacific/Kiritimati
America/Lima	Australia/LHI	Pacific/Kosrae
America/Los_Angeles	Australia/Lindeman	Pacific/Kwajalein
America/Louisville	Australia/Lord_Howe	Pacific/Majuro
America/Maceio	Australia/Melbourne	Pacific/Marquesas
America/Managua	Australia/North	Pacific/Midway
America/Manaus	Australia/NSW	Pacific/Nauru
America/Marigot	Australia/Perth	Pacific/Niue
America/Martinique	Australia/Queensland	Pacific/Norfolk
America/Mazatlan	Australia/South	Pacific/Noumea
America/Mendoza	Australia/Sydney	Pacific/Pago_Pago
America/Menominee	Australia/Tasmania	Pacific/Palau
America/Merida	Australia/Victoria	Pacific/Pitcairn
America/Mexico_City	Australia/West	Pacific/Ponape
America/Miquelon	Australia/Yancowinna	Pacific/Port_Moresby
America/Moncton	Brazil/Acre	Pacific/Rarotong
America/Monterrey	Brazil/DeNoronha	Pacific/Saipan
America/Montevideo	Brazil/East	Pacific/Samoa
America/Montreal	Brazil/West	Pacific/Tahiti
America/Montserrat	Buenos_Aires	Pacific/Tarawa
America/Nassau	Canada/Atlantic	Pacific/Tongatapu
America/New_York	Canada/Central	Pacific/Truk
America/Nipigon	Canada/Eastern	Pacific/Wake

America/Nome	Canada/East-Saskatchewan	Pacific/Wallis
America/Noronha	Canada/Mountain	Pacific/Yap
America/North_Dakota/	Canada/Newfoundland	Poland
America/North_Dakota/Center	Canada/Pacific	Portugal
America/Panama	Canada/Saskatchewan	PRC
America/Pangnirtung	Canada/Yukon	PST8PDT
America/Paramaribo	CET	ROC
America/Phoenix	Chile/Continental	ROK
America/Port_of_Spain	Chile/EasterIsland	Singapore
America/Port-au-Prince	ComodRivadavia	Turkey
America/Porto_Acre	CST6CDT	UCT
America/Porto_Velho	Cuba	Universal
America/Puerto_Rico	EET	US/Alaska
America/Rainy_River	Egypt	US/Aleutian
America/Rankin_Inlet	Eire	US/Arizona
America/Recife	EST	US/Central
America/Regina	EST5EDT	US/Eastern
America/Resolute	Etc/GMT	US/East-Indiana
America/Rio_Branco	Etc/GMT+0	US/Hawaii
America/Rosario	Etc/GMT+1	US/Indiana-Starke
America/Santarem	Etc/GMT+10	US/Michigan
America/Santiago	Etc/GMT+11	US/Mountain
America/Santo_Domingo	Etc/GMT+12	US/Pacific
America/Sao_Paulo	Etc/GMT+2	US/Samoa
America/Scoresbysund	Etc/GMT+3	UTC
America/Shiprock	Etc/GMT+4	WET
America/St_Barthelemy	Etc/GMT+5	W-SU
		Zulu

Time Zones Supported by



APPENDIX D

FAQs: Operations Center and Prime Infrastructure

FAQs: Operations Center and

Alarms and Events

Q. Why doesn't the aggregated Alarm Summary count shown in Operations Center match the same count shown in the managed instances of ?

A. Users must make sure that Operations Center and all the instances it is managing are using the same alarm categories.

To ensure that Operations Center and all the instances are using the same categories:

1. Log on to Operations Center using an ID with administrator privileges, then select Administration > User Preferences.
2. Under Alarms, click Edit Alarm Categories.
3. Take note of the alarm categories currently selected for Operations Center. Under normal circumstances, the following categories will be selected:
    - Alarm Summary
    - AP
    - Controller
    - Coverage Holes
    - Mesh Links
    - Mobility Service
    - Performance

FAQs: Operations Center and Prime Infrastructure

- Rogue AP
- Security
- Routers
- Application Performance
- Switches and Hubs
- System

4. If you need to change any of the selections, click the check box next to the alarm category you want to select or deselect, then click Done.
5. Repeat the preceding steps on each of the managed instances of , ensuring that the same selections are made on each instance.

Q. Why doesn't the total alarm count shown in Operations Center match the same count shown in the managed instances?

A. By default, Operations Center counts all alarms when calculating the total alarm count, but the managed instances of hide Acknowledged and Cleared alarms. If you want the total alarm count on all the managed instances to match the alarm count in Operations Center, you must set all the managed instances to show Acknowledged and Cleared alarms:

1. Log in to the first managed instance of .
2. Select Administration System SettingsAlarms and Events.
3. Under Alarm Display Options, make sure that the check boxes next to "Hide acknowledged alarms" and "Hide cleared alarms" are both unchecked.
4. Click Save to save your changes.
5. Repeat these steps on all the other managed instances.

Q. Why doesn't the aggregated Events and Syslogs count shown in Operations Center match the same count shown in the managed instances?

A. Events and syslogs, by their nature, are constantly changing on managed instances. You can see this for yourself by clicking on the refresh button every five seconds. There is always a slight lag from the time the Event and Syslog count changes to when that count is updated in the corresponding NBI call. Since this is constantly changing, the aggregated count displayed in Operations Center should not be compared to the individual managed instances.

Cross Launching

Q. Why are there discrepancies when cross-launching from the Network Device Summary (NDS) dashlet to the Devices page for Wireless Controllers (WLCs)?

A. This is an issue with differences in the way fetches data for dashlets and individual wireless devices. To get the Network Device Summary count, the dashlet queries a data structure that has an entry when the device is reachable, but does not check the inventory collection status. When you cross-launch the Devices page for the open WLC, the count comes from a table that has an entry only when the inventory

collection status is successful(at least once) for the device. Please note that this is an issue in , not Operations Center.

Q. Are there known Issues with cross launching from a specific device group on the Network Devices page?

A. There is a known issue with cross-launching from a specific device group under the Network Devices page in Operations Center to the same device group in a managed instance. The user is redirected to the Network Devices page in the managed instance, but all the device groups are displayed instead of the device group selected in Operations Center.

Q. Why isn't cross-launching working properly for third-party APs on the Network Device Summary dashlet?

A. There is a known issue in cross-launching from the Network Device Summary dashlet for third-party APs in Operations Center. When you cross-launch from Operations Center, none of the third-party APs are displayed on the Network Devices page.

Q. Cross-launching for syslogs does not work as expected.

A. Currently, does not support filtering by Instance ID for syslogs. As a result, Operations Center cannot support filtering on syslogs when cross-launching to a managed instance of .

Devices

Q. Why are there differences between the VLAN ID and Association ID on the Clients and Users page in Operations Center and the same page given in the managed instances?

A. This happens due to quick updating of these values. If you update these values in Operations Center, the same data on a managed instance may have already changed.

Q. Why is there a discrepancy between what Operations Center and the managed instances show in the "CPU Utilization" and "Memory Utilization" fields for Autonomous APs on the Device Details page?

A. One reason for the discrepancy is that these values change very quickly. When you update these values in Operations Center, the same data on one or more of the managed instances may have already changed.

Reporting

Q. Why do Operations Center and have minor discrepancies in the report values they generate?

A. This is expected behavior. generates its report values using fractional values at its disposal, but Operations Center aggregates these values using a set of rounded numbers. This results in the discrepancies.

Q. Why is report data not being polled from 2.1 instances?

A. If you try to generate a report in Operations Center with the same name as an existing report on a 2.1 instance, the data for that instance will be ignored in Operations Center. To work around this issue, specify a report name that is unique across both Operations Center and all your managed instances.

Miscellaneous

Q. Why isn't site information retrieved from 2.1 managed instances?

A. When choosing Performance > Device > ***Select a Device*** > Site, the site information for 2.1 instances is not retrieved. This is due to an internal (IFM) API that changed between version 2.1 and 2.2.

Q. Why do Operations Center and have different columns for the Current Associated Wired Clients table?

A. The Current Associated Wired Clients table in Operations Center has fixed columns. The same table in managed instances of has customizable columns. Later versions of Operations Center may change this.

FAQs: Operations Center and Prime Infrastructure