



Cisco Prime Infrastructure 3.5 Administrator Guide

First Published: 2018-05-10

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1

Set Up the Prime Infrastructure Server 1

- Server Setup Tasks 1
- User Management Setup Tasks 2
- Fault Management Setup Tasks 3
- Administrator Setup Tasks 4
 - Set Up Operations Center 4
 - Activate Your Operations Center License 4
 - Add Instances to Operations Center 6
 - Disable Idle User Timeouts for Operations Center 6
 - Enable AAA for Operations Center 7
- Required Software Versions and Configurations 8
 - Configure SNMP 8
 - Configure NTP 9
- Configure Data Sources for With Assurance 9
 - Supported Assurance Data Sources 9
 - Configure Assurance Data Sources 10
- Enable Medianet NetFlow 11
- Enable NetFlow and Flexible NetFlow 13
- Deploy Network Analysis Modules NAMs 14
- Enable Performance Agent 15
- Install Patches 16

CHAPTER 2

Licenses and Software Updates 19

- Prime Infrastructure Licensing 19

Purchase Prime Infrastructure Licenses	20
Verify License Details	20
Add Licenses	21
Delete Licenses	21
Troubleshoot Licenses	21
Controller Licensing	23
MSE Licensing	25
MSE License Structure Matrix	25
Sample MSE License File	25
Revoke and Reuse an MSE License	26
MSE Services Coexistence	27
Manage MSE Licenses	27
Register Product Authorization Keys	28
Install Client and wIPS License Files	29
Delete Mobility Services Engine License Files	29
Assurance Licensing	30
Verify Assurance License Details	30
Add License Coverage For NetFlow and NAM Devices	31
Delete License Coverage for NetFlow and NAM Devices	31
Smart Licensing	32
Set Up Cisco Smart Licensing on Prime Infrastructure	32
Set Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager	33
Enable Smart License on Prime Infrastructure	34
Register Prime Infrastructure with the Cisco Smart Software Manager	35
Generate Token ID	35
Convert from Traditional Licensing	35
Register Product Instance	36
Choose Smart Software Licenses	36
Configure License Thresholds for the Prime Infrastructure License Dashboard	37
View the Licensing Dashboard	37
Disable Smart Licensing	38
Perform Additional Actions	38
Reference: Product Registration and License Authorization Statuses	39
Manage Software Updates	40

What Are Software Updates?	40
View the Installed Product Software Version	40
View Installed Software Updates	41
Enable or Disable Notifications About Software Updates	41
Validate Images (ISO and OVA) Before Installing Them	41
Download and Install a Software Update from Cisco.com	43
Copy a File from a Client Machine to the Server	44

CHAPTER 3
Backup and Restore 45

Backup and Restore Concepts	45
Backup Types: Application and Appliance	45
Backup Scheduling	46
Backup Repositories	46
Backup Filenames	47
Backup Validation Process	48
Information That Is Backed Up	48
Information That Is Not Backed Up	50
Set Up and Manage Repositories	50
Create a Local Backup Repository	50
Use a Remote Backup Repository	51
Use Remote NFS Backup Repositories	51
How to Use Remote SFTP Backup Repositories	52
How to Use Remote FTP Backup Repositories	53
Delete a Local Backup Repository	54
Set Up Automatic Application Backups	54
Schedule Automatic Application Backups	55
Specify the Backup Repository for Automatic Backups	55
Change the Number of Automatic Application Backups That Are Saved	55
Perform a Manual Backup	56
Perform an Immediate Appliance Backup Using the CLI	56
Perform an Immediate Application Backup Using the Web GUI	56
Perform an Immediate Application Backup Using the CLI	57
Perform a Manual Appliance Backup	57
Restore Data	57

Restore an Application Backup	58
Restore an Appliance Backup	58
Recover from Failed Restores	59
How to Manage Disk Space Issues During Backup and Restore	59
Migrate to Another Virtual Appliance Using Backup and Restore	60
Migrate to Another Physical Appliance Using Backup and Restore	61
Backup and Restore with Operations Center	61

CHAPTER 4**Configure the Prime Infrastructure Server 63**

View the Server Configuration	63
Available System Settings	64
Secure the Connectivity of the Server	70
Set Up HTTPS Access to Prime Infrastructure	70
Generate and Apply Self-Signed Certificates	71
Import CA-Signed Host Certificates	71
Import Private Key	73
Export Private Key	74
Set Up Certificate Validation	74
MIB to Prime Infrastructure Alert/Event Mapping	75
Establish an SSH Session With the Server	78
Set Up NTP on the Server	78
Set Up the Proxy Server	79
Configure Server Port and Global Timeout Settings	79
Set Up the SMTP E-Mail Server	80
Enable FTP/TFTP/SFTP Service on the Server	80
Configure Stored Cisco.com Credentials	81
Create a Login Banner (Login Disclaimer)	81
Stop and Restart	81
Configure Global SNMP Settings for Communication with Network Elements	82
Configure Global SNMP Settings	82
View SNMP Credential Details	83
Add SNMP Credentials	84
Import SNMP Credentials	85
Enable Compliance Services	87

Configure ISE Servers	87
Configure Software Image Management Servers	88
Add Device Information to a User Defined Field	88
Manage OUIs	89
Add a New Vendor OUI Mapping	89
Upload an Updated Vendor OUI Mapping File	89
Sample Log File from North-Bound SNMP Receiver	90
Work With Server Internal SNMP Traps That Indicate System Problems	90
Customize Server Internal SNMP Traps and Forward the Traps	91
Troubleshoot Server Internal SNMP Traps	91
Set Up Defaults for Cisco Support Requests	92
Configure Cisco Product Feedback Settings	92
Migrating Data from Prime Infrastructure to Cisco Digital Network Architecture Center	93

CHAPTER 5**Maintain Prime Infrastructure Server Health 97**

Overview Dashboard	97
Performance Dashboard	98
Admin Dashboard	98
How to Evaluate OVA Size and System Resources	99
View the Number of Devices Prime Infrastructure Is Managing	100
How to Improve the Performance of Prime Infrastructure	101
Tune the Server	101
Modify VM Resource Allocation Using VMware vSphere Client	101
Compact the Prime Infrastructure Database	102
Configure Client Performance Settings	102
Enable Automatic Client Troubleshooting	103
Enable DNS Hostname Lookup	103
Specify How Long to Retain Client Association History Data	104
Poll Clients When Receiving Client Traps/Syslogs	104
Save Client Traps as Events	105
Save 802.1x and 802.11 Client Traps as Events	105
Enable Enhanced Client Traps	105
Optimize Memory for Assurance Processing	106
Monitor Assurance Memory Allocation and Demand	106

- Increase the Assurance Memory Pool Via CLI 107
- How to Balance the Assurance Memory Allocation 107
- Reset Assurance Memory Allocation 108
- Reset the Assurance Memory Pool 108
- Manage Data Sources 108
 - View Current Data Sources 109
 - Delete Data Sources 110
- Special Administrative Tasks 110
 - How to Connect Via CLI 111
 - Start Prime Infrastructure 111
 - Check Prime Infrastructure Server Status 112
 - Check Prime Infrastructure Version and Patch Status 112
 - Stop Prime Infrastructure 113
 - Restart Prime Infrastructure Using CLI 113
 - Restart Prime Infrastructure Using GUI 113
 - How to Remove Prime Infrastructure 114
 - Reset Prime Infrastructure to Defaults 114
 - Change the Prime Infrastructure Host Name 115
 - Enable the FTP User 115
 - Change the Root User Password 116
 - Change the Admin Password using CLI 116
 - How to Recover Administrator Passwords on Virtual Appliances 117
 - How to Recover Administrator Passwords on Physical Appliances 118
 - 119
 - How to Recover Administrator Passwords on Hyper-V Virtual Appliances 120
 - How to Get the Installation ISO Image 121
- How to Update Prime Infrastructure With Latest Software Updates 122
 - View Installed and Available Software Updates 122
 - How to Get Software Update Notifications 123
 - Configure Software Update Notifications 123
 - View Details of Installed Software Updates 124
 - View Installed Updates From the Login Page 124
 - View Installed Updates From the About Page 124
 - Install Software Updates 125

Install Software Updates from Cisco.com	125
Upload and Install Downloaded Software Updates	126
How to Use Your Cisco.com Account Credentials with Prime Infrastructure	126
Save Cisco.com Account Credentials in Prime Infrastructure	127
Deleting Cisco.com Account Credentials	127
How to Configure Support Request Settings	127
How to Manage Disk Space Issues	128

CHAPTER 6
Data Collection and Background Tasks 131

Control Data Collection Jobs	131
How Data Retention Settings Affect Web GUI Data	131
About Historical Data Retention	132
Performance and System Health Data Retention	133
Specify Data Retention By Database Table	134
Specify Client Data Retrieval and Retention	135
Enable Data Deduplication	135
Control Report Storage and Retention	136
Specify Inventory Collection After Receiving Events	136
Control Configuration Deployment Behavior	137
Archive Device Configurations Before Template Deployment	137
Roll Back Device Configurations on Template Deployment Failure	137
Specify When and How to Archive WLC Configurations	137
Alarm, Event, and Syslog Purging	139
Log Purging	139
Report Purging	139
Backup Purging	140
Device Configuration File Purging	140
Software Image File Purging	140
Control System Jobs	140
Schedule Data Collection Jobs	140
Resume Data Collection Jobs	141
Run Data Collection Jobs Immediately	141
About System Jobs	141
Migrate Data from Cisco Prime LMS to Cisco Prime Infrastructure	150

CHAPTER 7**User Permissions and Device Access 153**

- User Interfaces, User Types, and How To Transition Between Them **153**
 - User Interfaces and User Types **153**
 - How to Transition Between the CLI User Interfaces in **155**
 - Transition Between the admin CLI and config CLI **155**
 - Log In and Out as the Linux CLI root User **155**
- Enable and Disable root Access for the Linux CLI and the Web GUI **156**
 - Disable and Enable the Linux CLI Users in **156**
 - Disable and Enable the Web GUI root User **157**
- Control the Tasks Users Can Perform (User Groups) **157**
 - Types of User Groups **157**
 - User Groups—Web UI **158**
 - User Groups—NBI **158**
 - View and Change the Tasks a User Can Perform **159**
 - View and Change the Groups a User Belongs To **160**
 - View User Groups and Their Members **160**
 - User Group Permissions and Task Description **160**
 - Create a Customized User Group **178**
 - Add User with Wireless Persona **179**
 - View and Change the Tasks a Group Can Perform **180**
 - Use User Groups with RADIUS and TACACS+ **181**
 - Export the User Group and Role Attributes for RADIUS and TACACS+ **181**
- Add Users and Manage User Accounts **182**
 - Change User Group Memberships **182**
 - Create Web GUI Users with Administrator Privileges **183**
 - Add and Delete Users **183**
 - Disable (Lock) a User Account **184**
 - Change a User's Password **184**
- Configure Guest Account Settings **184**
- Use Lobby Ambassadors to Manage Guest User Accounts **185**
 - Manage Guest User Accounts: Workflows **186**
 - Create Lobby Ambassador Accounts **186**
 - Login as a Lobby Ambassador **187**

Create Guest User Accounts as a Lobby Ambassador	187
Schedule Guest User Accounts	187
Print or Email Guest User Details	188
View Lobby Ambassador Activities	188
Save Guest Accounts on a Device	189
Edit Guest User Credentials	189
Find Out Which Users Are Currently Logged In	189
View the Tasks Performed By Users (Audit Trail)	190
Configure Job Approvers and Approve Jobs	190
Configure Job Notification Mail for User Jobs	191
Configure Global Password Policies for Local Authentication	191
Configure the Global Timeout for Idle Users	191
Disable Idle User Timeout	192
Set Up the Maximum Sessions per User	192
Create Virtual Domains to Control User Access to Devices	193
What Are Virtual Domains?	193
How Virtual Domains Affect Features	194
Reports and Virtual Domains	194
Search and Virtual Domains	194
Alarms and Virtual Domains	194
Maps and Virtual Domains	194
Configuration Templates and Virtual Domains	195
Config Groups and Virtual Domains	195
Email Notifications and Virtual Domains	195
Create New Virtual Domains	195
Create Virtual Domains Directly Under ROOT-DOMAIN	195
Create Child Virtual Domains (Subdomains)	196
Import a List of Virtual Domains	197
Add Network Devices to Virtual Domains	197
Add Groups to Virtual Domains	198
Assign Virtual Domains to Users	198
Edit a Virtual Domain	199
Delete a Virtual Domain	199
Use Virtual Domains with RADIUS and TACACS+	200

Export the Virtual Domain Attributes for RADIUS and TACACS+	200
Configure Local Authentication	201
Use SSO With Local Authentication	201
Configure External Authentication	201
Integrate with an LDAP Server	202
Use RADIUS or TACACS+ for External Authentication	202
Add a RADIUS or TACACS+ Server to	202
Configure RADIUS or TACACS+ Mode on the Server	202
Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes	203
Renew AAA Settings After Installing a New Prime Infrastructure Version	203
Use Cisco ISE With RADIUS or TACACS+ for External Authentication	203
Supported Versions of Cisco ISE in	204
Add as a Client in Cisco ISE	204
Create a User Group in Cisco ISE	205
Create a User and Add the User to a User Group in Cisco ISE	205
Create an Authorization Profile for RADIUS in Cisco ISE	205
Create an Authorization Profile for TACACS+ in Cisco ISE	206
Configure an Authorization Policy in Cisco ISE	207
Configure an Authorization Policy for TACACS in Cisco ISE	208
Create an Authentication Policy in Cisco ISE	208
Use Cisco ACS With RADIUS or TACACS+ for External Authentication	208
Supported Versions of Cisco ACS in	209
Add as a Client in Cisco ACS	210
Create a User Group in Cisco ACS	210
Create a User and Add the User to a User Group in Cisco ACS	210
Create an Authorization Profile for RADIUS in Cisco ACS	210
Create an Authorization Profile for TACACS+ in Cisco ACS	211
Create an Access Service for in Cisco ACS	212
Create an Authorization Policy Rule in Cisco ACS	213
Configure a Service Selection Policy in Cisco ACS	213
Use SSO with External Authentication	214
Add the SSO Server	214
Configure SSO Mode on the Prime Infrastructure Server	214

CHAPTER 8**Fault Management Administration Tasks 215**

- Event Receiving, Forwarding, and Notifications 215
 - User Roles and Access Permissions for Configuring Alarm Notification Settings 216
 - Points to Remember While Adding a New Notification Policy 216
 - Configure Alarms Notification Destination 219
 - Customize Alarm Notification Policies 220
 - Convert Old Email and Trap Notification Data to New Alarm Notification Policy 221
- Specify Alarm Clean Up, Display and Email Options 222
- Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms 224
- Change Severity Levels 224
- Customize the Troubleshooting Text for an Alarm 225
- Change Alarm Auto-Clear Intervals 225
- Change the Information Displayed in the Failure Source for Alarms 226
- Change the Behavior of Expedited Events 226
- Customize Generic Events That Are Displayed in the Web GUI 226
 - Disable and Enable Generic Trap and Syslog Handling 227
 - Disable and Enable Generic Trap Processing 227
 - Disable and Enable Generic Syslog Processing 227
 - Customize Generic Events Based on SNMP Traps 227
- Troubleshoot Fault Processing Errors 228
- Get Help from the Cisco Support Community and Technical Assistance Center (TAC) 229
 - Open a Cisco Support Case 229
 - Join the Cisco Support Community 230

CHAPTER 9**Audits and Logs 231**

- Audit Configuration Archive and Software Management Changes () 231
- Audit Changes Made By Users (Change Audit) 231
 - Generate a Change Audit Report 231
 - Enable Change Audit Notifications and Configure Syslog Receivers 232
 - View Change Audit Details 233
- Audit Actions Executed from the GUI (System Audit) 233
- System Logs 234
 - View and Manage General System Logs 234

View the Logs for a Specific Job	234
Adjust General Log File Settings and Default Sizes	234
Download and E-Mail Log Files for Troubleshooting Purposes	235
Forward System Audit Logs As Syslogs	241
Enable SNMP Traces and Adjust SNMP Log Settings (Levels, Size)	241

CHAPTER 10**Configure Controller and AP Settings 243**

Configure Protocols for CLI Sessions	243
Enable Unified AP Ping Reachability Settings on the Prime Infrastructure	243
Refresh Controllers After an Upgrade	245
Track Switch Ports to Rogue APs	245
Configure Switch Port Tracing	246
Configuring SNMP credentials	247
View the switch port trace details	248
Establish Switch Port Tracing	249
Configure SNMP Credentials for Rogue AP Tracing	249
Switch Port Tracing Details	249
Switch Port Tracing Troubleshooting	250
Frequently Asked Questions on Rogues and Switch Port Tracing	250
How Do You Configure Auto SPT?	251
How Does Auto SPT Differ From Manual SPT?	251
Where Can I See SPT Results (Manual and Auto)?	252
Why Does Auto SPT Take Longer to Find Wired Rogues?	252
How Can I Detect Wired Rogues on Trunk Ports?	253
How Do You Configure Switch Port Location?	253
How Can I Use the Auto SPT “Eliminate By Location” Feature?	254
What is the Difference Between “Major Polling” and “Minor Polling”?	254

CHAPTER 11**Configure High Availability 257**

How High Availability Works	257
About the Primary and Secondary Servers	259
Sources of Failure	259
File and Database Synchronization	259
HA Server Communications	260

Health Monitor Process	260
Health Monitor Web Page	261
Using Virtual IP Addressing With HA	262
How to Use SSL Certificates in an HA Environment?	263
Import Client Certificates Into Web Browsers	264
Hot Standby Behavior	264
Planning HA Deployments	264
Network Throughput Restrictions on HA	265
Using the Local Model	266
Using the Campus Model	267
Using the Remote Model	267
What If I Cannot Use Virtual IP Addressing?	268
Automatic Versus Manual Failover	268
Enable HA for Operations Center	269
Set Up High Availability	271
Before You Begin Setting Up High Availability	272
How to Install the HA Secondary Server	273
How to Register HA on the Primary Server	273
Check Readiness for HA Registration/Configuration	275
Check High Availability Status	277
What Happens During HA Registration	277
How to Patch HA Servers	278
How to Patch New HA Servers	278
How to Patch Paired HA Servers Set for Manual Failover	279
How to Patch Paired HA Servers Set for Automatic Failover	281
Monitor High Availability	283
Access the Health Monitor Web Page	284
How to Trigger Failover	284
How to Trigger Failback	285
Force Failover	285
Respond to Other HA Events	286
HA Registration Fails	286
Network is Down (Automatic Failover)	287
Network is Down (Manual Failover)	288

Process Restart Fails (Automatic Failover)	289
Process Restart Fails (Manual Failover)	290
Primary Server Restarts During Sync (Manual Failover)	291
Secondary Server Restarts During Sync	291
Both HA Servers Are Down	292
Both HA Servers Are Powered Down	292
Both HA Servers Are Down and the Secondary Will Not Restart	293
How to Replace the Primary Server	294
How to Recover From Split-Brain Scenario	295
How to Resolve Database Synchronization Issues	295
High Availability Reference Information	295
HA Configuration Mode Reference	296
HA State Reference	296
HA State Transition Reference	297
High Availability CLI Command Reference	299
Reset the HA Authentication Key	299
Remove HA Via the GUI	299
Remove HA Via the CLI	300
Remove HA During Restore	300
Remove HA During Upgrade	301
Using HA Error Logging	301
Reset the HA Server IP Address or Host Name	302
Configure MSE High Availability	302
Overview of the MSE High Availability Architecture	302
MSE High Availability Pairing Matrix	303
Guidelines and Limitations for MSE High Availability	303
Failover Scenario for MSE High Availability	304
Failback Scenario for MSE High Availability	304
Licensing Requirements for MSE High Availability	304
Set Up MSE High Availability: Workflow	304
Prepare the MSEs for High Availability	305
Configure MSE High Availability on Primary MSEs	305
Configure MSE High Availability on Secondary MSEs	313
Replace Primary MSEs	319

CHAPTER 12	Configure Wireless Redundancy	321
	About Wireless Controller Redundancy	321
	Prerequisites and Limitations for Redundancy	321
	Configure Redundancy Interfaces	322
	Configure Redundancy on Primary Controllers	322
	Configure Redundancy on Secondary Controllers	323
	Monitor Redundancy States	324
	Configure Peer Service Port IPs and Subnet Mask	324
	Add Peer Network Routes	325
	Reset and Upload Files from the Secondary Server	325
	Disable Redundancy on Controllers	326
<hr/>		
CHAPTER 13	Manage Traffic Metrics	327
	How to Manage Traffic Metrics	327
	Prerequisites for Traffic Metrics With Mediatrace	327
	Configure to Use NAM Devices as Data Sources	328
	Configure to Use Routers and Switches as Data Sources	328
	Configure Mediatrace on Routers and Switches	329
	Configure WSMA and HTTP(S) Features on Routers and Switches	329
<hr/>		
CHAPTER 14	Plan Network Capacity Changes	331
	How to Plan the Network Capacity Changes	331
<hr/>		
APPENDIX A	Best Practices: Server Security Hardening	335
	Disable Insecure Services	335
	Disable Root Access	335
	Use SNMPv3 Instead of SNMPv2	336
	Use SNMPv3 to Add Devices	336
	Use SNMPv3 to Import Devices	337
	Use SNMPv3 to Run Discovery	337
	Authenticate With External AAA	338
	Set Up External AAA Via GUI	338
	Set Up External AAA Via CLI	338

Enable NTP Update Authentication 339

Enable OCSP Settings on the Prime Infrastructure Server 340

Set Up Local Password Policies 340

Disable Individual TCP/UDP Ports 341

Check On Server Security Status 342

APPENDIX B

Internal SNMP Trap Generation 343

About Internal Trap Generation 343

Prime Infrastructure SNMP Trap Types 344

Generic SNMP Trap Format 346

Northbound SNMP Trap-to-Alarm Mappings 347

Prime Infrastructure SNMP Trap Reference 350

Configure Prime Infrastructure Traps 355

 Configure Notifications 356

 Port Used To Send Traps 357

 Configure Email Notifications for SNMP Traps 357

 Configure Email Server Settings 357

 View Events and Alarms for SNMP Traps 358

 Filter Events and Alarms for SNMP Traps 358

 Filter for SNMP Traps Using Quick Filters 358

 Filter for SNMP Traps Using Advanced Filters 358

 Purge Alarms for SNMP Traps 359

 How to Troubleshoot Prime Infrastructure SNMP Traps 360

APPENDIX C

Configure High Availability for Plug and Play Gateway 361

How Cisco Plug and Play Gateway HA Works 361

Cisco Plug and Play Gateway HA Prerequisites 361

Set up Standalone Cisco Plug and Play Gateway for Prime Infrastructure HA 362

 in HA with Virtual IP Address 362

 in HA with Different IP Address 362

Cisco Standalone Plug and Play Gateway Server HA Setup 363

Cisco Plug and Play Gateway Status 364

Remove Cisco Plug and Play Gateway in HA 365

Cisco Plug and Play Gateway HA and Combinations 366

Limitations of Cisco Plug and Play Gateway HA 366



CHAPTER 1

Set Up the Prime Infrastructure Server

This section contains the following topics:

- [Server Setup Tasks, on page 1](#)
- [User Management Setup Tasks, on page 2](#)
- [Fault Management Setup Tasks, on page 3](#)
- [Administrator Setup Tasks, on page 4](#)

Server Setup Tasks

Task	See
Verify the backup settings	Set Up Automatic Application Backups, on page 54
Install any required product licenses and software updates	
Modify the stored Cisco.com credentials (user name and password) used to log on to Cisco.com and: <ul style="list-style-type: none">• Check for product updates• Check for device software image updates• Open or review Cisco support cases	Configure Stored Cisco.com Credentials, on page 81
For software updates: <ul style="list-style-type: none">• Enable notifications for product software updates (critical fixes, device support, add-ons)• Specify whether you want credentials stored on Cisco.com when checks for software updates, and if yes, whether you want the user to be prompted for credentials when checking for updates	Enable or Disable Notifications About Software Updates, on page 41
Set up HTTPS on the server for secure interactions between the server and browser-based GUI client (you can use HTTP but HTTPS is recommended)	Secure the Connectivity of the Server, on page 70

Task	See
Configure high availability	
Adjust data retention and purging	
For server-related traps that signal system problems, customize the threshold settings and severities, and forward the traps as SNMP trap notifications to configured receivers	Customize Server Internal SNMP Traps and Forward the Traps, on page 91
Set up NTP (Network Time Protocol) so that time is synchronized between the server and network devices	Set Up NTP on the Server, on page 78
Configure FTP/TFTP on the server for file transfers between the server and network devices	Enable FTP/TFTP/SFTP Service on the Server, on page 80
Configure a proxy for the server	Set Up the Proxy Server , on page 79
Configure the email server	Set Up the SMTP E-Mail Server, on page 80
Set global SNMP polling parameters for managed network elements	Configure Global SNMP Settings for Communication with Network Elements, on page 82
Enable the Compliance feature if you plan to use it to identify device configuration deviations	
Configure product feedback to help Cisco improve its products	Set Up Defaults for Cisco Support Requests, on page 92
Configure product feedback to help Cisco improve its products	Configure Cisco Product Feedback Settings, on page 92

User Management Setup Tasks

Task	See
Create web GUI users that have administration privileges, and disable the web GUI root account	Create Web GUI Users with Administrator Privileges, on page 183 Disable and Enable the Web GUI root User, on page 157
Set up user audits	Audit Configuration Archive and Software Management Changes () , on page 231
Set up user authentication and authorization	Configure External Authentication, on page 201 Configure Local Authentication, on page 201
Create user accounts and user groups	Control the Tasks Users Can Perform (User Groups), on page 157

Task	See
Adjust user security settings (password rules for local authentication, idle time logout setting)	Configure Global Password Policies for Local Authentication, on page 191 Configure the Global Timeout for Idle Users, on page 191
Specify which users can approve jobs	Configure Job Approvers and Approve Jobs, on page 190
Create virtual domains to control device access	Create Virtual Domains to Control User Access to Devices, on page 193
Create a message that is displayed when users log in to the GUI client	Create a Login Banner (Login Disclaimer), on page 81

Fault Management Setup Tasks

Task	See
Forward alarms and events to other receivers in e-mail format	
Forward alarms and events to other receivers in SNMP trap format	
Configure global settings for alarm and event displays and searches: <ul style="list-style-type: none"> • Hide acknowledged, assigned, and cleared alarms in the Alarms and Events tables • Include acknowledged and assigned alarms in search results • Include device names in alarm messages 	Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms, on page 224
Customize the severity for specific events	Change Severity Levels, on page 224
Customize the troubleshooting text that is associated with an alarm	Customize the Troubleshooting Text for an Alarm, on page 225
Customize the auto-clear interval for specific alarms	Change Alarm Auto-Clear Intervals, on page 225
Make the text in the alarm Failure Source field more user-friendly	Change Severity Levels, on page 224
Control generic event handling	Disable and Enable Generic Trap Processing, on page 227
Control if and how users can create Cisco Support Requests	Set Up Defaults for Cisco Support Requests, on page 92

Administrator Setup Tasks

Set Up Operations Center

Operations Center is a licensed feature that allows you to manage multiple instances of from a single instance. Before you can use Operations Center, you must first:

1. Activate your Operations Center license on the server that will host Operations Center. Applying the license will automatically enable Operations Center as the SSO server for the cluster of instances it manages.



Note You can also activate your operation center license on the Prime Infrastructure server that will host Operations Center using smart licensing feature. Applying the smart license will also automatically enable Operations Center as the SSO server for the cluster of Prime Infrastructure instances it manages. To know more on Smart Licensing, see [Smart Licensing, on page 32](#).

2. Add to Operations Center the instances you want to manage. You can configure each instance as an SSO client as it is added to Operations Center
3. (Optional) Disable the personal and global idle-user timeouts for Operations Center and all of its managed instances.
4. (Optional) Configure remote AAA using TACACS+ or RADIUS servers for Operations Center and all of its managed instances,

The Related Topics explain how to complete each of these tasks.

Related Topics

[Add Instances to Operations Center, on page 6](#)

[Disable Idle User Timeouts for Operations Center, on page 6](#)

Activate Your Operations Center License

Before setting up Operations Center:

- Verify that the DNS entry for the server that will host the Operations Center matches the host name configured on that server. For example: Running the commands **nslookup ipaddress** and **hostname** on the server that will host the Operations Center should yield the same output.
- Ensure that all users who will access network information using Operations Center have both NBI Read and NBI Write access privileges. You can do this by editing these users' profiles to make them members of the "NBI Read" and "NBI Write" User Groups (see "Change User Group Memberships" in Related Topics).
- By default, five is the maximum SSO login sessions for one Operations Center user. This is also applicable for instances. Hence, ensure that the number of Active SSO Sessions does not exceed five, or else the managed instances will go into an "unreachable" state.
- If you plan to use remote AAA with Operations Center: Set up a RADIUS or TACACS+ AAA server before you begin (see "Enable AAA for Operations Center" in Related Topics)

Operations Center does not require a separate installation. Instead, you can select or install the server that you want to use to manage other instances, and then activate an Operations Center license on that server.

When activating the license, Operations Center automatically configures itself as the SSO server.

The number of instances you can manage using Operations Center depends on the license you have purchased. For details, see the [Cisco Prime Infrastructure Ordering and Licensing Guide](#).

-
- Step 1** Select **Administration > Licenses and Software Updates > Licenses > Files > License Files**. The License Files page displays.
- Step 2** Click **Add**. The **Add a License File** dialog box displays.
- Step 3** Click **Choose File**.
- Step 4** Navigate to your license file, select it, then click **Open**.
- Step 5** Click **OK**. will confirm that the Operations Center license has been added.
- Step 6** If you are notified that SSO is not set up:
- Click **Yes**, to configure this new Operations Center as an SSO server automatically.
 - Click **No** to configure SSO with DNS Name. Seamless SSO will Add SSO server with DNS Name.
- Step 7** When prompted to log out: Click **OK**. The newly active license should now be listed in the **Licenses > License Files** page.
- Step 8** Log out of and then log back in. The login page that appears should display “Cisco Prime Infrastructure Operations Center [SSO]”, which indicates the license has been applied.
-

Related Topics

- [Set Up Operations Center](#), on page 4
- [Enable AAA for Operations Center](#), on page 7
- [Change User Group Memberships](#), on page 182

Enable Smart Software Licenses for Operations Center

- Step 1** If this is the first time you are choosing Smart licenses:
- Choose **Administration > Licenses and Software Updates > Licenses**.
After a few moments, Prime Infrastructure displays a dialog box informing you that you cannot access the page because you are not using traditional licensing. This is normal.
 - In the dialog box, click **Smart License Settings**.
 - Click the **Licensing Settings** tab.
- Step 2** If you are already using Smart Licensing:
- Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.
 - Click the **Licensing Settings** tab.
- Step 3** Click **Smart Software Licensing** radio button.
- Step 4** Choose Prime Infrastructure Operation Center from the **Product Name** drop-down list and click **Enable Smart Software Licensing**.

Note To enable Operation Center SSO, click **Yes** in the **If you want to add SSO for the same server with IP/DNS** dialog box.

Step 5 Select the licenses in the Available Licenses dialog box, then click **Save**.

Add Instances to Operations Center

Once you have activated your Operations Center license, you must add to Operations Center each of the server instances you want to manage using Operations Center.

Note that each server instance you plan to manage using Operations Center must be enabled as an SSO client of the Operations Center server. You can do this in advance, by adding Operations Center as the SSO server for the managed instance (see “Add SSO Servers” in Related Topics). You can also have Operations Center do this for you when you add the server to Operations Center (you must know the password for the “root” user on the server instance).

Step 1 Log in to **Prime Infrastructure Operations Center**.

Step 2 Select **Monitor > Manage and Monitor Servers**.

Step 3 Click **Add**.

Step 4 Enter the IP address/FQDN of the server instance that you want to manage using Operations Center. You may also enter an alias or host name for the server.

The port number 443 is preset for HTTPS communications between Operations Center and its managed instances. Do not change this value unless you have configured HTTPS for a different port.

Step 5 Click **OK**.

If the server instance you are adding is already configured to use Operations Center as its SSO server, it is added as a managed server instance.

If the server instance is not configured as an SSO client:

- a) Select **Enable Single-Sign-On Automatically**. Operations Center prompts you for a **Username** and **Password**.
- b) Enter the user name and password for the “root” user on the server instance you want to add.

Note When you login as an SSO authenticated user and want to run an API query, make sure that you login as a local user in that particular instance, because SSO does not support basic authentication required by the API.

- c) Click **OK** again.

Step 6 Repeat these steps to add more servers, up to the license limit.

Related Topics

[Set Up Operations Center](#), on page 4

[Add the SSO Server](#), on page 214

Disable Idle User Timeouts for Operations Center

By default, automatically signs out all users whose sessions stay idle for too long. This feature is enabled by default to preserve network bandwidth and processing cycles for active use.

This feature can be annoying for Operations Center users, who will typically have sessions opened not only with Operations Center, but with one or more of the instances of that Operations Center is managing. Idleness in one of these sessions can force a global idle-user timeout for all the sessions, resulting in a sudden logout without warning.

To avoid this inconvenience, administrators must:

1. Disable the global idle user timeout feature, as explained in *Adjust Your GUI Idle Timeout and Other Settings* section in [Cisco Prime Infrastructure User Guide](#). Note that the administrator must disable this feature *separately*, on *each* of the managed instances that Operations Center manages.
2. Instruct Operations Center users to disable the user-specific idle-user timeout feature for the managed instances they access, as explained in *Change Your Idle User Timeout* section in [Cisco Prime Infrastructure User Guide](#). Note that each user must disable this feature *separately*, on *each* of the managed instances they access.

Related Topics

[Set Up Operations Center](#), on page 4

Enable AAA for Operations Center

Operations Center supports local authentication as well as remote AAA using TACACS+ and RADIUS servers. Using remote AAA is optional, but if you want to use it, follow this workflow:

1. Complete the setup for TACACS+ or RADIUS in the remote server. See [Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 208](#) or [Use Cisco ISE With RADIUS or TACACS+ for External Authentication, on page 203](#)
2. Log in to Operations Center server and navigate to **Administration > Users > Users, Roles & AAA**
3. Add a TACACS+ or RADIUS server to Operations Center.
4. Click on **SSO Server Settings**. Depending on the remote server authentication, select TACACS+ or RADIUS under **SSO Server AAA mode**.
5. Click on **Enable Fall-back to Local** check box and select "On Authentication Failure or No Response from Server" from the drop-down list. Remember that the shared secret configured on the AAA server must match the shared secret.



Note Make sure you do not change the AAA setting under **Administration > Users > Users, Roles & AAA > AAA Mode Setting**. It should be in SSO mode only.

6. Perform steps to manage instance in Prime Infrastructure servers.



Note Prime Infrastructure Manage Instance will only fall back to TACACS+ or RADIUS if SSO server is unreachable or not responding.

What to do Next

When you have completed the setup tasks, you are ready to use Operations Center.

You can enable the Operations Center instance for High Availability (HA). HA uses a pair of linked, synchronized Prime Infrastructure servers, to minimize or eliminate the impact of application or hardware failures that may take place on either server. For details, see “Enable HA for Operations Center” in Related Topics

Related Topics

[Set Up Operations Center](#), on page 4

[Enable HA for Operations Center](#), on page 269

Required Software Versions and Configurations

To work with , your devices must run at least the minimum required software versions shown in the list of supported devices. You can access this list using the user interface: Choose **Help > Supported Devices**.

You must also configure your devices to support SNMP traps and syslogs, and the Network Time Protocol (NTP), as explained in the related topics.

Related Topics

[Configure SNMP](#), on page 8

[Configure NTP](#), on page 9

Configure SNMP

To ensure that can query SNMP devices and receive traps and notifications from them, you must:

- Set SNMP credentials (community strings) on each device you want to manage using.
- Configure these same devices to send SNMP notifications to the server.

Use the following Cisco IOS configuration commands to set read/write and read-only community strings on an SNMP device:

- `admin(config)# snmp-server community private RW`
- `admin(config)# snmp-server community public RW`

where:

- *private* and *public* are the community strings you want to set.

After you set the community strings, you can specify that device notifications be sent as traps to the server using the following Cisco IOS global configuration command on each SNMP device:

```
admin(config)# snmp-server host Host traps version community notification-type
```

where:

- *Host* is the IP address of the server.
- *version* is the version of SNMP that is used to send the traps.
- *community* is the community string sent to the server with the notification operation.
- *notification-type* is the type of trap to send.

You may need to control bandwidth usage and the amount of trap information being sent to the server using additional commands.

For more information on configuring SNMP, see:

- The [snmp-server community](#) and [snmp-server host commands](#) in the Cisco IOS Network Management Command Reference.
- The [Configuring SNMP Support](#) section and the [list of notification-type values](#) in the Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2.

If you are planning on implementing IPsec tunneling between your devices and the server, be advised that you will not receive syslogs transmitted from those devices to the server after implementing IPsec tunneling because IPsec does not support free-form syslogs. However, IPsec does support SNMP traps. To continue getting SNMP notifications of any kind from these devices, you need to configure your devices to send SNMP traps to the server.

Configure NTP

Network Time Protocol (NTP) must be properly synchronized on all devices in your network as well as on the server. This includes all -related servers: any remote FTP servers that you use for backups, secondary high-availability servers, the Plug and Play Gateway, VMware vCenter and the ESX virtual machine, and so on.

You specify the default and secondary NTP servers during server installation. You can also use **ntp server** command to add to or change the list of NTP servers after installation. For details, see [How to Connect Via CLI, on page 111](#) and the section on the **ntp server** command in the [Command Reference Guide](#). Note that cannot be configured as an NTP server; it acts as an NTP client only.

Failure to manage NTP synchronization across your network can result in anomalous results in . Management of network time accuracy is an extensive subject that involves the organization's network architecture, and is outside the scope of this Guide. For more information on this topic, see (for example) the Cisco White Paper [Network Time Protocol: Best Practices](#).

Configure Data Sources for With Assurance

If you are licensing the Assurance features, you must complete pre-installation tasks so that Assurance can monitor your network interfaces and services. See Supported Assurance Data Sources for information about these tasks.

Supported Assurance Data Sources

with Assurance needs to collect data from your network devices using the exported data sources shown in [Table 1: Assurance: Supported Data Sources, Devices and Software Versions](#). For each source, the table shows the devices that support this form of export, and the minimum version of Cisco IOS or other software that must be running on the device to export the data.

Use [Table 1: Assurance: Supported Data Sources, Devices and Software Versions](#) to verify that your network devices and their software are compatible with the type of data sources uses. If needed, upgrade your hardware or software. Note that each software version given is a *minimum*. Your devices can run any later version of the same software or Cisco IOS release train.

You may also need to make changes to ensure that can collect data using SNMP, as explained in [Configure SNMP](#).

Configure Assurance Data Sources

Before installing e, you should enable the supported devices shown in the below table to provide with fault, application, and performance data, and ensure that time and date information are consistent across your network. The following table provide guidelines on how to do this.

Table 1: Assurance: Supported Data Sources, Devices and Software Versions

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
Catalyst 3750-X / 3560-X	15.0(1)SE IP base or IP services feature set and equipped with the network services module.	TCP and UDP traffic	See the <i>Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches</i> section in the Cisco Prime Infrastructure User Guide .
Catalyst 3850	15.0(1)EX	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, See the <i>Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches</i> section in the Cisco Prime Infrastructure User Guide . To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon
Catalyst 4500	15.0(1)XO and 15.0(2)	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, See the <i>Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches</i> section in the Cisco Prime Infrastructure User Guide . To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon
Catalyst 6500	SG15.1(1)SY	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, See the <i>Configure NetFlow on Catalyst 3000, 4000, and 6000 Family of Switches</i> section in the Cisco Prime Infrastructure User Guide . To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon

Device Type	Cisco IOS Releases That Support NetFlow	Supported NetFlow Export Types	NetFlow Configuration
ISR	15.1(3) T	TCP and UDP traffic, Voice & Video	To configure TCP and UDP traffic, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Collecting Traffic Statistics To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon
ISR G2	15.2(1) T and 15.1(4)M	TCP and UDP traffic, application response time, Voice & Video	To configure TCP, UDP, and ART, see the <i>Configure NetFlow on ISR Devices</i> section in Cisco Prime Infrastructure User Guide . To configure Voice & Video, use this CLI template: Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Medianet - PerfMon
ISR G2	15.2(4) M2 or later, 15.3(1)T or later	TCP and UDP traffic, application response time, Voice and Video	To configure TCP, UDP, and ART, see the <i>Improve Application Performance With Application Visibility and Control</i> chapter in the Cisco Prime Infrastructure User Guide .
ASR	15.3(1)S1 or later	TCP and UDP traffic, application response time,	
ISR G3	15.3(2)S or later	Voice & Video, HTTP URL visibility	

Enable Medianet NetFlow

To ensure that Cisco can make use of Medianet data, your network devices must:

- Enable Medianet NetFlow data export for the basic set of statistics supported in .
- Export the Medianet NetFlow data to the server and port.

Use a configuration like the following example to ensure that gets the Medianet data it needs:

- flow record type performance-monitor PerfMonRecord
- match ipv4 protocol
- match ipv4 source address
- match ipv4 destination address
- match transport source-port
- match transport destination-port

- collect application media bytes counter
- collect application media bytes rate
- collect application media packets counter
- collect application media packets rate
- collect application media event
- collect interface input
- collect counter bytes
- collect counter packets
- collect routing forwarding-status
- collect transport packets expected counter
- collect transport packets lost counter
- collect transport packets lost rate
- collect transport round-trip-time
- collect transport event packet-loss counter
- collect transport rtp jitter mean
- collect transport rtp jitter minimum
- collect transport rtp jitter maximum
- collect timestamp interval
- collect ipv4 dscp
- collect ipv4 ttl
- collect ipv4 source mask
- collect ipv4 destination mask
- collect monitor event
- flow monitor type performance-monitor PerfMon
- record PerfMonRecord
- exporter PerfMonExporter
- flow exporter PerfMonExporter
- destination PrInIP
- source Loopback0
- transport udp PiInPort
- transport udp PiInPort
- class class-default

- ! Enter flow monitor configuration mode.
- flow monitor PerfMon
- ! Enter RTP monitor metric configuration mode.
- monitor metric rtp
- ! Specifies the minimum number of sequential packets required to identify a stream as being an RTP flow
- min-sequential 2
- ! Specifies the maximum number of dropouts allowed when sampling RTP video-monitoring metrics.
- max-dropout 2
- max-reorder 4
- ! Enter IP-CBR monitor metric configuration mode
- monitor metric ip-cbr
- ! Rate for monitoring the metrics (1 packet per sec)
- rate layer3 packet 1
- interface interfacename
- service-policy type performance-monitor input PerfMonPolicy
- service-policy type performance-monitor output PerfMonPolicy

In this example configuration:

- *PrInIP* is the IP address of the server.
- *PiInPort* is the UDP port on which the server is listening for Medianet data (the default is 9991).
- *interfacename* is the name of the interface (such as GigabitEthernet0/0 or fastethernet 0/1) sending Medianet NetFlow data to the specified *PrInIP*.

For more information on Medianet configuration, see the [Medianet Reference Guide](#).

Enable NetFlow and Flexible NetFlow

To ensure that can make use of NetFlow data, your network devices must:

- Have NetFlow enabled on the interfaces that you want to monitor.
- Export the NetFlow data to the server and port.

As of version 2.1, supports Flexible NetFlow versions 5 and 9. Note that you must enable NetFlow on each *physical* interface for which you want to collect data. These will normally be Ethernet or WAN interfaces. This applies to physical interfaces only. You do not need to enable NetFlow on VLANs and Tunnels, as they are included automatically whenever you enable NetFlow on a physical interface.

Use the following commands to enable NetFlow on Cisco IOS devices:

- Device(config)# interface interfaceName

- Device(config)# ip route-cache flow where *interfaceName* is the name of the interface (such as fastethernet or fastethernet0/1) on which you want to enable NetFlow.

Once NetFlow is enabled on your devices, you must configure exporters to export NetFlow data to . You can configure an exporter using these commands:

- Device(config)# ip flow-export version 5
- Device(config)# ip flow-export destination PrInIP PiInPort
- Device(config)# ip flow-export source interfaceName where:
 - *PrInIP* is the IP address of the server.
 - *PiInPort* is the UDP port on which the server is listening for NetFlow data. (The default is 9991.)
 - *interfaceName* is the name of the interface sending NetFlow data to the specified *PrInIP* . This will cause the source interface's IP address to be sent to as part of NetFlow export datagrams.

If you configure multiple NetFlow exporters on the same router, make sure that only one of them exports to the server. If you have more than one exporter on the same router exporting to the same destination, you risk data corruption.

Use the following commands to verify that NetFlow is working on a device:

- Device# show ip flow export
- Device# show ip flow export
- Device# show ip cache flow
- Device# show ip cache verbose flow

For more information on NetFlow configuration, see:

- [Cisco IOS Switching Services Configuration Guide, Release 12.2](#)
- [Flexible NetFlow Configuration Guide, Cisco IOS Release 15.1M&T](#)
- [Catalyst 6500/6000 Switches NetFlow Configuration and Troubleshooting](#)

Deploy Network Analysis Modules NAMs

Ensure that your NAMs are placed appropriately in the network. For more information, see:

- Cisco Network Analysis Module Software 5.1 User Guide — Includes deployment scenarios and covers a variety of topics, including deploying NAMs in the branch, and deploying NAMs for WAN optimization.
- Cisco Network Analysis Module Deployment Guide — See the section [Places in the Network Where NAMs Are Deployed](#).

If your NAMs are deployed properly, then no other pre installation work is required. When you conduct discovery using Cisco Prime AM, you will need to enter HTTP access credentials for each of your NAMs.

uses a more efficient REST interface to query NAMs. For this reason, it does not support the direct export of NetFlow data from NAMs. Any device exporting NetFlow data must export that NetFlow data directly to , not via a NAM. Exporting NetFlow data from any NAM to will result in data duplication.

Enable Performance Agent

To ensure that can collect application performance data, use the Cisco IOS **mace** (for Measurement, Aggregation and Correlation Engine) keyword to configure Performance Agent (PA) data flow sources on your branch-office routers.

For example, use the following commands in Cisco IOS global configuration mode to configure a PA flow exporter on a router:

- Router (config)# flow exporter mace-export
- Router (config)# destination 172.30.104.128
- Router (config)# transport udp 9991
- Use commands like the following to configure flow records for applications with flows across the router:
 - Router (config)# flow record type mace mace-record
 - Router (config)# collect application name

Router (config)# collect art all where application name is the name of the application whose flow data you want to collect. To Configure the PA flow Monitor type:

- Router (config)# flow monitor type mace mace-monitor
- Router (config)# record mace-record
- Router (config)# exporter mace-export

To collect traffic of interest, use commands like the following:

- Router (config)# **access-list 100 permit tcp any host 10.0.0.1 eq 80**
- Router (config)# **class-map match-any mace-traffic**
- Router (config)# **match access-group 100**

To configure a PA policy map and forward the PA traffic to the correct monitor:

- Router (config)# policy-map type mace mace_global
- Router (config)# class mace-traffic
- Router (config)# flow monitor mace-monitor

Finally, enable PA on the WAN interface:

- Router (config)# interface Serial0/0/0
- Router (config)# mace enable

For more information on configuring Performance Agent, see the [Cisco Performance Agent Deployment Guide](#).

Install Patches

You may need to install patches to get your version of to the level at which upgrade is supported. You can check the version and patch version you are running by using the CLI commands **show version** and **show application**.

Different patch files are provided for each version of and its predecessor products. Download and install only the patch files that match the version of your existing system and that are required before you upgrade to a later version. You can find the appropriate patches by pointing your browser to the Cisco Download Software navigator .

Before installing a patch, you will need to copy the patch file to your server's default repository. Many users find it easy to do this by first downloading the patch file to a local FTP server, then copying it to the repository. You can also copy the patch file to the default repository using any of the following methods:

- cdrom—Local CD-ROM drive (read only)
- disk—Local hard disk storage
- ftp—URL using an FTP server
- http—URL using an HTTP server (read only)
- https—URL using an HTTPS server (read only)
- nfs—URL using an NFS server
- sftp—URL using an SFTP server
- tftp—URL using a TFTP server

Step 1 Download the appropriate point patch to a local resource in your environment:

- a) With the Cisco Download Software navigator displayed in your browser, choose **Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > .**
- b) Select the version of that most closely matches the one you are currently using.
- c) Click **Prime Infrastructure Patches** to see the list of available patches for that version of the product.
- d) Next to each patch that is required, click **Download**, then follow the prompts to download the file.

Step 2 Open a command-line interface session with the server (see [How to Connect Via CLI, on page 111](#)).

Step 3 Copy the downloaded patch file to the default local repository. For example:

```
admin# copy source path/defaultRepo
```

Where:

- *source* is the downloaded patch file's location and name.
- *path* is the complete path to the default local backup repository, defaultRepo (for example: /localdisk)

Step 4 Install the patch:

```
admin# patch install patchFile Repositoryname
```

Where:

- *patchFile* is the name of the patch file you copied to /localdisk/defaultRepo

- *Repositoryname* is the name of the repository

For example: admin# patch install test.tar.gz defaultRepo



CHAPTER 2

Licenses and Software Updates

This section contains the following topics:

- [Prime Infrastructure Licensing](#) , on page 19
- [Controller Licensing](#), on page 23
- [MSE Licensing](#) , on page 25
- [Assurance Licensing](#) , on page 30
- [Smart Licensing](#), on page 32
- [Manage Software Updates](#), on page 40

Prime Infrastructure Licensing

You purchase licenses to access the Prime Infrastructure features required to manage your network. Each license also controls the number of devices you can manage using those features. The maximum number of license files that can be added to Prime Infrastructure is 25.

The **Administration > Licenses and Software Updates > Licenses** page allows you to manage traditional Cisco Prime Infrastructure, wireless LAN controllers, and Mobility Services Engine (MSE) licenses.

Although Prime Infrastructure and MSE licenses can be fully managed from the **Administration > Licenses and Software Updates > Licenses page**, you can only view Cisco Wireless LAN Controllers (WLC). You must use Cisco WLC or Cisco License Manager (CLM) to manage Cisco WLC licenses.

The **Administration > Licenses and Software Updates > Smart Software** Licensing page allows you to manage smart licenses.

You need a base license and the corresponding feature licenses (such as Assurance licenses) to get full access to the respective Prime Infrastructure features to manage a set number of devices.

If you have installed Prime Infrastructure for the first time you may access the lifecycle and assurance features using the built-in evaluation license that is available by default. The default evaluation license is valid for 60 days for 100 devices. You can send a request to ask-prime-infrastructure@cisco.com if:

- You need to extend the evaluation period
- You need to increase the device count
- You already have a particular feature license and need to evaluate the other feature licenses

You will need to order a base license and then purchase the corresponding feature license before the evaluation license expires. The license that you purchase must be sufficient to:

- Enable access to all the Prime Infrastructure features you want to use to manage your network.

- Include all the devices in your network that you want to manage using Prime Infrastructure.

To ensure you have the licenses to achieve these goals, do the following:

1. Familiarize yourself with the types of license packages available to you, and their requirements.
2. View the existing licenses. See for help on ordering and downloading licenses.
3. Calculate the number of licenses you will need, based both on the package of features you want and the number of devices you need to manage.
4. Add new licenses.
5. Delete existing licenses.



Note As Prime Infrastructure no longer supports the node-locked licensing approach, the UDI information required to generate licenses are limited to a standard syntax as shown below:

- PID = PRIME-NCS-APL (For Physical Appliance)
PID = PRIME-NCS-VAPL (For Virtual Appliance/Virtual Machine)
- SN = ANY:ANY

You must provide the subtleties in the mentioned format to generate new licenses.

For more information, see [Cisco Prime Infrastructure Ordering and Licensing Guide](#).

Related Topics

- [Verify License Details](#) , on page 20
- [Add Licenses](#) , on page 21
- [Delete Licenses](#), on page 21

Purchase Prime Infrastructure Licenses

Prime Infrastructure licenses control the features you can use and the number of devices you can manage using those features. For more information about Prime Infrastructure license types and how to order them, see the [Cisco Prime Infrastructure Ordering and Licensing Guide](#) for the version of Prime Infrastructure that you want to use.

You can ignore warning messages like “Base license is missing” or “Multiple base licenses present, use only one” displayed in the **Administration > Licenses and Software Updates > Licenses > Files > License Files** area.

Verify License Details

Before you order new licenses, you might want to get details about your existing licenses. For example, number of devices managed by your system.

To verify license details, choose **Administration > Licenses and Software Updates > Licenses**.

Related Topics

- [Prime Infrastructure Licensing](#) , on page 19
- [Controller Licensing](#), on page 23
- [MSE Licensing](#) , on page 25

[Assurance Licensing](#) , on page 30

Add Licenses

You need to add new licenses when:

- You have purchased a new Prime Infrastructure license.
- You are already using Prime Infrastructure and have bought additional licenses.

-
- Step 1** Choose **Administration > Licenses and Software Updates > Licenses**.
- Step 2** In the **Summary** folder, click **Files**, then click **License Files**.
- Step 3** Click **Add**.
- Step 4** Browse to the location of the license file, then click **OK**.
-

Related Topics

- [Delete Licenses](#), on page 21
- [Troubleshoot Licenses](#), on page 21
- [MSE License Structure Matrix](#), on page 25
- [Verify Assurance License Details](#), on page 30

Delete Licenses

When you delete licenses from Prime Infrastructure, all licensing information is removed from the server. Make a copy of your original license file in case you want to add it again later. There are several reasons you might want to delete licenses:

- You installed temporary licenses and want to delete them before applying your permanent licenses.
- You want to move your licenses to a different server. You must first delete the licenses from the original server, then send an email to licensing@cisco.com requesting a re-host for your licenses. You can then apply the re-hosted licenses to the new server.

-
- Step 1** Choose **Administration > Licenses and Software Updates > Licenses**.
- Step 2** Click **Files > License Files**.
- Step 3** Select the license file you want to delete, then click **Delete**.
-

Related Topics

- [Add Licenses](#) , on page 21
- [Troubleshoot Licenses](#), on page 21
- [MSE License Structure Matrix](#), on page 25
- [Verify Assurance License Details](#), on page 30

Troubleshoot Licenses

To troubleshoot licenses, you will need to get details about the licenses that are installed on your system. to:

- Get a quick list of the licenses you have: Click **Help > About Prime Infrastructure**.
- Get license details: Choose **Administration > Licenses and Software Updates > Licenses**.

When troubleshooting licenses, it is important to remember that Prime Infrastructure has six types of licenses:

- **Base:** Required for every Prime Infrastructure installation. The requirement stems primarily from the need to do accurate royalty accounting by knowing how many Prime Infrastructure instances have been purchased. A Base license is required for each instance of Prime Infrastructure, and is a prerequisite for all other license types.
- **Lifecycle:** Regulates the total number of devices under Prime Infrastructure management. Lifecycle license is consumed only for admin VDC in Prime Infrastructure. The child VDC does not consume any license. It is either auto-added by admin or added separately.
- **Assurance:** Regulates the total number of NetFlow devices under Prime Infrastructure management.
- **Collector:** Regulates the total number of NetFlow data flows per second that Prime Infrastructure can process.

Lifecycle and Assurance licenses are supplied in either evaluation or permanent form (there is no explicit evaluation version of the Base or Collector licenses):

- **Evaluation:** These licenses permit or extend access to Prime Infrastructure for a pre-set period. You can apply only one evaluation license of each type (that is, only one Lifecycle evaluation license, one Assurance evaluation license, and so on). You cannot apply an evaluation license over a permanent form of the same license.
- **Permanent License:** These permit access to Prime Infrastructure features as specified and are not time-limited. Permanent licenses can be applied over evaluation licenses, and can also be applied incrementally (that is, you can have multiple permanent Assurance licenses, and so on).

Prime Infrastructure also performs the following basic license checks:

- A Lifecycle license is a required prerequisite for Assurance licenses.
- An Assurance license is a required prerequisite for Collector licenses.

Also note that:

- From Release 3.0 Prime Infrastructure enables the user to set threshold limit for generating an alarm for all licenses. To set threshold limit for licenses, see “Configuring Notifications” in Related Topics.
- Prime Infrastructure hides Assurance-related features, menu options and links until an Assurance license is applied. Even if you have purchased an Assurance license, these features remain hidden until you apply it.
- Whenever you apply an Assurance license, you automatically apply a Collector license permitting an instance of Prime Infrastructure to process up to 20,000 NetFlow data flows per second. Collector licenses permitting 80,000 flows per second can be applied only with the Professional or equivalent configurations, due to the hard disk requirements imposed by this data rate.
- You can add Lifecycle and Assurance permanent licenses incrementally. However, you can add only one Collector 80K license, and then only with the Professional or equivalent configuration.

The following table provides some scenarios and tips for troubleshooting.

Table 2: Troubleshooting Scenarios

Scenario	Possible Cause	Resolution
Prime Infrastructure reports a Licensing error.	The license file may be corrupted and unusable. This can occur anyone attempts to modify the license file.	<ol style="list-style-type: none"> 1. Delete the existing license. 2. Download and install a new license.

Scenario	Possible Cause	Resolution
Unable to add new licenses.	Some types of license must be added in the correct order. The Base license is a prerequisite for adding Lifecycle licenses. A Lifecycle license is a prerequisite for adding an Assurance license. An Assurance license is a prerequisite for adding a Collector license (a Collector license is added automatically with the Assurance license).	<ol style="list-style-type: none"> 1. Add the Base license 2. Add Lifecycle licenses 3. Add Assurance licenses 4. Add Datacenter licenses 5. Add Collector licenses
The state of the devices has changed to unmanaged.	The device limit must be less than or equal to lifecycle license limit. The state of the inventoried devices will change to unmanaged if you add or delete devices.	<ol style="list-style-type: none"> 1. Delete the additional devices. 2. The state of the devices will change to managed after the 24 hours synchronization. <p>To verify that the status of the inventoried devices has changed to “managed” after synchronization:</p> <ol style="list-style-type: none"> 1. Choose Monitor > Network Devices. 2. Check the Inventory Collection Status column for the row listing the devices in which you are interested. This will give you a summary of current collection status efforts for those devices. 3. For details about the collection status, hover the mouse cursor over the cross-hair icon in the Inventory Collection Status column.

Related Topics

- [Configure Notifications](#), on page 356
- [Add Licenses](#), on page 21
- [Delete Licenses](#), on page 21
- [MSE License Structure Matrix](#), on page 25
- [Verify Assurance License Details](#), on page 30

Controller Licensing

To view controller licenses, choose **Administration > Licenses and Software Updates > Licenses**, then select **Files > Controller Files** from the left sidebar menu.



Note Prime Infrastructure does not directly manage controller licenses, rather it simply monitors the licenses. To manage the licenses you can use command-line interface (CLI) commands, Web UI, or Cisco License Manager (CLM).

This page displays the following parameters:

- Controller Name
- Controller IP—The IP Address of the controller.
- Feature—License features include wplus-ap-count, wplus, base-ap-count, and base.

For every physical license installed, two license files display in the controller: a feature level license and an ap-count license. For example if you install a “WPlus 500” license on the controller, “wplus” and “wplus-ap-count” features are displayed. There are always two of these features active at any one time that combine to enable the feature level (WPlus or Base) and the AP count.

You can have both a WPlus and a Base license, but only one can be active at any given time.

- AP Limit

AP Limit—The maximum capacity of access points allowed to join this controller.

- EULA status—Displays the status of the End User License Agreement and is either Accepted or Not Accepted.
- Comments

Comments—User entered comments when the license is installed.

- Type

Type—The four different types of licenses are as follows:

- Permanent

Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.

- Evaluation—Licenses are non-node locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node locked, their usage is recorded on the device. The number of days left displays for the evaluation license with the fewest number of remaining active license days.
- Extension—Licenses are node locked and metered. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
- Grace Period—Licenses are node locked and metered. These licenses are issued by Cisco licensing portal as part of the permission ticket to rehost a license. They are installed on the device as part of the rehost operation, and you must accept a EULA as part of the rehost operation.

Types other than Permanent display the number of days left until the license expires. Licenses not currently in use do not have their counts reduced until they become “In Use.”

- Status

- In Use—The license level and the license are in use.
- Inactive—The license level is being used, but this license is not being used.
- Not In Use—The license level is not being used and this license is not currently recognized.
- Expired In Use—The license is being used, but is expired and will not be used upon next reboot.
- Expired Not In Use—The license has expired and can no longer be used.
- Count Consumed—The ap-count license is In Use.

If you need to filter the list of license files, you can enter a controller name, feature, or type and click Go.

MSE Licensing

The MSE packages together multiple product features related to network topology, design such as NMSP, Network Repository along with related Service Engines, and application processes, such as the following:

- Context-Aware Service
- Wireless Intrusion Prevention System(WIPS)

To enable smooth management of MSE and its services, various licenses are offered.

You must have a Cisco Prime Infrastructure license to use MSE and its associated services.

Related Topics

- [MSE License Structure Matrix](#), on page 25
- [Sample MSE License File](#), on page 25
- [Revoke and Reuse an MSE License](#), on page 26
- [MSE Services Coexistence](#), on page 27
- [Manage MSE Licenses](#), on page 27

MSE License Structure Matrix

The following table lists the breakdown of the licenses between the High end, Low end and Evaluation licenses for MSE, Location services, SCM, wIPS, and MIR.

Table 3: MSE License Structure Matrix

	High End	Low End	Evaluation
MSE Platform	High-end appliance and infrastructure platform, such as the Cisco 3350 and 3355 mobility services engines	Low-end appliance and infrastructure platform, such as Cisco 3310 mobility services engine	—
Context Aware Service	25,000 Tags	2000 Tags	Validity 60 days, 100 Tags and 100 Elements
	25,000 Elements	2000 Elements	
wIPS	3000 access points	2000 access points	Validity 60 days, 20 access points

Related Topics

- [Sample MSE License File](#), on page 25
- [Revoke and Reuse an MSE License](#), on page 26
- [MSE Services Coexistence](#), on page 27
- [Manage MSE Licenses](#), on page 27

Sample MSE License File

The following is a sample MSE license file:

```

FEATURE MSE cisco 1.0 permanent uncounted \
VENDOR_STRING=UDI=udi,COUNT=1 \
HOST ID=ANY \
NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</LicLineID> \
<PAK>dummyPak</PAK>" \
SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"

```

This sample file has five license entries. The first word of the first line of any license entry tells you what type of license it is. It can either be a Feature or Increment license. A feature license is a static lone item to license. There can be multiple services engines running in MSE. An Increment license is an additive license. In MSE, the individual service engines are treated as increment licenses.

The second word of the first line defines the specific component to be licensed. For example, MSE, LOCATION_TAG. The third word depicts the vendor of the license, for example Cisco. The fourth word denotes the version of the license, for example 1.0. The fifth word denotes the expiration date; this can be permanent for licenses that never expire or a date in the format dd-mm-yyyy. The last word defines whether this license is counted.

Related Topics

- [MSE License Structure Matrix](#), on page 25
- [Revoke and Reuse an MSE License](#), on page 26
- [MSE Services Coexistence](#), on page 27
- [Manage MSE Licenses](#), on page 27

Revoke and Reuse an MSE License

You can revoke an MSE appliance license from one system and reuse it on another system. When you revoke a license, the license file is deleted from the system. If you want to reuse the license on another system, then the license needs to be rehosted.

If you want to reuse a license with an upgrade stock keeping unit (SKU) on another system, then you must have the corresponding base license SKU installed in the system to which you want to reuse the upgrade SKU. You cannot reuse the upgrade license SKU in a system if the corresponding base license SKU is deleted from it.

When you revoke a license, MSE restarts the individual service engines to reflect the changes to the licenses. Then the service engines receives the updated capacity from MSE during startup.

Related Topics

- [MSE License Structure Matrix](#), on page 25
- [Sample MSE License File](#), on page 25
- [MSE Services Coexistence](#), on page 27
- [Manage MSE Licenses](#), on page 27

MSE Services Coexistence

With MSE 6.0 and later, you can enable multiple services (Context Aware and wIPS) to run concurrently. Before Version 6.0, mobility services engines only supported one active service at a time.

The following must be considered with coexistence of multiple services:

- Coexistence of services might be impacted by license enforcement. As long as the license is not expired, you can enable multiple services.

**Note**

Limits for individual services differ. For example, a low-end mobility services engine (MSE-3310) tracks a total of 2,000 CAS elements; a high-end mobility services engine (MSE-3350) tracks a total of 25,000 CAS elements. A low-end mobility services engine has a maximum limit of 2000 wIPS elements; a high-end mobility services engine has a maximum limit of 3000 wIPS elements.

- Expired evaluation licenses prevent the service from coming up.
- If a CAS license is added or removed, this process restarts all services on the mobility services engine including wIPS. If a wIPS license is added or removed, the process does not impact CAS; only wIPS restarts.
- Other services can be enabled in evaluation mode even if a permanent license for the maximum number of elements has been applied.

Whenever one of the services has been enabled to run with its maximum license, another service cannot be enabled to run concurrently because the capacity of the MSE is not sufficient to support both services concurrently. For example, on MSE-3310, if you install a wIPS license of 2000, then you cannot enable CAS to run concurrently. However, evaluation licenses are not subject to this limitation.

Related Topics

- [MSE License Structure Matrix](#), on page 25
- [Sample MSE License File](#), on page 25
- [Revoke and Reuse an MSE License](#), on page 26
- [Manage MSE Licenses](#), on page 27

Manage MSE Licenses

To view Mobility Services Engine (MSE) licenses, choose **Administration > Licenses and Software Updates > Licenses**, then select **Files > MSE Files** from the left sidebar menu.

The page displays the MSE licenses found and includes the following information:

- MSE License File—Indicates the MSE License.
- MSE—Indicates the MSE name.
- Type—Indicates the type of mobility services engine (client elements, wIPS local mode or wIPS monitor mode access points).
- Limit—Displays the total number of client elements or wIPS monitor mode access points licensed across the mobility services engine.
- License Type—Permanent licenses are the only license types displayed on this page. Permanent licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.

Tag licenses are installed using the AeroScout System Manager only if the tags are tracked using the Partner engine. Otherwise the tags will be counted along with the CAS element license. Because tag licenses are added and managed using appropriate vendor applications, tag licenses are not displayed in this page. For more information, see the AeroScout Support Page in Related Topics. Evaluation (demo) licenses are also not displayed.

For more information, see [AeroScout Support Page](#).

Related Topics

[Register Product Authorization Keys](#), on page 28

[Install Client and wIPS License Files](#), on page 29

[Delete Mobility Services Engine License Files](#), on page 29

Register Product Authorization Keys

You receive a product authorization key (PAK) when you order a client, wIPS, or tag license from Cisco. You must register the PAK to receive the license file for installation on the mobility services engine. License files are emailed to you after successfully registering a PAK.

Client and wIPS PAKs are registered with Cisco.

Tag PAKs are registered with AeroScout. To register your tag PAK, navigate to the AeroScout Support Page given in Related Topics.

To register a product authoritative key (PAK) and obtain a license file for installation, follow these steps:

-
- Step 1** Point your browser to the Cisco Product License Registration Portal (see Related Topics).
You can also access this site by clicking the Product License Registration link located on the License Center page of Prime Infrastructure.
- Step 2** Enter the PAK and click SUBMIT.
- Step 3** Verify the license purchase. Click Continue if correct. The licensee entry page appears.
If the license is incorrect, click the TAC Service Request Tool link to report the problem.
- Step 4** In the Designate Licensee page, enter the mobility service engine UDI in the host ID text box. This is the mobility services engine on which the license will be installed.
UDI information for a mobility services engine is found in the General Properties area at **Services > Mobility Services Engine > Device Name > System**.
- Step 5** Select the Agreement check box. Registrant information appears beneath the check box.
Modify information as necessary.
Ensure that the phone number does not include any characters in the string for the registrant and end user. For example, enter 408 555 1212 rather than 408.555.1212 or 408-555-1212.
- Step 6** If registrant and end user are not the same person, select the License (End-User) check box beneath registrant information and enter the end-user information.
- Step 7** Click Continue.
- Step 8** At the Finish and Submit page, review registrant and end-user data. Click Edit Details to correct information, if necessary, then click Submit. For more information, see [AeroScout Support Page](#) and [Cisco Product License Registration Portal](#).
-

Related Topics

[Install Client and wIPS License Files](#), on page 29

[Delete Mobility Services Engine License Files](#), on page 29

Install Client and wIPS License Files

You can install CAS element licenses and wIPS licenses from Prime Infrastructure.

Tag licenses are installed using the AeroScout System Manager. See the [AeroScout Support Page](#).

To add a client or wIPS license to Prime Infrastructure after registering the PAK, follow these steps

Step 1 Choose **Administration > Licenses and Software Updates > Licenses**.

Step 2 From the left sidebar menu, choose **Files > MSE Files**.

Step 3 Click **Add** to open the **Add a License File** dialog box.

Step 4 From the MSE Name drop-down list, choose the mobility services engine to which you want to add the license file.

Note Verify that the UDI of the selected mobility services engine matches the one you entered when registering the PAK.

Step 5 Enter the license file in the License File text box or browse to the applicable license file.

Step 6 Once displayed in the License File text box, click **Upload**. Newly added license appears in mobility services engine license file list.

Note

- A Context Aware Service (CAS) restarts if a client or tag license is installed; a wIPS service restarts if a wIPS license is installed.
- Services must come up before attempting to add or delete another license.

Related Topics

[Delete Mobility Services Engine License Files](#), on page 29

Delete Mobility Services Engine License Files

Step 1 Choose **Administration > Licenses and Software Updates > Licenses**, then select **Files > MSE Files** from the left sidebar menu.

Step 2 Select the check box of the mobility services engine license file that you want to delete.

Step 3 Click **Delete**, then click **OK** to confirm the deletion.

Related Topics

[Register Product Authorization Keys](#), on page 28

[Install Client and wIPS License Files](#), on page 29

Assurance Licensing

As explained in “Purchasing Prime Infrastructure Licenses” (see Related Topics), licenses for Assurance features are based on the number of NetFlow-monitored devices and Network Analysis Module (NAM) data collection-enabled devices you have in your network. You manage, verify, and troubleshoot Assurance licenses much as you do with other feature licenses, as explained in “Add Licenses”, “Delete Licenses” and “Troubleshoot Licenses”.

In addition to these functions, Prime Infrastructure also lets you choose which NetFlow and NAM devices you want to manage using Assurance features. For example, if you have only 50 Assurance feature licenses and more than 50 NetFlow and NAM devices, you can choose to manage only your most critical devices. If you later purchase additional Assurance licenses, you can add license coverage for the devices previously left unmanaged.

Related Topics

[Purchase Prime Infrastructure Licenses](#), on page 20

[Verify Assurance License Details](#), on page 30

[Add Licenses](#), on page 21

[Delete Licenses](#), on page 21

[Troubleshoot Licenses](#), on page 21

Verify Assurance License Details

Before you buy new Assurance licenses, you may want to get details about your existing Assurance licenses and how they are being used. You can find Assurance license information using the resources in the following table.

Table 4: Finding Assurance License Information

To see	Choose
The NetFlow-enabled devices in your network that are under Assurance management, as a percentage of the total number of Assurance licenses you have.	Administration > Licenses and Software Updates > Licenses > Summary.
The total number of Assurance licenses you have and the files associated with them.	Administration > Licenses and Software Updates > Licenses > Files.
A list of the devices sending NetFlow or NAM polling data to Prime Infrastructure.	Administration > Licenses and Software Updates > Licenses > Assurance Licenses (link is in upper right corner of the page)
The number of Assurance Licenses in use.	
The maximum number of Assurance licenses available to you.	

By default, the total count of Assurance licenses on the Assurance Licenses page and on the Summary and Files > License Files pages is always updated whenever you add or delete Assurance licenses. Addition or removal of devices covered under these added or deleted Assurance licenses takes place as part of a System Defined Job, which runs automatically once every 12 hours. It can take up to 12 hours for the added or deleted devices to appear.

You can always access the **Administration > Licenses and Software Updates > Licenses > Assurance Licenses page** from the **Assurance Licenses** link in the upper right corner of the **Administration > Licenses and Software Updates > Licenses > Summary** and **Administration > Licenses and Software Updates > Licenses > Files** pages.

Related Topics

[Install Client and wIPS License Files](#), on page 29

[Delete Mobility Services Engine License Files](#), on page 29

Add License Coverage For NetFlow and NAM Devices

You want to add license coverage for NetFlow or NAM devices when:

- You have purchased new or additional Assurance licenses.
- You have NetFlow and NAM devices not already licensed for Assurance management.

-
- Step 1** Choose **Administration > Licenses and Software Updates > Licenses > Assurance Licenses** (the **Assurance Licenses** link is in the upper right corner of the page).
- Step 2** Above the list of devices currently under Assurance management, click **Add Device**.
- Step 3** Select the check box next to each device you want to put under Assurance management, then click **Add License**. Prime Infrastructure adds the devices immediately.
- Step 4** When you are finished, click **Cancel**.

Related Topics

[Delete License Coverage for NetFlow and NAM Devices](#), on page 31

Delete License Coverage for NetFlow and NAM Devices

You may need to delete license coverage for a NetFlow or NAM device when:

- You have too many NetFlow and NAM devices for the number of Assurance licenses you have.
- You want to stop using Assurance management features with one or more NetFlow and NAM devices.

-
- Step 1** Choose **Administration > Licenses and Software Updates > Licenses > Assurance Licenses** (the **Assurance Licenses** link is in the upper right corner of the page).
- Prime Infrastructure displays the list of devices currently under Assurance management. It also displays the total number of Assurance licenses you have, and the total number of devices under Assurance management.
- Step 2** Select the check box next to each device you want to remove from Assurance management, then click **Remove Device**.

Related Topics

[Add License Coverage For NetFlow and NAM Devices](#) , on page 31

Smart Licensing

Smart Licensing feature provides a standardized licensing platform that simplifies user experience. When Smart Licensing is first enabled, Prime Infrastructure is in Evaluation mode until you register Prime Infrastructure with the Smart Software Manager (which resides on a centralized Cisco web site).

If you are currently using traditional licensing, Cisco recommends that you convert to Smart Licensing. For information on the differences between the two types of licensing, refer to the Cisco Smart Licensing Overview on Cisco.com .

The purpose of the smart licensing feature is to reduce license-related complexity by enabling users to:

- Purchase additional licenses and automatically update the information.
- Monitor current purchases and entitlements (duration and number of units).
- Monitor current usage information and trending information.
- Easily track if adequate licenses are purchased.
- Save time with the ability to transfer licenses across the company.



Note From Cisco Prime Infrastructure Release 3.5, Smart Licensing is supported for Operation Center.

The limitations of smart licensing feature are:

- In HA (High Availability), you can perform smart license actions (enable, register, deregister and disable) on the HA Primary server and these actions are not permitted on the HA Secondary server.
- While performing backup and restore operation, the license supported during backup will be restored. Smart licensing registration state cannot be restored on another server and in that case user has to register once again on the restored setup.
- While performing an upgrade from an older version, the license supported in the older version will be enabled by default in the new version.

Related Topics

[Set Up Cisco Smart Licensing on Prime Infrastructure](#), on page 32

[Set Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager](#), on page 33

[Enable Smart License on Prime Infrastructure](#), on page 34

[Register Prime Infrastructure with the Cisco Smart Software Manager](#), on page 35

[Choose Smart Software Licenses](#), on page 36

[Configure License Thresholds for the Prime Infrastructure License Dashboard](#), on page 37

[Perform Additional Actions](#), on page 38

[View the Licensing Dashboard](#), on page 37

[Reference: Product Registration and License Authorization Statuses](#), on page 39

Set Up Cisco Smart Licensing on Prime Infrastructure

Follow these steps to set up Cisco Smart Licensing. If you are currently using traditional licensing, use these same procedures to convert to Cisco Smart Licensing.

	Step	See:
1.	Create a Smart Account with Cisco Systems.	Go to: Smart Account Request and follow the instructions on the web site
2.	Set up communication between Prime Infrastructure and the Cisco Smart Software Manager (CSSM) on Cisco.com.	Setting Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager
3.	Enable Smart Licensing in Prime Infrastructure (you will have to restart the web GUI).	Enabling Smart License on Prime Infrastructure
4.	Register Prime Infrastructure with the CSSM on Cisco.com, then enter the license tokens into the Prime Infrastructure web GUI (you will have to restart the web GUI).	Registering Prime Infrastructure with the Cisco Smart Software Manager
5.	Choose the licenses you want to use in Prime Infrastructure.	Choosing Smart Software Licenses
6.	Set up the Smart License Dashboard to signal when you are running out of licenses.	Configuring License Thresholds for the Prime Infrastructure License Dashboard

Set Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager

Step 1 Choose **Administration > Settings > System Settings > General > Account Credentials** and select **Smart Licensing Transport** tab.

Alternatively, you can click the link mentioned in the **Smart Software Licensing** page to direct you to the **Smart Licensing Transport** tab to set up transport settings.

Step 2 You can select any of the following three modes:

- Direct mode—Select this option to send data directly to Cisco cloud. The Smart Call Home Server URL is a read-only and cannot be modified.
- Transport Gateway—Uses a Cisco Call Home transport gateway or a Cisco Smart Licensing Software satellite. (A Cisco Smart Licensing Software satellite is installed on customer premises and provides a subset of CSSM functionality. See [Cisco.com](https://www.cisco.com) for more information about satellites.) Specify an appropriate DNS mapped URL for the respective Smart Software Manager Satellite or Smart Software Manager. Refer Smart Software Manager User Guide for details.
- HTTP Proxy—Select this option to use an intermediate HTTP/HTTPS proxy between Prime Infrastructure and the Cisco cloud. To enable this option, you must first configure the proxy settings in the **Proxy** tab.

Step 3 Click **Test Connectivity** to test the connection status. Click **Save** to update the smart licensing transport mode.

Step 4 Proceed to Enabling Smart License on Prime Infrastructure .

Related Topics

[Smart Licensing](#), on page 32

- [Set Up Cisco Smart Licensing on Prime Infrastructure](#), on page 32
- [Enable Smart License on Prime Infrastructure](#), on page 34
- [Perform Additional Actions](#), on page 38
- [View the Licensing Dashboard](#), on page 37
- [Reference: Product Registration and License Authorization Statuses](#), on page 39

Enable Smart License on Prime Infrastructure

To enable smart license, follow these steps:

Before you begin

Make sure you have set up the transport mode. See "Set Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager" in Related Topics.

-
- Step 1** Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.
 - Step 2** In the **Licensing Settings** tab, select **Smart Software Licensing**.
 - Step 3** Choose **Prime Infrastructure** from the **Product Name** drop-down list.
 - Step 4** Click **Enable Smart Software Licensing**. Prime Infrastructure displays a dialog box informing you that you must log out of Prime Infrastructure and log back in, before you can proceed to the configuration step.
 - Step 5** Click **OK** in the dialog box.

Once the smart license is enabled and before it is registered, the product will be in **Evaluation Mode** for 90 days and you can manage any number of devices.

- Step 6** Perform one of the following:
 - a.** If you have not yet registered with the CSSM on Cisco.com, proceed to Registering Prime Infrastructure with the Cisco Smart Software Manager.
 - b.** If you have registered with the CSSM, proceed to Choosing Smart Software Licenses.

Note If you prefer traditional licenses, then in the **Licensing Settings** tab, select **Traditional Licensing** as the **Licensing Mode** and click **Register**. The **Administration > Licenses and Software Updates > Licenses** page is displayed.

Related Topics

- [Set Up Cisco Smart Licensing on Prime Infrastructure](#), on page 32
- [Register Prime Infrastructure with the Cisco Smart Software Manager](#), on page 35
- [Set Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager](#), on page 33
- [Perform Additional Actions](#), on page 38
- [View the Licensing Dashboard](#), on page 37
- [Disable Smart Licensing](#), on page 38
- [Reference: Product Registration and License Authorization Statuses](#), on page 39

Register Prime Infrastructure with the Cisco Smart Software Manager

This procedure creates a token which you will use to register your product instance with the CSSM. For information on how to use the CSSM, see the [Cisco Smart Software Manager User Guide](#).



Note Refer to the [Cisco Smart Software Manager User Guide](#) for information on other actions you can perform from the CSSM—for example, renewing license registration and license authorization, unregistering the product from Cisco Smart Licensing, and so forth.

Related Topics

[Generate Token ID](#), on page 35

[Register Product Instance](#), on page 36

Generate Token ID

If this is a new installation (you are not converting from traditional licensing), follow these steps:

Before you begin

If your organization does not have a Smart Account, go to software.cisco.com, choose **Request a Smart Account** (under Administration), and follow the instructions to create an account. If you are converting from traditional licensing, refer [Converting from Traditional Licensing](#).

-
- Step 1** Go to the Cisco Software Central web site (software.cisco.com).
 - Step 2** On Cisco Software Central, choose **License > Smart Software Licensing**.
 - Step 3** Select the appropriate virtual account (virtual accounts are automatically created when you create a Smart Account).
 - Step 4** Click the **General** tab, then click **New Token**.
 - Step 5** Follow the instructions to provide a name, duration, and export compliance applicability before accepting the terms and responsibilities.
 - Step 6** Click **Create Token**.
 - Step 7** Copy the Token ID to your clipboard and proceed to Registering Product Instance.
-

Convert from Traditional Licensing

If you are converting from traditional licensing, follow these steps:

-
- Step 1** Go to the Cisco Software Central web site (software.cisco.com).
 - Step 2** On Cisco Software Central, choose **License > Traditional Licensing**.
 - Step 3** Click **Continue to Product License Registration**.
 - Step 4** In the **Manage** area of the Product License Registration page, click the **PAKs/Tokens** tab and choose the entitlements you want to convert.
 - Step 5** From the **Actions** drop-down list, choose **Convert to Smart Entitlements**.

Step 6 Copy the Token ID to your clipboard and proceed to Registering Product Instance.

Register Product Instance

Enter the token IDs into the Prime Infrastructure web GUI and register the product.

Step 1 Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.

Step 2 Under the **Licensing Settings** tab, paste your token into the **Registration Token** field.

Step 3 Click **Register**.

Step 4 Log out of Prime Infrastructure, then log back in.

Step 5 Proceed to Choosing Smart Software Licenses.

Related Topics

[Set Up Cisco Smart Licensing on Prime Infrastructure](#), on page 32

[Choose Smart Software Licenses](#), on page 36

[Smart Licensing](#), on page 32

[Enable Smart License on Prime Infrastructure](#), on page 34

[Set Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager](#), on page 33

[Perform Additional Actions](#), on page 38

[View the Licensing Dashboard](#), on page 37

[Reference: Product Registration and License Authorization Statuses](#), on page 39

Choose Smart Software Licenses

Step 1 If this is the first time you are choosing Smart licenses:

a) Choose **Administration > Licenses and Software Updates > Licenses**.

After a few moments, Prime Infrastructure displays a dialog box informing you that you cannot access the page because you are not using traditional licensing. This is normal.

b) In the dialog box, click **Smart License Settings**.

c) Click the **Licensing Settings** tab.

Step 2 If you are already using Smart Licensing:

a) Choose **Administration > Licenses and Software Updates > Smart Software Licensing**.

b) Click the **Licensing Settings** tab.

Step 3 Click **Smart Software Licensing** radio button.

Step 4 Select the licenses in the Available Licenses dialog box, then click **Save**.

Step 5 Proceed to Configuring License Thresholds for the Prime Infrastructure License Dashboard.

Configure License Thresholds for the Prime Infrastructure License Dashboard

To manage your licenses more efficiently, configure the License Dashboard to indicate when you are nearing the point where your license count is depleted. The settings you configure here apply across the system.

-
- Step 1** Choose **Administration > Licenses and Software Updates > Smart Software Licensing**, then click the **License Dashboard Settings** tab.
 - Step 2** Select a license from the **License Type** drop-down list.
 - Step 3** Enter a value in the Threshold Value field.
 - Step 4** Click **Save**.

The threshold value is displayed as a straight line in the graphical representation of the **License Summary** and the **Device Distribution for License** dashlets.

Related Topics

- [View the Licensing Dashboard](#), on page 37
- [Choose Smart Software Licenses](#), on page 36
- [Set Up Cisco Smart Licensing on Prime Infrastructure](#), on page 32
- [Enable Smart License on Prime Infrastructure](#), on page 34
- [Register Prime Infrastructure with the Cisco Smart Software Manager](#), on page 35
- [Disable Smart Licensing](#), on page 38
- [Reference: Product Registration and License Authorization Statuses](#), on page 39

View the Licensing Dashboard

From the **Licensing** dashboard, you can determine whether traditional or smart software licensing is enabled (indicated in the **Active Licensing Mode** field at the top of the dashboard) and view the number of licenses that are currently in use. You can set the licensing mode from the **Smart Software Licensing** page (**Administration > Licenses and Software Updates > Smart Software Licensing**).

To open this dashboard, do one of the following:

- Choose **Administration > Dashboards > Licensing Dashboard**.
- Click the **Licensing Dashboard** link from the top-right corner of the **Smart Software Licensing** page.

The information displayed in the dashboard depends on the licensing mode that is enabled. If smart software licensing is currently enabled, the following dashlets are displayed:

- **License Summary Count** area—Displays the number of licenses consumed and the compliance status for each license type. The number of licenses displayed is based on the current date.
- **License Summary** dashlet—Displays a bar chart that graphs the number of licenses consumed for each license type during a particular time period. To view additional information, place your cursor over the chart.
- **Device Distribution for License** dashlet—To view the device distribution chart for a particular license, click its link from the top of the chart displayed in the **License Summary** dashlet. To view additional information, place your cursor over the chart.



Note The information displayed in the **License Dashboard** is refreshed daily after the SmartLicense job runs at 02:00 A.M. (its pre-configured run time). To view this job in the **Job Dashboard**, choose **Administration > Dashboards > Job Dashboard**.

If traditional licensing is currently enabled, the **Licensing** dashboard displays the **Traditional Licensing** dashlet. Specify whether you want to view information about Lifecycle or Assurance licenses by choosing the corresponding option from the **License Type** drop-down list. The dashlet updates, displaying information such as the device families with that license type, the number of tokens allocated to each device in those families, as well as the number of tokens that are not being used at the moment.

Disable Smart Licensing

- Step 1** Disable Smart licensing.
- Choose **Administration > Licenses and Software Updates > Smart Software Licensing**, then click the **Licensing Settings** tab.
 - At the bottom of the window, click **Disable Smart Licensing** and confirm your choice.
- Step 2** Enable traditional licensing. (This is done from the Smart License Settings page.)
- Choose **Administration > Licenses and Software Updates > Licenses**.
 - In the dialog box, click **Smart License Settings**.
 - Click the **Licensing Settings** tab.
 - For the Licensing Mode, select **Traditional Licensing**.
 - Click **Register**.

Related Topics

- [Configure License Thresholds for the Prime Infrastructure License Dashboard](#), on page 37
- [Enable Smart License on Prime Infrastructure](#), on page 34
- [Set Up Cisco Smart Licensing on Prime Infrastructure](#), on page 32
- [Register Prime Infrastructure with the Cisco Smart Software Manager](#), on page 35
- [Perform Additional Actions](#), on page 38

Perform Additional Actions

Choose any of the following actions from the **Actions** drop-down list. To know more about the status of licenses and product registration, refer [Reference: Product Registration and License Authorization Statuses](#).

- **Renew Authorization Now**—Click **Renew Authorization Now** to renew authorization with CSSM to enable Prime Infrastructure to remain compliant. By default, authorization periods are renewed every 30 days.
- **Renew Registration Now**—Click **Renew Registration Now** to renew the ID certificate that needs to be renewed every year for Prime Infrastructure to remain registered.
- **Deregister**—Prime Infrastructure will be de-registered from Smart Software Licensing and goes back to evaluation mode.

- Disable Smart Software Licensing—Prime Infrastructure will be unregistered from Smart Licensing and will be unlicensed. Once disabled, only **Administration** menu will be available on logging in. See [Disable Smart Licensing](#).

Related Topics

[Reference: Product Registration and License Authorization Statuses](#), on page 39

[Set Up Cisco Smart Licensing on Prime Infrastructure](#), on page 32

[View the Licensing Dashboard](#), on page 37

[Enable Smart License on Prime Infrastructure](#), on page 34

[Set Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager](#), on page 33

[Register Prime Infrastructure with the Cisco Smart Software Manager](#), on page 35

[Disable Smart Licensing](#), on page 38

Reference: Product Registration and License Authorization Statuses

Product Registration Status

The Product Registration Status reflects whether the product is properly registered with Cisco Smart Software Licensing on [Cisco.com](#).

Product Registration Status	Description
Unregistered	Smart Software Licensing is enabled on Prime Infrastructure, but Prime Infrastructure is not registered with the CSSM.
Registered	Prime Infrastructure is registered with the CSSM. Prime Infrastructure has received an ID certificate that will be used for future communication with the Cisco licensing authority.
Registration Expired	Prime Infrastructure did not successfully renew its registration prior to the expiration date and has been removed from CSSM.

License Authorization Status

The License Authorization Status reflects usage against purchased licenses and whether you are in compliance with Cisco Smart Licensing. If you exceed the number of purchased licenses, you will be Out of Compliance.

License Authorization Status	Description
Evaluation Mode	Prime Infrastructure is running in evaluation mode until the evaluation period expires (90 days).
Authorized	Prime Infrastructure has a valid Smart Account and is registered. All licenses requested by the product are authorized for use.
Out of Compliance	Prime Infrastructure has exceeded the number of licenses that were purchased. The Virtual account containing the product instance has a shortage of one or more of license types used.

License Authorization Status	Description
Evaluation Expired	The Evaluation period has expired and Prime Infrastructure will be in unlicensed state.
Authorization Expired	Prime Infrastructure did not successfully renew its license authorization prior to the authorization expiration date.

Related Topics

- [Smart Licensing](#), on page 32
- [Enable Smart License on Prime Infrastructure](#), on page 34
- [Set Up Cisco Smart Licensing on Prime Infrastructure](#), on page 32
- [Register Prime Infrastructure with the Cisco Smart Software Manager](#), on page 35
- [Perform Additional Actions](#), on page 38

Manage Software Updates

- [What Are Software Updates?](#), on page 40
- [View the Installed Product Software Version](#), on page 40
- [Enable or Disable Notifications About Software Updates](#), on page 41
- [View Installed Software Updates](#), on page 41

What Are Software Updates?

Cisco provides updates to the software periodically. These updates fall into the following three categories:

- **Critical Fixes**—Provide critical fixes to the software. We strongly recommend that you download and apply all of these updates as soon as they are available.
- **Device Support**—Adds support for managing devices which did not support at release time.
- **Add-ons**—Provide new features, which can include GUI screens and functionality, to supplement the version you are using. This includes maintenance packs and maintenance pack point patches.

The update notifications that displays depend on the Notification Settings specified by your administrator. See [Enable or Disable Notifications About Software Updates, on page 41](#). All software updates are packaged in .ubf files. A large update can contain individual smaller updates, from which you can choose what you want to install. When you install an update, does the following:

- Verifies that the file publisher is Cisco Systems and the file has not been tampered with
- Automatically installs any other updates that are required

If you have connectivity to <http://www.cisco.com>, you can download and install the updates directly from Cisco.com. If you do not have internet connectivity, copy the update from a server that has the necessary connectivity and install it from there.

View the Installed Product Software Version

Use one of these methods to check the product version:

To use the CLI, see [Establish an SSH Session With the Server, on page 78](#).

View Installed Software Updates

If you are not logged in to the web GUI, you can view a pop-up window that lists the software updates by clicking **View Installed Updates** from the login page.

If you are logged in to the web GUI, you can view the software updates in two ways:

- From the page, by clicking the settings icon at the top right of the page and clicking , and then clicking **View Installed Updates**. (The **View Installed Updates** link is also available from the login page.)
- By choosing **Administration > Licenses and Software Updates > Software Update** (this method provides the most detail).

The **Software Update** page displays two tabs:

- **Installed Updates**—Updates that is currently using.
- **Uploaded Update Files**—Update files that have been uploaded to the server (including those that are not being used). The Corresponding Updates field lists any prerequisite updates that were also uploaded.

If an update file has not yet been installed, it can be deleted. Select the file and click the **Delete** button.

Enable or Disable Notifications About Software Updates

By default, displays information about all available updates in the **Software Updates** page. Because the list can be quite long, you may want to adjust what is displayed and the updates for which you are notified. You can also disable all notifications and re-enable them later.

-
- Step 1** Configure the default Cisco.com credentials so that can get information about available updates.
- a) Choose **Administration > Settings > System Settings**, then choose **General > Account Settings**.
 - b) Click the **Cisco.com Credentials** tab, enter the credentials, then click **Save**.

- Step 2** Configure your software update notification settings.
- a) Choose **Administration > Settings > System Settings**, then choose **General > Software Update**.
 - b) Under **Notification Settings**, select or deselect the update categories. To disable all notifications, make sure no categories are selected. For an explanation of the categories, see [What Are Software Updates?, on page 40](#)
 - c) Click **Save**.
-

Validate Images (ISO and OVA) Before Installing Them

Before installing any software, you should verify the authenticity of the publisher by making sure the image is signed. This ensures that the image is from Cisco Systems and that it has not been tampered with.

software is provided in the following formats:

- .ubf files that you can download and install using the Software Update web GUI feature
- ISO or OVA images that are provided during major product releases and updates

You do not have to manually validate UBF packages that are downloaded using the Software Update feature. This is because automatically validates the .ubf files during the Software Update installation process. If a file is not signed, generates an error message and will not install the .ubf file. If this occurs, contact your Cisco representative.

You *do* need to manually validate ISO and OVA images. Use the following procedure to validate them before installation.

Step 1 If you do not have **openssl** installed, download and install it (see <http://www.openssl.org>).

Step 2 Place the following files in a temporary directory:

- The product file to be verified (*.iso or *.ova).
- The signature file (*.signature) that is packaged with the product file.
- The certificate file (*.pem). The same certificate is used to verify OVA and ISO images.

Step 3 Move to the temporary directory and run the following command as the Linux CLI root user (see [Log In and Out as the Linux CLI root User, on page 155](#)):

```
openssl dgst -sha512 -verify cert-file -signature sig-file content-file
```

Where:

- *cert-file* is the certificate file
- *sig-file* is the signature file
- *content-file* is the ISO file or OVA image to be verified

Step 4 If the result is **Verified OK**:

- For an ISO file, proceed with the installation (you do not have to perform any more steps as part of this validation procedure).
- For an OVA package, proceed to the next steps.

Step 5 (OVA package only) Verify that Cisco Systems is the publisher.

- a) In the VMware vSphere client, choose **File > Deploy OVF Template**.
- b) Browse to the OVA file (*.ova), select it, and click **Next**.
- c) Verify that the **Publisher** field in the **OVF Template Details** window displays **Cisco Systems, Inc.** with a green check mark next to it. Proceed to the next step.

Note Do not validate the image using the **Vendor** field. This field does not authenticate Cisco Systems as the publisher.

Note Do not proceed if the **Publisher** field displays **No certificate present**. This indicates the image is not signed, is not from Cisco Systems, or has been tampered with.

Step 6 Check the certificate chain.

- a) In the **OVF Template Details** window, click the **Cisco Systems, Inc.** hyperlink in the **Publisher** field.
- b) In the **Certificate** window, click the **Certification Path** tab.

- c) In the **Certification Path** tab (which lists the certificate chain), ensure that the **Certification Path** area displays **Cisco Systems, Inc.** and the **Certification Status** area displays **The certificate is OK.**

Download and Install a Software Update from Cisco.com

These steps explain how to download a software update from [cisco.com](https://www.cisco.com) and then install it on the server. If you are using high availability, .

Before you begin

Make sure you have an account on Cisco.com.

-
- Step 1** Back up your data. See [Perform a Manual Backup, on page 56](#).
 - Step 2** Download the file to your local machine, then upload it from your local machine to the server.
 - a) Log into [cisco.com](https://www.cisco.com) and go to the [Software Download site](#).
 - b) Locate the .ubf file you want to download, and download it to your local machine.
 - Step 3** Copy the file from your local machine to the server as described in [Copy a File from a Client Machine to the Server, on page 44](#).
 - Step 4** Log in to the web GUI as a user with Administrator privileges.
 - Step 5** Upload the file to the server.
 - a) Choose **Administration > Licenses and Software Updates > Software Update**.
 - b) Click **Upload** at the top of the page.
 - c) Click **Browse**, navigate to the file, and click **OK**. After the successful upload, the software will appear under the **Files** tab.
 - Step 6** Select the software update, click **Install**, and then click **Yes** in the confirmation pop-up window.

Note If the .ubf file is not signed or has been modified since it was downloaded from Cisco.com, will abort the installation. Contact your Cisco representative.

will auto-restart and the web GUI will not be accessible for some time. (If it does not, restart it by following the procedure in [Stop and Restart , on page 81](#).)
 - Step 7** When the web GUI is accessible, log in and check the version on the **Software Update** page.
 - a) Choose **Administration > Licenses and Software Updates > Software Update**.
 - b) Verify the information under the Updates tab.

What to do next

Instruct all users to clear their browser cache before opening the web GUI.

Copy a File from a Client Machine to the Server

Use the following SCP command to retrieve files from your client machine and copy them to the server's default local repository (/localdisk/defaultRepo). You should run this command as the Linux CLI root user (see [Log In and Out as the Linux CLI root User, on page 155](#)).

```
scp clientUsername@clientIP:/fullpath-to-file /localdisk/defaultRepo
```

Where:

- *clientUsername* is your username on the client machine
- *clientIP* is the IP address of the client machine where the file resides
- *fullpath-to-file* is the full pathname of the file on the client machine

For example:

```
scp jsmith@123.456.789.101:/temp/myfile.tar.gz /localdisk/defaultRepo
```

Before you begin

Make sure SCP is enabled on your client machine, and the required ports are open (see the).



CHAPTER 3

Backup and Restore

- [Backup and Restore Concepts](#), on page 45
- [Set Up and Manage Repositories](#), on page 50
- [Set Up Automatic Application Backups](#), on page 54
- [Perform a Manual Backup](#), on page 56
- [Restore Data](#), on page 57
- [How to Manage Disk Space Issues During Backup and Restore](#), on page 59
- [Backup and Restore with Operations Center](#), on page 61

Backup and Restore Concepts

- [Backup Types: Application and Appliance](#), on page 45
- [Backup Scheduling](#), on page 46
- [Backup Repositories](#), on page 46
- [Backup Filenames](#), on page 47
- [Backup Validation Process](#), on page 48
- [Information That Is Backed Up](#), on page 48
- [Information That Is Not Backed Up](#), on page 50

Backup Types: Application and Appliance

supports two types of backups:

- **Application backups**—Contain application data but do not include platform data (host-specific settings, such as the server hostname and IP address). Application backup should be used during upgrade, when you want to move only application data and not the platform/host specific configurations.
- **Appliance backups**—Contain all application data and platform data (host-specific settings, including the hostname, IP address, subnet mask, default gateway, and so on). Appliance backup should be used for disaster recovery (or to recover from platform hardware or software failures). For example, to recover from any disk or filesystem failure, the standard recovery process would be to reinstall and then restore from the appliance backup in order to restore all data as well as platform-specific configurations. You would then need to manually reconstruct the HA configurations as they are not included in the appliance backup.



Note For details on what is considered application data and what is considered platform data, see [Information That Is Backed Up, on page 48](#).

Note the following about application and appliance backups.

- Application and appliance backups can be restored to the same or a new host, as long as the new host has the same hardware and software configuration as the host from which the backup was taken.
- You can only restore an appliance backup to a host running the same version of the server software as the server from which the backup was taken.
- When upgrading to a later version of , application backup and restore can run across different releases, as long as the upgrade path is supported.
- You cannot restore an application backup using the appliance restore command, nor can you restore an appliance backup using the application restore command.

We recommend the following best practices:

- If you are *evaluating* , use the default automatic application backup to the local repository.
- If you are running *in a production environment* as a virtual appliance, take regular application backups to a remote backup server. You can use the application backups to restore your server for all failures except complete failure of the server hardware.

Backup Scheduling

performs automatic scheduled application backups. This feature is enabled by default and creates one application backup file every day in the default local backup repository.

You can change this schedule as needed. You can also take an automatic application backup at any time from the web GUI. Appliance backups can only be taken from the command line.

Automatic application backups can create storage space problems if the backup repository is local to the server. While this is usually acceptable in test implementations, it is not intended to substitute for routine scheduled backups to remote servers in a production environment.

We recommend the following for production environments:

- Set up remote repositories to store the backup files.
- Use the automatic schedule application backup to create backups on the remote repositories on a regular schedule.

Even if you are using scheduled backups, you can still use the command line to create application or appliance backups at any time.

Backup Repositories

By default, automatic application backup feature stores backup files in the local backup repository `/localdisk/defaultRepo`. You can use the web GUI to create a new local backup repository and then choose

it when you set up automatic application backups. You can also specify a remote repository but you must create the repository first as described in [Set Up and Manage Repositories, on page 50](#).

When taking application or appliance backups using the command line, you must specify the local or remote repository you want the backup to be stored in. In a production environment, this is normally a remote repository that is accessed via NFS, SFTP, or FTP. We recommend you use NFS because it is typically much faster and more reliable than other protocols.

There is no difference between performing an application backup from the command line or performing it from the web GUI. Both actions create the same backup file.

Whenever you use NFS to take backups or restore data from a remote backup, make sure the mounted NFS server remains active throughout the backup or restore operation. If the NFS server shuts down at any point in the process, the backup or restore operation will hang without warning or an error message.

Backup Filenames

Application backups launched from the web GUI—either automatically or manually—are assigned a filename with the following format:

```
host-yymmdd-hhmm_VERver_BKSZsize_CPUcpus_MEMtarget_RAMram_SWAPswap_APP_CKchecksum.tar.gpg
```

Application backups launched from the CLI use the same format, except that the file starts with the user-specified filename rather than the server name.

```
filename-yymmdd-hhmm_VERver_BKSZsize_CPUcpus_MEMtarget_RAMram_SWAPswap_APP_CKchecksum.tar.gpg
```

Appliance backups launched from the CLI have files that also start with the user-specified filename, but the type is indicated as SYS, not APP.

```
filename-yymmdd-hhmm_VERver_BKSZsize_CPUcpus_MEMtarget_RAMram_SWAPswap_SYS_CKchecksum.tar.gpg
```

The following table describes the variables used by the backup files.

Variable	Description
<i>host</i>	Host name of the server from which the backup was taken (for application backups launched from web GUI).
<i>filename</i>	Filename specified by user in command line (for application backups launched from CLI, and for appliance backups)
<i>yymmdd-hhmm</i>	Date and time the backup was taken
<i>ver</i>	Internal version.
<i>size</i>	Total size of the backup
<i>cpus</i>	Total number of CPUs in the server from which the backup was taken
<i>target</i>	Total amount of system memory in the server from which the backup was taken
<i>ram</i>	Total amount of RAM in the server from which the backup was taken
<i>swap</i>	Total size of the swap disk on the server from which the backup was taken
<i>checksum</i>	Backup file checksum

Backup Validation Process

performs the following steps to validate the backup files:

1. Before starting the backup process, validates disk size, fast-recovery area, and control files.
2. Validates the created backup database to ensure that it can be restored.
3. Validates the zipped application data against the files that were backed up.
4. Validates the TAR file to make sure it is correct and complete.
5. Validates the GPG file to ensure that it is correct.

If you manually transfer the backup file, or if you want to verify that the backup file transfer is completed, view the file's md5Checksum and file size.

Another best practice for validating a backup is to restore it to a standalone "test" installation of .

Information That Is Backed Up

The following table describes the information that is contained in backup files. This information is restored to the server from backups.

See [Information That Is Not Backed Up, on page 50](#) for details about data that is not saved by the backup mechanism.



Note

The `/opt/CSCOlumos/conf/Migration.xml` file contains all configuration files and reports that are backed up. This file is included in the backup and is restored.

Data Type	Feature	Information Saved and Restored

Application Data	Background job settings	Data in the database
	Configuration archive (device configuration files)	Data in the database
	Configuration templates	<ul style="list-style-type: none"> • Files in /opt/CSCOLumos: <ul style="list-style-type: none"> • /conf/ootb • /xmp_inventory/dar/customized-feature-parts/CONFIGURATION • Data in the database
	Credentials	Data in the database
	Device inventory data	Data in the database
	Licenses	Files in /opt/CSCOLumos/licenses
	Maps	<ul style="list-style-type: none"> • Files in /opt/CSCOLumos/domainmaps • Data in the database
	Reports	<ul style="list-style-type: none"> • Files in /localdisk/ftp: <ul style="list-style-type: none"> • /reports • /reportsOnDemand • Data in the database
	Managed device software image files	Data in the database
	System settings	Data in the database
	User preferences	<ul style="list-style-type: none"> • Files in /opt/CSCOLumos/conf/wap/datastore/webacs/xml/prefs • Data in the database
	users, groups, and roles	Data in the database
	Virtual domains	Data in the database

Platform Data	CLI settings	All CLI information and settings are preserved. This includes the list of backup repositories, the FTP user name, users created using the CLI, AAA information specified via the CLI, and other CLI settings (such as the terminal timeout).
	Credentials	Linux OS credentials file
	Network settings	Files in /opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml
	Linux user preferences	Linux data structure
	Linux users, groups, and roles	Linux data structure

Information That Is Not Backed Up

Before performing a backup, make sure that you manually note the following information because it is not saved as part of the backup process. You will need to reconfigure these settings after the data has been restored.

- High availability configurations
- Local customization (for example, report heap size)

Patch history information is also not saved.

For a list of information that is backed up, see [Information That Is Backed Up, on page 48](#).

Set Up and Manage Repositories

supports the following repository types:

- Remote repositories—NFS, FTP, SFTP

See the following topics for information on how to set up and manage these different types of repositories.

Create a Local Backup Repository

stores automatic backup files in the default local backup repository **/localdisk/defaultRepo**. You can create a different local backup repository and use it if you prefer.

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
- Step 2** Choose **System Jobs > Infrastructure**.
- Step 3** In the Jobs list, check the **Server Backup** check box.
- Step 4** Click **Edit** (the pencil icon) to open the Edit Job Properties dialog box.
- Step 5** Create the new local repository using the Edit Job properties dialog box.
- Click **Create**. The Create Backup Repository dialog box opens.

- b. Enter the name of the local repository you want to create.
- c. If it is an FTP repository, check the **FTP** check box and enter the location and credentials.
- d. Click **Submit**. The new repository is added to the Backup Repository drop-down list in the Edit Job Properties dialog box.

Step 6 Click **Save**.

Step 7 If you want to use the repository for future automatic application backups, specify it as described in [Specify the Backup Repository for Automatic Backups, on page 55](#).

Use a Remote Backup Repository

In production environments, we recommend that you use remote repositories for backups so that your network management data is protected from hardware and site failures. In most cases, this means you will need to:

1. Create one or more remote repositories to hold backup files. You will need to set these up yourself if your organization does not already have remote backup servers.
2. Specify the remote repository as the destination for automatic application backups.
3. If needed, specify the interval between automatic application backups and time of day to take them. You will need to monitor and manually archive automatic application backups stored on remote repositories (because the **Max backups to keep** setting does not apply to remote repositories).
4. Specify the remote repository as the backup destination when taking an application or appliance backup using the CLI backup commands.

As with any resource that you plan to access remotely, specifying the correct server IP address and login credentials during setup are a requirement for successful use of remote backup repositories with .

Use Remote NFS Backup Repositories

These topics explain how to use remote NFS backup repositories. After you have configured the NFS backupserver, you will need to contact your Cisco representative for information on how to configure PrimeInfrastructure to use the remote NFS server's backup repository. The procedure is not included here to protect the system's security.

Before You Set Up the NFS Backup Configuration

Before you begin, make sure:

- You know the IP address of the NFS server on which you want to stage and store backups. The staging and storage folders can be on the same NFS server, or on separate NFS servers. If you plan to stage and store on separate NFS servers, you will need IP addresses for both servers.
- You know the path names of the staging and storage folders on the NFS server. If you choose to stage and store on the same NFS server, the staging and storage folders.

How to Use Remote SFTP Backup Repositories

You can create backup repositories on a remote SFTP server and configure the Prime Infrastructure server to use them.

The SFTP server hosting your backups can be set up anywhere in your network, as long as the server:

- Has an IP address accessible from the Prime Infrastructure server.
- Has a user with write access to the SFTP server disk.
- Has a local shared folder where the backups will be stored.

Other than these requirements, no other configuration is needed on the SFTP backup server.

We recommend using remote NFS repositories.

For the SFTP server details to appear in the Backup Repository drop down list in UI, you should configure the SFTP server using CLI. You can configure the SFTP server only using CLI.

Step 1 Open a CLI session with the Prime Infrastructure server (see [How to Connect Via CLI, on page 111](#)).

Step 2 Enter configuration mode:

```
PIServer/admin# configure terminal
```

Step 3 Configure a symbolic link to the remote SFTP server:

```
PIServer/admin(config)# repository repositoryName
```

```
PIServer/admin(config-Repository)# url sftp://RemoteServerIP//sharedfolder
```

```
PIServer/admin(config-Repository)# user userName password plain userPassword
```

```
PIServer/admin(config-Repository)# exit
```

```
PIServer/admin(config)# exit
```

Where:

- repositoryName is the name of the repository (for example: MyRepo or PrimeInfrastructure).
- RemoteServerIP is the IP address of the SFTP server hosting the shared backup folder. Note that the example above specifies an absolute path to the shared folder. To specify a relative path to the shared folder, use only one slash in the URL. For example: **url sftp://RemoteServerIP//sharedfolder**
- sharedfolder is the name of the shared backup folder on the SFTP server.
- userName is the name of a user with write privileges to the repository on the SFTP server.
- userPassword is the corresponding password for that user.

Step 4 Verify creation of the symbolic link:

```
PIServer/admin# s how repository repositoryName
```

Step 5 When taking backups at the command line, specify the new repository as the repository name in the backup command. For example:

```
PIServer/admin# backup MyBackupFileName repository MyRepo application NCS
```


If you want to perform backups automatically, select the repository name you created as the repository name in the Prime Infrastructure web interface.

Related Topics

- [Use Remote NFS Backup Repositories](#), on page 51
- [Perform an Immediate Application Backup Using the CLI](#), on page 57
- [Perform an Immediate Appliance Backup Using the CLI](#), on page 56
- [Specify the Backup Repository for Automatic Backups](#), on page 55

How to Use Remote FTP Backup Repositories

You can create backup repositories on a remote FTP server and configure the Prime Infrastructure server to use them.

The SFTP server hosting your backups can be set up anywhere in your network, as long as the FTP server:

- Has an IP address accessible from the Prime Infrastructure server.
- Has a user (FTP user) with write access to the FTP server disk.
- Has a local subdirectory that matches the repository name you specify on the Prime Infrastructure server.
- Has a password of 15 characters or less.

Other than these requirements, no other configuration is needed on the FTP backup server.

We recommend using remote NFS repositories.

Step 1 Open a CLI session with the Prime Infrastructure server (see [How to Connect Via CLI](#), on page 111).

Step 2 Enter configuration mode:

```
PIServer/admin# configure terminal
```

Step 3 Configure a symbolic link to the remote FTP server:

```
PIServer/admin(config)# repository repositoryName  
PIServer/admin(config-Repository)# url ftp://RemoteServerIP/sharedfolder  
PIServer/admin(config-Repository)# user userName password plain userPassword  
PIServer/admin(config-Repository)# exit  
PIServer/admin(config)# exit
```

Where:

- `repositoryName` is the name of the repository (for example: MyRepo or PrimeInfrastructure).
- `RemoteServerIP` is the IP address of the FTP server hosting the shared backup folder.
- `sharedfolder` is the name of the shared backup folder on the FTP server.
- `userName` is the name of a user with write privileges to the repository on the FTP server.
- `userPassword` is the corresponding password for that user. This password must be 15 characters or less.

Step 4 Verify creation of the symbolic link:

```
PIServer/admin# s how repository repositoryName
```

Step 5 When taking backups at the command line, specify the new FTP repository as the repository name in the backup command. For example:

```
PIServer/admin# backup MyBackupFileName repository MyRepo application NCS
```

If you want to perform backups automatically, select the repository name you created as the repository name in the Prime Infrastructure web interface.

Related Topics

[Use Remote NFS Backup Repositories](#), on page 51

[Perform an Immediate Application Backup Using the CLI](#), on page 57

[Perform an Immediate Appliance Backup Using the CLI](#), on page 56

[Specify the Backup Repository for Automatic Backups](#), on page 55

Delete a Local Backup Repository

Use the following procedure to delete a local backup repository. This procedure ensures that the admin interface has the updated information.

Step 1 Log into the server as a CLI admin user (see [Establish an SSH Session With the Server](#), on page 78).

Step 2 List the local application backup repositories and identify the one that you want to delete:

```
show running-config | begin repository
```

Step 3 Enter configuration mode and delete the repository:

```
configure terminal
(config)# no repository repositoryName
```

Step 4 Repeat step 2 to verify that the repository was deleted.

Set Up Automatic Application Backups

Automatic application backups are enabled by default after installation. You can customize the schedule, specify a different backup repository, or adjust the number of backups that are saved.

To check what data is saved by the backup mechanism (and verify whether you need to manually save any data that is not backed up), see these topics:

- [Information That Is Backed Up](#), on page 48
- [Information That Is Not Backed Up](#), on page 50

Schedule Automatic Application Backups

Automatic application backups are enabled by default but you can adjust the day and interval at which these backups are performed. Performing a backup is resource-intensive and affects server performance. Avoid scheduling automatic backups to occur at peak traffic times.

If an automatic application backup fails, generates a Backup Failure alarm (with major severity). You can view these alarms just as you do other alarms. You can also get email notifications for these alarms if you include the System alarm category in your email notification settings.



Note After an automatic application backup fails, a pop-up message is displayed before every subsequent login attempt. This message will continue to appear until you acknowledge the corresponding alarm.

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
 - Step 2** Choose **System Jobs > Infrastructure**.
 - Step 3** In the Jobs list, check the **Server Backup** check box, then click **Edit Schedule**. The Schedule dialog box opens.
 - Step 4** In the Schedule dialog box, select a start date, recurrence interval, and optional end time.
 - Step 5** Click **Submit**. These settings will now be used for future automatic application backups.
-

Specify the Backup Repository for Automatic Backups

You can use the interface to specify a different backup repository for automatic application backups. The backup repository can be local or remote. You can also use the interface to create a new local backup repository if it does not already exist.

Before you begin

If you want to use a remote repository for automatic backups, you must create the repository first. Only local repositories can be created using this procedure. See [Set Up and Manage Repositories, on page 50](#).

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
 - Step 2** Choose **System Jobs > Infrastructure**.
 - Step 3** In the list of jobs, check the **Server Backup** check box.
 - Step 4** Click **Edit** (the pencil icon). The Edit Job Properties dialog box opens.
 - Step 5** Select a repository from the Backup Repository drop-down list, then click **Save**. will use the new repository when it performs the next automatic application backup.
-

Change the Number of Automatic Application Backups That Are Saved

Follow this procedure to adjust the number of automatic application backups that are saved on a local repository. When a backup exceeds the number you specify here, deletes the oldest backup from the repository.

The **Max UI backups to keep** setting does not apply if you are using remote repositories for automatic application backups. You must monitor and archive or delete old backups on remote repositories using your own methods.

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
 - Step 2** Choose **System Jobs > Infrastructure**.
 - Step 3** In the Jobs list, check the **Server Backup** check box.
 - Step 4** Click **Edit** (the pencil icon) to open the Edit Job Properties dialog box.
 - Step 5** Enter a value in the **Max UI backups to keep** field, then click **Save**. will enforce this setting at the next backup.
-

Perform a Manual Backup

The topics in this section explain how to perform manual application or appliance backups.

To check what data is saved by the backup mechanism (and verify whether you need to manually save any data that is not backed up), see these topics:

- [Information That Is Backed Up, on page 48](#)
- [Information That Is Not Backed Up, on page 50](#)

Perform an Immediate Appliance Backup Using the CLI

Users of Prime Infrastructure version 3.5 should be aware that appliance backups taken from a 3.1.x, 3.2.x, 3.3.x, or 3.4.x virtual or physical appliance cannot be restored to a Prime Infrastructure version 3.5 virtual or physical appliance, whereas appliance backups taken from a 3.5 virtual or physical appliance can be restored to a Prime Infrastructure version 3.5 virtual or physical appliance only.

-
- Step 1** Open a CLI session with the Prime Infrastructure server (see [How to Connect Via CLI, on page 111](#)).
 - Step 2** Display the list of appliance backups:

```
PIServer/(admin)#show repository repositoryName
```

where *repositoryName* is the repository on which you want to store the appliance backup.

- Step 3** Back up the appliance:

```
PIServer/(admin)#backup filename repository repositoryName
```

where *filename* is the name that you want to give the appliance backup file (for example, myBackup). The character length of the file name is 26. Other information is appended to the filename automatically, as explained in [Backup Filenames, on page 47](#)

Perform an Immediate Application Backup Using the Web GUI

Use this procedure to trigger an immediate application backup using the web GUI.

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard**.
- Step 2** Choose **System Jobs > Infrastructure**.
- Step 3** In the Jobs list, check the **Server Backup** check box, then click **Run**.
- Step 4** To view the backup status, scroll to the top of the table to locate the new job, then check its status and results.
-

Perform an Immediate Application Backup Using the CLI

Use this procedure to trigger an immediate application backup using the CLI.

-
- Step 1** Log into the server as a CLI admin user (see [Establish an SSH Session With the Server, on page 78](#)).
- Step 2** Display the list of backups, where *repositoryName* is the backup repository:
- ```
show repository repositoryName
```
- Step 3** Start the remote backup.
- ```
backup filename repository repositoryName application NCS
```
- where *filename* is the name that you want to give the appliance backup file (for example, myBackup). The character length of the file name is 26. Other information is appended to the filename automatically, as explained in [Backup Filenames, on page 47](#)
-

Perform a Manual Appliance Backup

Use this procedure to perform an appliance backup to a remote repository.

-
- Step 1** Make sure the remote host is available.
- Step 2** Log into the server as admin (see [Establish an SSH Session With the Server, on page 78](#)).
- Step 3** Start the remote backup:
- ```
(admin)# backup filename repository repositoryName
```
- Step 4** To verify that the backup transfer is complete, view the md5Checksum and file size.
- 

## Restore Data

All restore operations are performed using the CLI. Data can be restored to the host where the backup is executed (local host), or to a remote host. Backups can only be restored in their entirety; you cannot restore only parts of a backup.

See these topics for more information:

- [Restore an Application Backup, on page 58](#)

- [Restore an Appliance Backup, on page 58](#)

## Restore an Application Backup




---

**Note** To restore an *appliance* backup, use the procedure in [Restore an Appliance Backup, on page 58](#).

---

### Before you begin

If you are using high availability, read the guidelines in before restoring your data.

---

- Step 1** Log into the server as a CLI admin user (see [Establish an SSH Session With the Server, on page 78](#)).
- Step 2** If a previous restoration attempt failed, the database may have been corrupted. Run this command to recreate the database:
- ```
ncs run reset db
```
- Step 3** List the saved application backups and identify the one that you want to restore. *repositoryName* is the repository that contains the backup files.
- ```
show repository repositoryName
```
- Step 4** From the vmWare vSphere client (OVA) or the Cisco IMC server (Bare Metal), restore the data:
- ```
restore backupFileName repository repositoryName application NCS
```
- Step 5** If you are using Cisco Smart Licensing, re-register with the Cisco Smart Software Manager (CSSM) on Cisco.com. See .
-

Restore an Appliance Backup



Note To restore an *application* backup, use the procedure in [Restore an Application Backup, on page 58](#).

Before you begin

If you are using high availability, read the information in before restoring your data.

- Step 1** Log into the server as a CLI admin user (see [Establish an SSH Session With the Server, on page 78](#)).
- Step 2** If a previous restoration attempt failed, the database may have been corrupted. With the backup stored in an external repository, reinstall the setup using the same release and then retry the restore.
- Step 3** List the saved appliance backups and identify the one that you want to restore. *repositoryName* is the repository that contains the backup files.
- ```
show repository repositoryName
```
- Step 4** From the vmWare vSphere client (OVA) or the Cisco IMC server (Bare Metal), restore the data:
-

```
restore backupFileName repository repositoryName
```

**Step 5** Determine whether you should change the IP address, subnet mask, and default gateway.

- a) Check if your installation meets the following criteria:
- The restored host is on the same subnet as the old host, and the old host is still active.
  - The restored host is on a different subnet from the old host.

If it does, perform the next step.

- b) Change the IP address, subnet mask, default gateway and (optionally) the host name on the restored server.  
c) Write the changes to the server's running configuration and restart services. For example:

```
configure terminal
(config)# int GigabitEthernet 0
(config-GigabitEthernet)# ip address IPAddress subnetMask
(config-GigabitEthernet)# exit
(config)# ip default-gateway gatewayIP
(config)# hostname hostname
(config)# exit
(admin)# write mem
(admin)# ncs stop
(admin)# ncs start
(admin)# exit
```

**Step 6** If you are using Cisco Smart Licensing, re-register with the Cisco Smart Software Manager (CSSM) on Cisco.com. See

---

## Recover from Failed Restores

You may sometimes find that a restore does not complete, or reports a failure. Whenever a restore fails, you run the risk of database corruption, which can prevent the further restoration or re-installation. Perform the following steps to restore a corrupted database before attempting another restore or re-installation.

**Step 1** Open a CLI session with the server (see [Establish an SSH Session With the Server, on page 78](#)).

**Step 2** Enter the following command to reset the corrupted database:

```
ncs run reset db
```

---

## How to Manage Disk Space Issues During Backup and Restore

If you are experiencing issues with disk space *during* a backup or restore, we suggest that you either:

- Use the VMware **Edit Settings** feature to increase the amount of disk space allocated to the virtual machine (see [Modify VM Resource Allocation Using VMware vSphere Client](#)).

If you are using VMware ESXi 5.5 or later, use the vSphere Web Client to adjust this setting (see [Configuring Virtual Machine Hardware in the vSphere Web Client](#)).

- Use the method explained in [Migrate to Another Virtual Appliance Using Backup and Restore, on page 60](#) (or [Migrate to Another Physical Appliance Using Backup and Restore, on page 61](#)) to move your installation to a server with adequate disk space.

If you are unable to create a backup *after* a restore of your existing system, follow the steps explained in [Compact the Prime Infrastructure Database](#) to free disk space and create a successful backup.

If you are still unable to create a backup after using the **ncs cleanup** command, set up and use a remote repository (using FTP, SFTP, or NFS) for your backups, as explained in [Use a Remote Backup Repository](#).

#### Related Topics

- [Modify VM Resource Allocation Using VMware vSphere Client, on page 101](#)
- [Migrate to Another Physical Appliance Using Backup and Restore, on page 61](#)
- [Migrate to Another Virtual Appliance Using Backup and Restore, on page 60](#)
- [Compact the Prime Infrastructure Database, on page 102](#)
- [Use a Remote Backup Repository, on page 51](#)
- [How to Manage Disk Space Issues, on page 128](#)

## Migrate to Another Virtual Appliance Using Backup and Restore

You will need to migrate your data from an existing virtual appliance (OVA server installation) to a new one whenever you want to:

- Replace the old server entirely, such as after a catastrophic hardware failure. In this case, you can use your old installation media to re-create the new host on a replacement server, then migrate your application data from the old host to the new host.
- Migrate to a larger or more powerful server, so you can use to manage more of your network. In this case, you will want to ensure that you have the OVA installation file and install it on the new server using the larger installation option before retiring the older, smaller one. You can then migrate your application data from the old host.

In both cases, it is relatively easy to migrate your old data to the new virtual appliance by restoring to the new host an appliance or application backup taken from the old host.

- 
- Step 1** If you have not already done so, set up a remote backup repository for the old host, as explained in [Use a Remote Backup Repository, on page 51](#).
  - Step 2** Perform an application backup of the old host and save it to the remote repository (see [Perform an Immediate Application Backup Using the CLI, on page 57](#)).
  - Step 3** Install the new host .
  - Step 4** Configure the new host to use the same remote backup repository as the old host (see [Use a Remote Backup Repository, on page 51](#)).
  - Step 5** Restore the application backup on the remote repository to the new host (see [Restore an Application Backup, on page 58](#)).
-



## Migrate to Another Physical Appliance Using Backup and Restore

You will need to migrate your Prime Infrastructure data from an existing physical appliance to a new one whenever you want to:

- Replace the old appliance entirely, such as after a catastrophic hardware failure. In this case, you can order a replacement appliance, then migrate your data from the old appliance to the new appliance.
- Migrate to a newly installed appliance.

In both cases, it is relatively easy to migrate your old data to the new appliance by restoring to the new appliance an appliance or application backup from the old host.

- 
- Step 1** If the old appliance is still functional:
- a) If you have not already done so, set up a remote backup repository for the old appliance (see “Use a Remote Backup Repositories” in Related Topics).
  - b) Take an appliance or application backup of the old appliance on the remote repository (see “Take Appliance Backups” or “Take Application Backups”, as appropriate).
- Step 2** Configure the new appliance to use the same remote backup repository as the old appliance (see “Use a Remote Backup Repositories”).
- Step 3** Restore the appliance or application backup on the remote repository to the new appliance (see “Restore From Appliance Backups” or “Restore From Application Backups”, as appropriate). Be sure to follow the procedure appropriate for the type of backup you are restoring. For example: If you took an application backup from the old appliance, you must restore it using the procedure for restoring application backups, not appliance backups.

---

### Related Topics

- [Use a Remote Backup Repository](#), on page 51
- [Perform an Immediate Application Backup Using the CLI](#), on page 57
- [Perform an Immediate Appliance Backup Using the CLI](#), on page 56
- [Restore an Appliance Backup](#), on page 58
- [Restore an Application Backup](#), on page 58

## Backup and Restore with Operations Center

Prime Infrastructure instances running Operations Center can support restores of application backups taken using the CLI from Prime Infrastructure versions 3.1, 3.1.X, 3.2.X, 3.3.X, or 3.4.X.

You cannot schedule automatic application backups from the Prime Infrastructure instance running Operations Center.

For more details, see [Use a Remote Backup Repository](#) and [Restore an Application Backup](#).





## CHAPTER 4

# Configure the Prime Infrastructure Server

---

- [View the Server Configuration](#), on page 63
- [Available System Settings](#), on page 64
- [Secure the Connectivity of the Server](#), on page 70
- [MIB to Prime Infrastructure Alert/Event Mapping](#), on page 75
- [Establish an SSH Session With the Server](#), on page 78
- [Set Up NTP on the Server](#), on page 78
- [Set Up the Proxy Server](#), on page 79
- [Configure Server Port and Global Timeout Settings](#), on page 79
- [Set Up the SMTP E-Mail Server](#), on page 80
- [Enable FTP/TFTP/SFTP Service on the Server](#), on page 80
- [Configure Stored Cisco.com Credentials](#), on page 81
- [Create a Login Banner \(Login Disclaimer\)](#), on page 81
- [Stop and Restart](#), on page 81
- [Configure Global SNMP Settings for Communication with Network Elements](#), on page 82
- [Enable Compliance Services](#), on page 87
- [Configure ISE Servers](#), on page 87
- [Configure Software Image Management Servers](#), on page 88
- [Add Device Information to a User Defined Field](#), on page 88
- [Manage OUIs](#), on page 89
- [Work With Server Internal SNMP Traps That Indicate System Problems](#), on page 90
- [Set Up Defaults for Cisco Support Requests](#), on page 92
- [Configure Cisco Product Feedback Settings](#), on page 92
- [Migrating Data from Prime Infrastructure to Cisco Digital Network Architecture Center](#), on page 93

## View the Server Configuration

Use this procedure to view server configuration information such as the current server time, kernel version, operating system, hardware information, and so forth.

---

**Step 1** Choose **Administration > Dashboards > System Monitoring Dashboard**.

**Step 2** Click the **Overview** tab.

**Step 3** Click **System Information** at the top left of the dashboard to expand the System Information field.

## Available System Settings

The **Administration > Settings > System Settings** menu contains options to configure or modify Cisco Prime Infrastructure settings. You will want to customize many of these settings when you are first implementing Prime Infrastructure, but once in production, modify them only rarely.

The following table lists the types of settings you can configure or modify from the **Administration > Settings > System Settings** menu.

**Table 5: Available Prime Infrastructure System Settings Options**

| To do this:                                                                                                                                                                                                                                                                                                                                                                     | Choose <b>Administration &gt; Settings &gt; System Settings &gt;...</b>                                                                                                    | Applicable to:                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| Modify the stored Cisco.com credentials (user name and password) used to log on to Cisco.com and: <ul style="list-style-type: none"> <li>• Check for Cisco software image updates</li> <li>• Open or review Cisco support cases</li> </ul> You can also access this page from a link on the <b>Administration &gt; Settings &gt; System Settings &gt; Software Update</b> page. | General > Account Credentials                                                                                                                                              | Prime Infrastructure appliance |
| Configure proxies for the Prime Infrastructure server and its local authentication server.                                                                                                                                                                                                                                                                                      | General > Account Credentials > Proxy<br>See <a href="#">Set Up the Proxy Server</a> .                                                                                     | Not Applicable                 |
| Configure the settings for creating a technical support request.                                                                                                                                                                                                                                                                                                                | General > Account Credentials > Support Request<br>See <a href="#">Set Up Defaults for Cisco Support Requests</a> .                                                        | Wired and wireless devices     |
| Configure transport gateway mode to send information over the internet via Smart Call Home Transport Gateway, while smart licensing is enabled.                                                                                                                                                                                                                                 | General > Account Credentials > Smart Licensing Transport<br>See <a href="#">Set Up the Transport Mode Between Prime Infrastructure and Cisco Smart Software Manager</a> . | Prime Infrastructure appliance |
| Set the retention period for the following data types: Trends, Device Health, Performance, Network Audit, System Health.                                                                                                                                                                                                                                                        | <b>General &gt; Data Retention</b><br>See <a href="#">About Historical Data Retention, on page 132</a> .                                                                   | Wired and wireless devices     |

| To do this:                                                                                                                                                                                                                                                                                                                                                                                                                  | Choose Administration > Settings > System Settings >...                                                                                                             | Applicable to:                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Configure the guest account settings to globally remove all the guest accounts whose lifetime has ended. By default, Prime Infrastructure Lobby Ambassador can access all guest accounts irrespective of who created them. If you select the <b>Search and List only guest accounts created by this lobby ambassador</b> check box, the Lobby Ambassadors can access only the guest accounts that have been created by them. | <b>General &gt; Guest Account</b><br>See <a href="#">Configure Guest Account Settings, on page 184</a> .                                                            | Wireless devices only                         |
| To help Cisco improve its products, Prime Infrastructure collects the product feedback data and sends it to Cisco.                                                                                                                                                                                                                                                                                                           | General > Help Us Improve<br>See <a href="#">Configure Cisco Product Feedback Settings, on page 92</a> .                                                            | Wired and wireless devices                    |
| Enable job approval to specify the jobs which require administrator approval before the job can run.                                                                                                                                                                                                                                                                                                                         | <b>General &gt; Job Approval</b><br>See <a href="#">Configure Job Approvers and Approve Jobs, on page 190</a> .                                                     | Wired and wireless devices                    |
| Change the disclaimer text displayed on the login page for all users.                                                                                                                                                                                                                                                                                                                                                        | <b>General &gt; Login Disclaimer</b><br>See <a href="#">Create a Login Banner (Login Disclaimer), on page 81</a> .                                                  | Prime Infrastructure appliance                |
| Set the path where scheduled reports are stored and how long reports are retained.                                                                                                                                                                                                                                                                                                                                           | <b>General &gt; Report</b><br>See <a href="#">Control Report Storage and Retention, on page 136</a> .                                                               | Wired and wireless devices                    |
| <ul style="list-style-type: none"> <li>• Enable or disable FTP, TFTP, and HTTP/HTTPS server proxies, and specify the ports they communicate over.</li> <li>• See the NTP server name and local time zone currently configured for Prime Infrastructure</li> </ul>                                                                                                                                                            | <b>General &gt; Server</b><br>See <a href="#">Configure Server Port and Global Timeout Settings, on page 79</a> .                                                   | Prime Infrastructure appliance                |
| <ul style="list-style-type: none"> <li>• Specify that you do not want credentials stored on cisco.com when Prime Infrastructure checks cisco.com for Cisco software image updates</li> <li>• Select the kinds of Prime Infrastructure software updates for which you want to receive notifications (includes Critical Fixes, new Device Support, and Prime Add-On products)</li> </ul>                                       | <b>General &gt; Software Update</b>                                                                                                                                 | Wired and wireless devices                    |
| To migrate inventory, site groups, associated site maps and cmx data from Prime Infrastructure to DNA Center.                                                                                                                                                                                                                                                                                                                | <b>General &gt; DNA Center coexistence</b><br>See <a href="#">Migrating Data from Prime Infrastructure to Cisco Digital Network Architecture Center, on page 93</a> | Prime Infrastructure to DNA Center migration. |
| Enable Change Audit JMS Notification by selecting the <b>Enable Change Audit JMS Notification</b> check box.                                                                                                                                                                                                                                                                                                                 | <b>Mail and Notification &gt; Change Audit Notification</b><br>See <a href="#">Enable Change Audit Notifications and Configure Syslog Receivers, on page 232</a> .  | Wired and wireless devices                    |

| To do this:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Choose <b>Administration &gt; Settings &gt; System Settings &gt;...</b>                                                                                      | <b>Applicable to:</b>          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| To send job notification mail for every user job                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>Mail and Notification &gt; Job Notification Mail</b><br>See <a href="#">Configure Job Notification Mail for User Jobs</a> , on page 191                   | Wired and wireless devices     |
| Enable email distribution of reports and alarm notifications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Mail and Notification &gt; Mail Server Configuration</b><br>See <a href="#">Configure Email Server Settings</a> , on page 357.                            | Prime Infrastructure appliance |
| <ul style="list-style-type: none"> <li>• Set the protocol to be used for controller and autonomous AP CLI sessions.</li> <li>• Enable autonomous AP migration analysis on discovery.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                             | <b>Network and Device &gt; CLI Session</b><br>See <a href="#">Configure Protocols for CLI Sessions</a> , on page 243.                                        | Wireless devices only          |
| Enable auto refresh after a wireless controller upgrade, and process the save configuration trap.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>Network and Device &gt; Controller Upgrade</b><br>See <a href="#">Refresh Controllers After an Upgrade</a> , on page 245.                                 | Wireless devices only          |
| Enable Unified AP ping capability setting on the Cisco Prime Infrastructure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>Network and Device &gt; Unified AP Ping Reachability</b>                                                                                                  | Wireless devices only          |
| Modify the settings for Plug and Play.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Network and Device &gt; Plug &amp; Play</b>                                                                                                               | Wired devices only             |
| <p>Set global SNMP polling parameters, including trace display values, reachability parameters and the backoff algorithm.</p> <p>If you select <b>Exponential</b> for the Backoff Algorithm, each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time. If you select to use reachability parameters, the Prime Infrastructure defaults to the global Reachability Retries and Timeout that you configure. If unchecked, Prime Infrastructure always uses the timeout and retries specified.</p> | <b>Network and Device &gt; SNMP</b><br>See <a href="#">Configure Global SNMP Settings</a> , on page 82.                                                      | Wireless devices only          |
| Configure rogue AP settings to enable Prime Infrastructure to automatically track the switch port to which the rogue access point is connected in the network.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>Network and Device &gt; Switch Port Trace (SPT) &gt; Auto SPT</b><br>See <a href="#">Configure SNMP Credentials for Rogue AP Tracing</a> , on page 249.   | Wireless devices only          |
| Set the SNMP credentials and trace parameters to be used in tracing rogue AP switch ports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <b>Network and Device &gt; Switch Port Trace (SPT) &gt; Manual SPT</b><br>See <a href="#">Configure SNMP Credentials for Rogue AP Tracing</a> , on page 249. | Wireless devices only          |

| <b>To do this:</b>                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>Choose Administration &gt; Settings &gt; System Settings &gt;...</b>                                                                               | <b>Applicable to:</b>          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| Set basic and advanced switch port trace parameters.                                                                                                                                                                                                                                                                                                                                                                               | <b>Network and Device &gt; Switch Port Trace (SPT) &gt; SPT Configuration</b><br><br>See <a href="#">Configure Switch Port Tracing, on page 246</a> . | Wired devices only             |
| View, add, or delete the Ethernet MAC address available in Prime Infrastructure. If you add multiple Ethernet MAC addresses to this list, then Auto Switch Port Tracing will not scan these ports for Rogue AP.                                                                                                                                                                                                                    | <b>Network and Device &gt; Switch Port Trace (SPT) &gt; Known Ethernet MAC Address</b>                                                                | Prime Infrastructure appliance |
| Set basic control parameters used when deploying a device configuration, such as enabling backup of the running configuration, rollbacks, retrieval of <b>show</b> command output from the cache, and the number of CLI thread pools to use.                                                                                                                                                                                       | <b>Inventory &gt; Configuration</b><br><br>See <a href="#">Archive Device Configurations Before Template Deployment, on page 137</a> .                | Wired and wireless devices     |
| Set basic parameters for the configuration archive, such as protocol, timeout value, number of configuration versions to store, and so forth.                                                                                                                                                                                                                                                                                      | <b>Inventory &gt; Configuration Archive</b><br><br>See <a href="#">Specify When and How to Archive WLC Configurations, on page 137</a> .              | Wired and wireless devices     |
| Specify IPv4 or IPv6 address preferences                                                                                                                                                                                                                                                                                                                                                                                           | <b>Inventory &gt; Discovery</b>                                                                                                                       | Wired and wireless devices     |
| Determine whether you want to display groups that do not have members or children associated with them.                                                                                                                                                                                                                                                                                                                            | <b>Inventory &gt; Grouping</b>                                                                                                                        | Wired and wireless devices     |
| Configure global preference parameters for downloading, distributing, and recommending software Images.                                                                                                                                                                                                                                                                                                                            | <b>Inventory &gt; Software Image Management</b><br><br>See the Cisco Prime Infrastructure User Guide for information about Software Image Management. | Wired and wireless devices     |
| Enable inventory collection to allow Prime Infrastructure to collect inventory when it receives a syslog event for a device.                                                                                                                                                                                                                                                                                                       | <b>Inventory &gt; Inventory</b><br><br>See <a href="#">Specify Inventory Collection After Receiving Events, on page 136</a> .                         | Wired and wireless devices     |
| Store additional information about a device.                                                                                                                                                                                                                                                                                                                                                                                       | <b>Inventory &gt; User Defined Fields</b><br><br>See <a href="#">Add Device Information to a User Defined Field, on page 88</a> .                     | Wired devices only             |
| <ul style="list-style-type: none"> <li>• Change which alarms, events, and syslogs are deleted, and how often.</li> <li>• Set the alarm types for which email notifications are sent, and how often they are sent.</li> <li>• Set the alarm types displayed in the Alarm Summary view.</li> <li>• Change the content of alarm notifications sent by email.</li> <li>• Change how the source of any failure is displayed.</li> </ul> | <b>Alarms and Events &gt; Alarms and Events</b><br><br>See <a href="#">Specify Alarm Clean Up, Display and Email Options, on page 222</a> .           | Wired and wireless devices     |

| To do this:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Choose <b>Administration &gt; Settings &gt; System Settings &gt;...</b>                                                                                                                                                                                                                              | Applicable to:                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------|
| <p>Configure remote event and alarm receivers who will receive notifications from Prime Infrastructure.</p> <p>Alerts and events are sent as SNMPv2 notifications to configured notification destination. If you are adding a notification destination with the notification type UDP, the destination you add should be listening to UDP on the same port on which it is configured. By default, only INFO level events are processed for the selected category. Only SNMPV2 traps are considered for northbound notification.</p> | <p><b>Mail and Notification &gt; Notification Destination</b></p> <p>See <a href="#">Configure Alarms Notification Destination, on page 219</a>.</p> <p><b>Alarms and Events &gt; Alarm Notification Policies</b></p> <p>See <a href="#">Customize Alarm Notification Policies, on page 220</a>.</p> | Wired and wireless devices     |
| Set the severity level of any generated alarm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p><b>Alarms and Events &gt; Alarm Severity and Auto Clear</b></p> <p>See <a href="#">Change Severity Levels, on page 224</a>.</p>                                                                                                                                                                   | Wired and wireless devices     |
| Configure SNMP traps and events generated for the Prime Infrastructure hardware appliance.                                                                                                                                                                                                                                                                                                                                                                                                                                          | <p><b>Alarms and Events &gt; System Event Configuration</b></p> <p>See <a href="#">Internal SNMP Trap Generation, on page 343</a>.</p>                                                                                                                                                               | Prime Infrastructure appliance |



| To do this:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Choose Administration > Settings > System Settings >...                                                                  | Applicable to:             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <ul style="list-style-type: none"> <li>• Enable automatic troubleshooting of clients on the diagnostic channel.</li> <li>• Enable lookup of client hostnames from DNS servers and set how long to cache them.</li> <li>• Set how long to retain disassociated clients and their session data.</li> <li>• Poll Wired clients to identify their sessions only when a trap or syslog is received.</li> </ul> <p><b>Note</b> This is not a recommended option to be used in a network with large number of wireless clients.</p> <ul style="list-style-type: none"> <li>• Enable discover clients from enhanced traps to discover client and session information from enhanced trap received from the compatible Cisco WLCs.</li> </ul> <p>You must configure the WLCs to send the traps using the following CLI commands:</p> <ul style="list-style-type: none"> <li>• config trapflags client enhanced-802.11-associate</li> <li>• config trapflags client enhanced-802.11-deauthenticate</li> <li>• config trapflags client enhanced-802.11-stats</li> <li>• config trapflags client enhanced-authentication</li> <li>• Enable discover wired clients on trunk ports to discover the unmanaged entity other than switch and router, which is connected to trunk ports.</li> <li>• Disable saving of client association and disassociation traps and syslogs as events.</li> <li>• Enable saving of client authentication failure traps as events, and how long between failure traps to save them.</li> </ul> | <p><b>Client and User &gt; Client</b></p> <p>See <a href="#">Configure Client Performance Settings, on page 102.</a></p> | Wired and wireless devices |
| Add a vendor Organizationally Unique Identifier (OUI) mapping XML file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p><b>Client and User &gt; User Defined OUI</b></p> <p>See <a href="#">Add a New Vendor OUI Mapping.</a></p>             | Wired and wireless devices |
| Upload an updated vendor OUI mapping XML file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <p><b>Client and User &gt; Upload OUI</b></p> <p>See <a href="#">Upload an Updated Vendor OUI Mapping File.</a></p>      | Wired and wireless devices |
| Configure the Cisco WAAS Central Manager IP address in Cisco Prime Infrastructure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p><b>Services &gt; Service Container Management</b></p> <p>See Cisco WAAS Central Manager Integration (user guide).</p> | Wired devices only         |

## Secure the Connectivity of the Server

For data security, encrypts data in transit using standard public key cryptography methods and public key infrastructure (PKI). You can obtain more information about these technologies from the internet. encrypts the data that is exchanged between the following connections:

- Between the web server and the web client
- Between a CLI client and the CLI shell interface (handled by SSH)
- Between the and systems such as AAA and external storage

To secure communication between the web server and web client, use the public key cryptography services that are built in as part of the HTTPS mechanism. For that you need to generate a public key for the web server, store it on the server, and then share it with the web client. This can be done using the standard PKI certificate mechanism which not only shares the web server public key with the web client, but also guarantees that the public key belongs to the web server (URL) you are accessing. This prevents any third party from posing as the web server and collecting sensitive information that the web client is sending to the web server.

These topics provide additional steps you can take to secure the web server:

- Cisco recommends that the web server authenticate web clients using certificate-based authentication.
- To secure connectivity between a CLI client and the CLI interface, refer to the security hardening procedures in .
- To secure connectivity between the and systems such as AAA and external storage, refer to the recommendations in .

## Set Up HTTPS Access to Prime Infrastructure

Prime Infrastructure supports secure HTTPS client access. HTTPS access requires that you apply a private key and corresponding certificate files to the Prime Infrastructure server and that users update their client browsers to trust these certificates.

To accomplish this, you can use certificate files that are either:

- Self-signed. You can generate and apply self-signed certificates as explained in the related topic “Generate and Apply Self-Signed Certificates”.
- Digitally signed by a Certificate Authority (CA). CAs are organizations (like Cisco and VeriSign) that validate identities and issue certificates. Certificates issued by a CA bind a public key to the name of the entity (such as a server or device) identified in the certificate. You can obtain CA certificates from a third-party CA and apply them to the Prime Infrastructure server as explained in related topic “Import CA-Signed Host Certificates”.




---

**Note** A private key and self-signed certificate with default parameters is generated at the time of installation.

---

### Related Topics

[Generate and Apply Self-Signed Certificates](#), on page 71

[Import CA-Signed Host Certificates](#), on page 71

[Import Private Key](#), on page 73

[Export Private Key](#), on page 74

## Generate and Apply Self-Signed Certificates

Use Prime Infrastructure to generate and apply self-signed certificates.

- 
- Step 1** Start a CLI session with Prime Infrastructure (see [How to Connect Via CLI, on page 111](#)). Do not enter “configure terminal” mode.
- Step 2** Enter the following command to generate a new RSA key and self-signed certificate with domain information:
- ```
PIServer/admin# ncs key genkey -newdn
```
- You will be prompted for the Distinguished Name (DN) fields for the certificate. It is important to specify the fully qualified domain name (FQDN) of the server as the domain name that will be used to access Prime Infrastructure.
- Step 3** To make the certificate valid, restart Prime Infrastructure (see [Restart Prime Infrastructure Using CLI, on page 113](#)).
- To avoid login complaints, instruct users to add the self-signed certificate to their browsers’ trust stores when they next access the Prime Infrastructure login page.
-

Import CA-Signed Host Certificates

Use Prime Infrastructure to generate a Certificate Signing Request (CSR) file and send it to a Certificate Authority (CA) for validation. The method you use to send the CSR file to the CA will vary with the CA.

Once you have generated and sent the CSR file for certification, do *not* use the **genkey** command again to generate a new key on the same Prime Infrastructure server. If you do, importing the CA-signed certificates will result in mismatches between keys in the file and the server.

Note that signed server certificates are host-specific. They are preserved in Prime Infrastructure backups, but are restored only if the backup and restore servers have the same host name.



Note High Availability Virtual IP is designed to simplify the server management. signed server certificate configuration does not work with the Prime Infrastructure HA Virtual IP deployment.

- Step 1** Start a CLI session with Prime Infrastructure using "admin" credentials and check the existing trusted certificates (see “How to Connect Via CLI”). Do not enter “configure terminal” mode.
- ```
PIServer/admin# ncs key listcacerts
```
- where **listcacerts** is the command to list the existing trusted certificates.
- Step 2** Go to the PI server location **"/opt/CSCOncs/migrate/restore"** and check the imported certificates using "root" CLI credentials.
- Step 3** If certificates are found, delete the certificates through "admin" CLI credentials (see “Delete CA-Signed Certificates”). If no certificates are found, go to . Step 4 .
- ```
PIServer/admin# pi/admin# ncs key deletecacert <certificate name>
```
- Restart Prime Infrastructure server after deleting the certificates.

Step 4 Enter the following command to generate a CSR file in the default backup repository:

```
PIServer/admin# ncs key genkey -newdn -csr <csrfilename> repository <repositoryname>
```

where -newdn— Generates a new RSA key and self-signed certificate with domain information.

-csr—Generates a new CSR certificate.

Csrfilename—CSR filename. It is an arbitrary name of your choice (for example: MyCertificate.csr).

repositoryname— file location. The file name can contain up to 80 alphanumeric characters.

Example:

```
PIServer/admin# ncs key genkey -newdn -csr CSRFile.csr repository <repositoryname>
```

The NCS server is running. Changes will take effect on the next server restart

Enter the fully qualified domain name of the server: <FQDN>

Enter the name of your organizational unit: <organization>

Enter the name of your organization: <organization>

Enter the name of your city or locality: <city>

Enter the name of your state or province: <state>

Enter the two letter code for your country: <country code>

Specify subject alternate names.

If none specified, CN will be used.

Use comma seperated list - DNS:<name>,IP:<address>

DNS:<FQDN>,IP:<IPADDRESS>

Specify the public key algorithm [rsa/ec] : **rsa**

Specify the RSA key size [2048/4096/8192] : **4096**

Specify the signature algorithm [sha256/sha512] : **sha256**

Key and CSR/Certificate will be generated with following details

Subject : /C=US/ST=CA/L=SJ/O=Cisco Systems/OU=Prime Infra/CN=DNS:<FQDN>

Subject Alternate Name : DNS:<FQDN>,IP:<IPADDRESS>

Public Key Alg : rsa, 4096

Signature Alg : sha256

Continue [yes] : yes

Generating...

Completed...Changes will take affect on the next server restart

Note If you does not provide "Subject Alternate Name" - the CA certificate can be imported only in this machine.

If you provide "Subject Alternate Name" - You can import the CA certificate to be received from CA in any of the servers having the specified FQDN. To import CA certificate in SAN sepcified servers, you need to export private key from the server where you have generated the CSR and import the private key along with the signed certificate in other specified servers.

In SAN List, you should add the current server's FQDN.

Step 5 Send the CSR file to a Certificate Authority (CA) of your choice.

The CA will respond by sending you an signed server certificate and one or more CA certificate files. The CA response will indicate which of the files is:

- The signed server certificate. This is typically given a filename that reflects the host name of the server to which you will apply it.
- The CA certificates , which are typically given filenames that reflect the name of the CA.

Combine all the certificates in to one single file by concatenating them. Host certificate should be the first one in the file followed by the CA certificates in the same order as in the chain.

For example, in linux the following command can be used to combine files:

```
cat host.pem subca.pem rootca.pem > servercert.pem
```

Note Certificates should be in PEM format

Step 6 Enter the following command to import the signed server certificate file into the Prime Infrastructure server:

```
PIServer/admin# ncs key importcacert tomcat <certificate_name> repository <repositoryname>
```

Step 7 Enter the following command to import the Signed certificate file into the Prime Infrastructure server:

```
PIServer/admin# ncs key importsignedcert <certificate_name> repository <repositoryname>
```

Step 8 To activate the CA-signed certificates, restart Prime Infrastructure (see “Restarting Prime Infrastructure”).

If the CA who signed the certificate is not already a trusted CA in your organization: Instruct users to add the CA-signed certificate to their browsers’ trust stores when they next access the Prime Infrastructure login page.

Note If you want to import CA certiifcate to have secure connection between PI and External devices/server use below command:

```
PIServer/admin# ncs key importcacert truststore {system | devicemgmt}alias <alias_name>
<CA_certificate_name> repository <repository_name>
```

For more information, see [How to Connect Via CLI, on page 111](#) and [Restart Prime Infrastructure Using CLI, on page 113](#).

Import Private Key

You can generate the private key and signed certificate externally. If you are generating them external, following command can be used to import both key and certificate together.

```
ncs key importkey <private_key_filename> <certificate_filename> repository <repository_name>
```

Export Private Key

The following is the command to export private key,

```
ncs key exportkey <private_key_filename> <certificate_filename> repository <repository_name>
```

After executing the above command private key will be generated and placed in the file location pointed in the repository.

Set Up Certificate Validation

During secure transactions like TLS/HTTPS connection, user authentication (when certificate based authentication is enabled), Prime Infrastructure will receive certificates from external entities. Prime Infrastructure needs to validate these certificate to ascertain the integrity of the certificate and the identity of the certificate holder. Certificate validation features allows the user to control how the certificates received from other entities are validated.

When the certificate validation is enforced, certificates received from other entities would be accepted by Prime Infrastructure only if that certificate is signed by certificate authority (CA) trusted by Prime Infrastructure. Trust store is where user can maintain the trusted CA certificates. If the signed certificate chain is not rooted to one of the CA certificates in the trust store, validation will fail.

Managing Trust Store

User can manage the trusted CAs in the trust store. Prime Infrastructure provides different trust stores namely – pubnet, system, devicemgmt and user.

- pubnet – Used while validating certificates received from remote hosts when connecting to servers in public network.
- system – Used while validating certificates received from remote systems when connecting to systems within network.
- devicemgmt – Used while validating certificates received from managed devices.
- user – Used to validate user certificates (When certificate based authentication is enabled).

CLIs to Manage Trust Store

The following is the CLI used to manage the trust store.

- [Importing a CA certificate to Trust Store, on page 74](#)
- [Viewing a CA Certificate in a Trust Store, on page 74](#)
- [Deleting a CA certificate from a trust store, on page 75](#)

Importing a CA certificate to Trust Store

The following is the command to import CA certificate to a trust store:

- `ncs certvalidation trusted-ca-store importcert alias <ALIAS> repository <Repository-name> <certificate-file> truststore {devicemgmt | pubnet | system | user}`

Viewing a CA Certificate in a Trust Store

The following is the command to view CA certificate in a trust store:

- ncs certvalidation trusted-ca-store listcacerts truststore {devicemgmt | pubnet | system | user}

Deleting a CA certificate from a trust store

The following is the command to delete CA certificate to a trust store:

- ncs certvalidation trusted-ca-store deletecacert alias <ALIAS> truststore {devicemgmt | pubnet | system | user}

Configuring Certificate Validation

User can configure the certificate validation for the following category:

- Enable certificate validation
- Disable certificate validation
- TOFU (Trust-on-first-use) - Trust stores are not used instead the certificate received from remote host is trusted when the connection is made for the first time. If the remote host sends a different certificate for any sub-sequent connection, connection will be rejected.

Enable certificate validation

The following is the command to enable to certificate validation:

- ncs certvalidation certificate-check trust-on-first-use trustzone {devicemgmt | pubnet | system | user}

View Certificate Validation List

The following is the command to view to certificate validation list:

- ncs certvalidation tofu-certs listcerts

Delete Certificate Validation

The following is the command to delete to certificate validation:

- ncs certvalidation tofu-certs deletecert host <host>

Auto Updating CA List

From time to time, Cisco releases a standard set of CA certificates recommended by Cisco. These trust stores can be configured automatically to update the CA list with Cisco trusted CA bundle during software update.

The following is the command to configure auto update CA list:

- ncs certvalidation trusted-ca-store auto-ca-update enable truststore {devicemgmt | pubnet | system | user}

MIB to Prime Infrastructure Alert/Event Mapping

The following table summarizes how the CISCO_WIRELESS_NOTIFICATION_MIB fields and OIDs map to Prime Infrastructure alerts and events.

Table 6: CISCO_WIRELESS_NOTIFICATION_MIB to Prime Infrastructure Alert/Event Mapping

Field Name and Object ID	Data Type	Prime Infrastructure Event/Alert field	Description
cWNotificationTimestamp	DateAndTime	createTime - NmsAlert eventTime - NmsEvent	Creation time for alarm/event.
cWNotificationUpdatedTimestamp	DateAndTime	modTime - NmsAlert	Modification time for Alarm. Events do not have modification time.
cWNotificationKey	SnmpAdminString	objectId - NmsEvent entityString- NmsAlert	Unique alarm/event ID in string form.
cWNotificationCategory	CWirelessNotificationCategory	NA	Category of the Events/Alarms. Possible values are: unknown accessPoints adhocRogue clients controllers coverageHole interference contextAwareNotifications meshLinks mobilityService performance rogueAP rrm security wes switch ncs
cWNotificationSubCategory	OCTET STRING	Type field in alert and eventType in event.	This object represents the subcategory of the alert.
cWNotificationServerAddress	InetAddress	N/A	Prime Infrastructure IP address.

Field Name and Object ID	Data Type	Prime Infrastructure Event/Alert field	Description
cWNotificationManagedObjectAddressType	InetAddressType	N/A	The type of Internet address by which the managed object is reachable. Possible values: 0—unknown 1—IPv4 2—IPv6 3—IPv4z 4—IPv6z 16—DNS Always set to “1” because Prime Infrastructure only supports IPv4 addresses.
cWNotificationManagedObjectAddress	InetAddress	getNode() value is used if present	getNode is populated for events and some alerts. If it is not null, then it is used for this field.
cWNotificationSourceDisplayName	OCTET STRING	sourceDisplayName field in alert/event.	This object represents the display name of the source of the notification.
cWNotificationDescription	OCTET STRING	Text - NmsEvent Message - NmsAlert	Alarm description string.
cWNotificationSeverity	INTEGER	severity - NmsEvent, NmsAlert	Severity of the alert/event: cleared(1) critical(3) major(4) minor(5) warning(6) info(7)
cWNotificationSpecialAttributes	OCTET STRING	All the attributes in alerts/events apart from the base alert/event class.	This object represents the specialized attributes in alerts like APAssociated, APDisassociated, RogueAPAlert, CoverageHoleAlert, and so on. The string is formatted in property=value pairs in CSV format.

Field Name and Object ID	Data Type	Prime Infrastructure Event/Alert field	Description
cWNotificationVirtualDomains	OCTET STRING	N/A	Virtual Domain of the object that caused the alarm. This field is empty for the current release.

Establish an SSH Session With the Server

When you connect to the server, use SSH and log in as the admin user. (See [User Interfaces, User Types, and How To Transition Between Them](#), on page 153 for more information.)

- Step 1** Start your SSH session and log in as the admin user.
- From the command line, enter the following, where *server-ip* is the :


```
ssh admin server-ip
```
 - Open an SSH client and log in as **admin**.

- Step 2** Enter the admin password. The prompt will change to the following:

```
(admin)
```

To view a list of the operations the admin user can perform, enter `?` at the prompt.

To enter admin config mode, enter the following command (note the change in the prompt):

```
(admin) configure terminal
(config)
```

Set Up NTP on the Server

Network Time Protocol (NTP) must be properly synchronized on all devices in your network as well as on the server. Failure to manage NTP synchronizations across your network can result in anomalous results in . This includes all -related servers: Any remote FTP servers that you use for backups, secondary high-availability servers, and so on.

You specify the default and secondary NTP servers during server installation. You can also use 's **ntp server** command to add to or change the list of NTP servers after installation.



Note cannot be configured as an NTP server; it acts as an NTP client only. Up to three NTP servers are allowed.

Step 1 Log in to the server as the admin user and enter config mode. See [Establish an SSH Session With the Server](#), on page 78.

Step 2 Set up the NTP server using one of the following commands.

```
ntp server ntp-server-IP ntp-key-id ntp-key
```

Where:

- *ntp-server-IP* is the IP address or hostname of the server providing the clock synchronization to the server
 - *ntp-key-id ntp-key* is the md5 key ID md5 key of the authenticated NTP server
-

Set Up the Proxy Server

Use this procedure to configure proxies for the server and, if configured, its local authentication server. If you use a proxy server as a security barrier between your network and the Internet, you need to configure the proxy settings as shown in the following steps:

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

Step 2 Click the **Proxy** tab.

Step 3 Select the **Enable Proxy** check box and enter the required information about the server that has connectivity to Cisco.com and will act as the proxy.

Step 4 Select the **Authentication Proxy** check box and enter the proxy server's user name and password.

Step 5 Click **Test Connectivity** to check the connection to the proxy server.

Step 6 Click **Save**.

Configure Server Port and Global Timeout Settings

The Server page allows you to enable or disable Prime Infrastructure's FTP, TFTP, and HTTP/HTTPS services.

FTP and TFTP services are normally enabled by default. HTTP services are disabled by default. You should enable HTTP services if you use the Plug and Play feature and your devices are configured to use HTTP to acquire the initial configuration in the bootstrap configuration.

See the latest [Prime Infrastructure Quick Start Guide](#) for more information.

Step 1 Choose **Administration > Settings > System Settings > General > Server**.

Step 2 To modify the FTP, TFTP, or HTTP service status and ports that were established during installation, enter the port number (or port number and root, where required) that you want to modify, then click **Enable** or **Disable**.

The Global Idle Timeout is enabled by default and is set to 10 minutes. The Global Idle Timeout setting overrides the User Idle Timeout setting in the My Preferences page. Only users with administrative privileges can disable the Global Idle Timeout value or change its time limit.

- Step 3** Click **Save**.
- Step 4** A server restart is required to apply your changes (see [Restart Prime Infrastructure Using CLI, on page 113](#)).

Set Up the SMTP E-Mail Server

To enable to send email notifications (for alarms, jobs, reports, and so forth), the system administrator must configure a primary SMTP email server (and, preferably, a secondary email server).

- Step 1** Choose **Administration > Settings > System Settings**, then choose **Mail and Notification > Mail Server Configuration**.
- Step 2** Under Primary SMTP Server, complete the Hostname/IP, User Name, Password, and Confirm Password fields as appropriate for the email server you want to use. Enter the IP address of the physical server. and the Enter the hostname of the primary SMTP server.
- Note** You cannot enter a virtual IP address in the Hostname/IP field, and the IP address cannot be behind a load balancer.
- Step 3** (Optional) Complete the same fields under Secondary SMTP Server. SMTP server username and password.
- Step 4** Under Sender and Receivers, enter a legitimate email address for .
- Step 5** When you are finished, click **Save**.

Enable FTP/TFTP/SFTP Service on the Server

FTP/TFTP/SFTP is used to transfer files between the server and devices for device configuration and software image file management. These protocols are also used in high availability deployments to transfer files to a secondary server. These services are normally enabled by default. If you installed in FIPS mode, they are disabled by default. If you use this page to enable these services, will become non-compliant with FIPS.

SFTP is the secure version of the file transfer service and is used by default. FTP is the unsecured version of the file transfer service; TFTP is the simple, unsecured version of the service. If you want to use either FTP or TFTP, you must enable the service after adding the server.

- Step 1** Configure to use the FTP, TFTP, or SFTP server.
- Choose **Administration > Servers > TFTP/FTP/SFTP Servers**.
 - From the **Select a command** drop-down list, choose **Add TFTP/FTP/SFTP Server**, then click **Go**.
 - From the **Server Type** drop-down list, choose **FTP, TFTP, SFTP, or All**.
 - Enter a user-defined name for the server.
 - Enter the IP address of the server.
 - Click **Save**.
- Step 2** If you want to use FTP or TFTP, enable it on the server.
- Choose **Administration > Settings > System Settings**, then choose **General > Server**.
 - Go to the FTP or TFTP area.

- c) Click **Enable**.
- d) Click **Save**.

Step 3 Restart to apply your changes. See [Stop and Restart](#), on page 81.

Configure Stored Cisco.com Credentials

stores only the username and not the password to log in to Cisco.com while performing the following tasks:

- Checks for product software updates
- Checks for device software image updates

To download the updates and open/review a support case, you are required to enter a password.

If these settings are not configured, will prompt users for their credentials when they perform these tasks. To configure a global Cisco.com user name and password:

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

Step 2 Under the **Cisco.com Credentials** tab, enter a user name and password, and click **Save**.

Create a Login Banner (Login Disclaimer)

When you have a message that you want to display to all users before they log in, create a login disclaimer. The text will be displayed on the GUI client login page below the login and password fields.

Step 1 Choose **Administration > Settings > System Settings**, then choose **General > Login Disclaimer**.

Step 2 Enter (or edit) the login disclaimer text.

Note Carriage returns are ignored.

Your changes will take effect immediately.

Stop and Restart

A restart is needed in rare cases, such as after a product software upgrade. When you stop the server, all user sessions are terminated.

To stop the server, open a CLI session with the server and enter:

```
ncs stop
```

To restart the server, open a CLI session with the server and enter:

```
ncs start
```

Configure Global SNMP Settings for Communication with Network Elements

The SNMP Settings page controls the how the server uses SNMP to reach and monitor devices. These settings will determine when a device is considered unreachable. Any changes you make on this page are applied globally and are saved across restarts, as well as across backups and restores.



Note The default network address is 0.0.0.0, which indicates the entire network. An SNMP credential is defined per network, so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. You should update the prepopulated SNMP credential with your own SNMP information.

-
- Step 1** Choose **Administration > Settings > System Settings**, then choose **Network and Device > SNMP**.
- Step 2** (Optional) Select the **Trace Display Values** check box to display mediation trace-level logging data values that are fetched using SNMP.
- Step 3** Choose an algorithm from the **Backoff Algorithm** drop-down list.
- **Exponential**—Each SNMP try will wait twice as long as the previous try, starting with the specified timeout for the first try.
 - **Constant**—Each SNMP try will wait the same length of time (timeout). This is useful on unreliable networks where the desired number of retries is large. Because it does not double the timeout per try, it does not take as long to timeout with a high number of retries.
- Step 4** If you do not want to use the timeout and retries specified by the device, configure the following parameters.
- Note** If switch port tracing is taking a long time to complete, reduce the Reachability Retries value.
- **Reachability Retries**—Enter the number of global retries.
 - **Reachability Timeout**—Enter a global timeout.
- Step 5** In the **MaximumVarBinds per PDU** field, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU. This Maximum VarBinds per PDU field enables you to make necessary changes when you have any failures associated to SNMP. For customers who have issues with PDU fragmentation in their network, this number can be reduced to 50, which typically eliminates the fragmentation.
- Step 6** Optionally adjust the **Maximum Rows per Table**.
- Step 7** Click **Save**.
-

Configure Global SNMP Settings

The SNMP Settings page allows you to configure global SNMP settings for Prime Infrastructure.

Any changes you make on this page affect Prime Infrastructure globally. The changes are saved across restarts as well as across backups and restores.

The default network address is 0.0.0.0, which indicates the entire network. SNMP credentials are defined per-network so only network addresses are allowed. 0.0.0.0 is the SNMP credential default and is used when no specific SNMP credential is defined. You should update the pre-populated SNMP credential with your own SNMP information.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > SNMP**.
- Step 2** (Optional) Select the **Trace Display Values** check box to display mediation trace-level logging data values fetched from the controller using SNMP. If unselected, these values do not appear.
- Step 3** From the Backoff Algorithm list, choose **Exponential** or **Constant Timeout**. If you choose Exponential, each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try. If you choose Constant Timeout, each SNMP try waits the same, specified amount of time.
- Constant Timeout is useful on unreliable networks (such as satellite networks) where the desired number of retries is large. Because it does not double the timeout per try, it does not take as long to timeout with a high number of retries.
- Step 4** Determine if you want to use reachability parameters. If selected, Prime Infrastructure defaults to the global Reachability Retries and Timeout that you configure. If unselected, Prime Infrastructure always uses the timeout and retries specified per controller or per IOS access point.
- Adjust this setting downward if switch port tracing is taking a long time to complete.
- Step 5** In Reachability Retries, enter the number of global retries used for determining device reachability. This field is only available if the **Use Reachability Parameters** check box is selected.
- Adjust this setting downward if switch port tracing is taking a long time to complete.
- Note** You cannot edit the value of Reachability Timeout. The default value is 2 seconds.
- Step 6** In the Maximum VarBinds per PDU field, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU.
- This Maximum VarBinds per PDU field enables you to make necessary changes with when you have any failures associated to SNMP.
- For customers who have issues with PDU fragmentation in their network, this number can be reduced to 50, which typically eliminates the fragmentation.
- The maximum rows per table field is configurable. The configured value is retained even if you upgrade Prime Infrastructure to a newer version.
- Step 7** Click **Save** to confirm these settings.

Related Topics

- [View SNMP Credential Details](#), on page 83
- [Add SNMP Credentials](#), on page 84
- [Import SNMP Credentials](#), on page 85

View SNMP Credential Details

The SNMP credentials listed in this page will be used only for tracing the Rogue APs Switch Port.

Step 1 Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**.

Step 2 Click the Network Address link to display the SNMP Credential Details page. The page displays the following information:

- General Parameters
 - Add Format Type—Display only. For details, see “Add SNMP Credentials” in Related Topics.
 - Network Address
 - Network Mask
- SNMP Parameters—Choose the applicable versions for SNMP parameters. The SNMP credentials are validated according to which SNMP versions are selected.
- Enter SNMP parameters for write access, if available. With display-only access parameters, the switch is added but you cannot modify its configuration in Prime Infrastructure. Device connectivity tests use the SNMP retries and timeout parameters.
- Retries—The number of times that attempts are made to discover the switch.
- Timeout—The session timeout value in seconds, which specifies the maximum amount of time allowed for a client before it is forced to reauthenticate.
- SNMP v1 Parameters or v2 Parameters—If selected, enter the applicable community in the available text box.
- SNMP v3 Parameters—If selected, configure the following parameters:
 - Username
 - Auth. Type
 - Auth. Password
 - Privacy Type
 - Privacy Password

If SNMP v1 or v2 with default community is configured, the network is open to easy attacks because default communities are well known. SNMP v1 or v2 with a non default community is more secure than a default community, but SNMP v3 with Auth and Privacy type and no default user is the most secure SNMP connection.

Step 3 Click **OK** to save your changes.

Related Topics

[Configure Global SNMP Settings](#), on page 82

[Add SNMP Credentials](#), on page 84

[Import SNMP Credentials](#), on page 85

Add SNMP Credentials

Prime Infrastructure needs device SNMP credentials to poll your network devices, back up and change their configurations, and so on. You can add SNMP credentials by hand. You can also import them in bulk (see “Importing SNMP Credentials” in Related Topics).

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**.
- Step 2** Choose **Select a command > Add SNMP Entries > Go**.
- Step 3** In the **Add Format Type** drop-down list, choose **SNMP Credential Info**.
- Step 4** Enter the IP address of the switch you want to add. If you want to add multiple switches, use a comma between each IP address.
- Step 5** In the **Retries** field, enter the number of times that attempts are made to discover the switch.
- Step 6** Provide the session timeout value in seconds. This determines the maximum amount of time allowed for a client before it is forced to reauthenticate.
- Step 7** Choose the applicable versions for the SNMP parameters. The SNMP credentials are validated according to which SNMP versions are selected.
- If **SNMP v1 Parameters** or **v2 Parameters** is selected, enter the applicable community in the available text box.
 - If **SNMP v3 Parameters** is selected, configure the following parameters:
 - Username
 - Auth. Type
 - Auth. Password
 - Privacy Type
 - Privacy Password
- If **SNMP v1** or **v2** with default community is configured, the network is open to easy attacks because default communities are well known. **SNMP v1** or **v2** with a non-default community is more secure than a default community, but **SNMP v3** with **Auth** and **Privacy** type and no default user is the most secure SNMP connection.
- Step 8** Click **OK**.
- If Prime Infrastructure can use the SNMP credential listed to access the switch, the switch is added for later use and appears in the **Network Devices** page accessible via **Configuration > Network > Network Devices**. If you manually add switches through the **Network Devices** page, switch port tracing uses the credentials from that page, not the ones listed in the **SNMP Credentials** page. If the manually added switch credentials have changed, you need to update them using the **Network Devices** pages.

Related Topics

- [Configure Global SNMP Settings](#), on page 82
- [View SNMP Credential Details](#), on page 83
- [Import SNMP Credentials](#), on page 85

Import SNMP Credentials

Prime Infrastructure needs device SNMP credentials to poll your network devices, back up and change their configurations, and so on. You can import SNMP credentials in bulk by importing them from a CSV file. You can also add them by hand (see “Adding SNMP Credentials” in Related Topics).

Related Topics Make sure you have created a CSV file with the proper format, and that it is available for upload from a folder on the client machine you use to access Prime Infrastructure. Here is a sample SNMP credentials CSV file suitable for import:

```
ip_address,snmp_version,snmp_community,snmpv3_user_name,snmpv3_auth_type,snmpv3_auth_password,
snmpv3_privacy_type,snmpv3_privacy_password,network_mask 1.1.1.0,v2,private,user1,HMAC-MD5,
12345,DES,12345,255.255.255.0 2.2.2.0,v2,private,user1,HMAC-MD5,password3,DES,password4,
255.255.255.0 10.77.246.0,v2,private,user1,HMAC-MD5,12345,DES,12345,255.255.255.0
```

The first row of the file is mandatory, as it describes the column arrangement. The IP Address column is also mandatory. The CSV file can contain the following fields:

- ip_address:IP address
- snmp_version:SNMP version
- network_mask:Network mask
- snmp_community:SNMP V1/V2 community
- snmpv3_user_name:SNMP V3 username
- snmpv3_auth_type:SNMP V3 authorization type. Can be None or HMAC-MD5 or HMAC-SHA
- snmpv3_auth_password:SNMP V3 authorization password
- snmpv3_privacy_type:SNMP V3 privacy type. Can be None or DES or CFB-AES-128
- snmpv3_privacy_password:SNMP V3 privacy password
- snmp_retries:SNMP retries
- snmp_timeout:SNMP timeout

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**.
- Step 2** Choose **Select a command > Add SNMP Entries > Go**.
- Step 3** In the **Add Format Type** drop-down list, choose File.
- Step 4** Click Browse to navigate to the CSV file you want to import and select it.
- Step 5** Click OK to import the file.

If Prime Infrastructure can use the SNMP credential listed to access the switch, the switch is added for later use and appears in the Network Devices page accessible via **Configuration > Network > Network Devices**. If you manually add switches through the Network Devices page, switch port tracing uses the credentials from that page, not the ones listed in the SNMP Credentials page. If the manually added switch credentials have changed, you need to update them using the Network Devices pages.

Related Topics

[Configure Global SNMP Settings](#), on page 82

[View SNMP Credential Details](#), on page 83

[Add SNMP Credentials](#), on page 84

Enable Compliance Services

Compliance Services allow Prime Infrastructure users to run Cisco PSIRT security and EOX obsolete-device compliance reports. This feature also lets users establish baseline device configuration standards, and then audit field configurations against these standards, identifying devices that are non-compliant and how their configuration differ from standards.

Compliance Services are disabled by default. In order to use them, the Prime Infrastructure administrator must enable the feature. You must also re-synchronize the server's device inventory. All users must also log out and then log back in to see the **Configuration > Compliance** menu option.

Compliance Services are available only on the following Prime Infrastructure server options:

- The Professional virtual appliance. For details, see the sections "Virtual Appliance Options" and "Understanding System Requirements" in the latest [Cisco Prime Infrastructure Quick Start Guide](#).
- The Cisco Unified Computing System (UCS) Gen 2 physical appliance. For details, see the sections "Virtual Appliance Options" and "Understand System Requirements" in the latest [Cisco Prime Infrastructure Quick Start Guide](#).
- Standard Prime Infrastructure virtual appliance. For details, see the section "Prime Infrastructure Minimum Server Requirements" in the latest [Cisco Prime Infrastructure Quick Start Guide](#).

Do not attempt to enable Compliance Services on Express, Express-Plus. If you do, the feature itself will not work. In addition, if you enable it and then try to migrate your data to a newly installed Professional or Gen 2 UCS appliance, the settings in the migrated data from the source Express or Express-Plus will prevent Compliance Services from working on the target appliance. You can avoid all this by simply leaving the Compliance Services feature disabled on the Express or Express-Plus, and then migrating your data to the Professional or Gen2 UCS appliance.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Server**.
- Step 2** Next to **Compliance Services**, click **Enable**.
- Step 3** Click **Save**.
- Step 4** Re-synchronize Prime Infrastructure's device inventory: Choose **Inventory > Network Devices**, select **All Devices**, then click the **Sync** icon.
- Step 5** Ask any users who are currently logged in to Prime Infrastructure to log out. They will be able to see the new **Configuration > Compliance** menu option when they log in again.
- For details, see [Virtual Appliance Options](#) and [Physical Appliance Options](#).
-

Configure ISE Servers

-
- Step 1** Choose **Administration > Servers > ISE Servers**.
- Step 2** Choose **Select a command > Add ISE Server**, then click **Go**.
- Step 3** Enter the ISE server's IP address, user name, and password.

Step 4 Confirm the ISE server password.

Step 5 Click **Save**.

Configure Software Image Management Servers

You can add up to three software image management servers for image distribution.

Step 1 Click **Administration > Servers > Software Image Management Servers**.

Step 2 Click the add icon and complete the following fields:

- Server Name
- IP Address
- Sites Served
- Description

Step 3 Click **Save**.

Step 4 Click **Manage Protocols** to add the protocols.

Step 5 Click the add icon and complete the following fields:

- Protocol
- Username
- Password
- Protocol Directory

Note If you choose TFTP protocol, enter the relative path without a leading slash in the **Protocol Directory** field. If you leave the **Protocol Directory** field empty, the image transfer will use the default home directory of your external server.

Step 6 Click **Save**.

Add Device Information to a User Defined Field

The User Defined Fields (UDFs) are used to store additional information about devices, such as device location attributes (for example: area, facility, floor, and so on). UDF attributes are used whenever a new device is added, imported or exported.

Step 1 Choose **Administration > Settings > System Settings > Inventory > User Defined Field**.

Step 2 Click **Add Row** to add a UDF.

Step 3 Enter the field label and description in the corresponding fields.

Step 4 Click **Save** to add a UDF.

Manage OUIs

Prime Infrastructure relies on the IEEE Organizational Unique Identifier (OUI) database to identify the client vendor name mapping. Prime Infrastructure stores vendor OUI mappings in an XML file named vendorMacs.xml. This file is updated for each release of Prime Infrastructure. With the OUI update, you can change the vendor display name for an existing OUI, add new OUIs to Prime Infrastructure and refresh the vendorMacs.xml file with new vendor OUI mappings and upload it to Prime Infrastructure.

Related Topics

[Add a New Vendor OUI Mapping](#), on page 89

[Upload an Updated Vendor OUI Mapping File](#), on page 89

Add a New Vendor OUI Mapping

The User Defined OUI List page displays a list of vendor OUI mappings that you created. This page allows you to add a new vendor OUI mapping, delete an OUI entry, and update the vendor name for an OUI that is existing in the vendorMacs.xml file.

When you add an OUI, Prime Infrastructure verifies the vendorMacs.xml file to see if the OUI exists. If the OUI exists, Prime Infrastructure updates the vendor name for the OUI. If the OUI does not exist, Prime Infrastructure adds a new OUI entry to the vendor OUI mapping.

-
- Step 1** Choose **Administration > Settings > System Settings > Client and User > User Defined OUI**. The User Defined OUI page appears.
 - Step 2** Choose **Add OUI Entries** from the **Select a Command** drop-down list, then click **Go**.
 - Step 3** In the OUI field, enter a valid OUI. The format is aa:bb:cc.
 - Step 4** Click **Check** to verify if the OUI exists in the vendor OUI mapping.
 - Step 5** In the Name field, enter the display name of the vendor for the OUI.
 - Step 6** Select the **Change Vendor Name** check box to update the display name of the vendor, if the OUI exists in the vendor OUI mapping, then click **OK**.
-

Upload an Updated Vendor OUI Mapping File

Prime Infrastructure allows you to get OUI updates online from the IEEE Registration Authority database (see the link to the RA database in Related Topics). If Prime Infrastructure is unable to reach the IEEE database, a message appears instructing you to save and upload the file to your Prime Infrastructure server.

-
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Upload OUI**. The Upload OUI From File page appears.
 - Step 2** Click **Update online from IEEE** to get OUI updates from the IEEE Registration Authority database (see the link to the RA database in Related Topics). If Prime Infrastructure is unable to reach the IEEE database, a message appears instruction you to save and upload the file.
 - Step 3** Click **OK** after the update completes successfully.

After you upload the `vendorMac.xml` file in the **Administration > Settings > System Settings > Upload OUI** page: If the vendor name is not reflected for existing unknown vendor clients in the Unique Clients and Users Summary report, run the `updateUnknownClient.sh` script. This script is located in the `/opt/CSColumos/bin` folder.

For more information, see [IEEE Registration Authority database](#).

Sample Log File from North-Bound SNMP Receiver

The following sample output shows the `ncs_nb.log` file generated by Prime Infrastructure. This log file is located in the log file directory on Prime Infrastructure server (`/opt/CSColumos/logs`). The log output helps you troubleshoot when alarms are not being received by the North Bound SNMP receiver.

```
2013-12-02 17:11:53,868 [main] INFO services - Queue type is order
2013-12-02 17:11:53,870 [main] INFO services - Starting the notification thread..
2013-12-02 17:11:53,871 [NBNotifier] INFO services - Fetching the head of the queue
2013-12-02 17:11:53,871 [NBNotifier] INFO services - The Queue is empty
2013-12-02 17:11:53,871 [main] INFO notification - Setting the NB process flag
2013-12-02 17:41:50,839 [Task Scheduler Worker-10] ERROR notification - Unable to get OSS
list
2013-12-03 08:22:39,227 [main] INFO services - Queue type is order
2013-12-03 08:22:39,229 [main] INFO services - Starting the notification thread..
2013-12-03 08:22:39,231 [NBNotifier] INFO services - Fetching the head of the queue
2013-12-03 08:22:39,231 [NBNotifier] INFO services - The Queue is empty
2013-12-03 08:22:39,231 [main] INFO notification - Setting the NB process flag
2013-12-03 08:44:40,287 [main] INFO services - Queue type is order
2013-12-03 08:44:40,289 [main] INFO services - Starting the notification thread..
2013-12-03 08:44:40,290 [NBNotifier] INFO services - Fetching the head of the queue
2013-12-03 08:44:40,290 [NBNotifier] INFO services - The Queue is empty
2013-12-03 08:44:40,290 [main] INFO notification - Setting the NB process flag
2013-12-03 08:56:18,864 [Task Scheduler Worker-8] ERROR notification - Unable to get OSS
list
```

Work With Server Internal SNMP Traps That Indicate System Problems

generates internal SNMP traps that indicate potential problems with system components. This includes hardware component failures, high availability state changes, backup status, and so forth. The failure trap is generated as soon as the failure or state change is detected, and a clearing trap is generated if the failure corrects itself. For TCAs (high CPU, memory and disk utilization traps, and so forth), the trap is generated when the threshold is exceeded.

A complete list of server internal SNMP traps is provided in . sends traps to notification destination on port 162. This port cannot be customized at present.

You can customize and manage these traps as described in the following topics:

- [Customize Server Internal SNMP Traps and Forward the Traps, on page 91](#)
- [Troubleshoot Server Internal SNMP Traps, on page 91](#)

Customize Server Internal SNMP Traps and Forward the Traps

You can customize server internal SNMP traps by adjusting their severity or (for TCAs) thresholds. You can also disable and enable the traps. Server internal SNMP traps are listed in .



Note does not send SNMPv2 Inform or SNMPv3 notifications.

Step 1 Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > System Event Configuration**.

Step 2 For each SNMP event you want to configure:

- a) Click on the row for that event.
- b) Set the **Event Severity** to Critical, Major, or Minor, as needed.
- c) For the CPU, disk, memory utilization, and other hardware traps, Enter the **Threshold** percentage (from 1–99). These events will send the associated SNMP traps when the utilization exceeds the threshold limit. (You cannot set thresholds for events for which the threshold setting is shown as NE.) These events send traps whenever the associated failure is detected.
- d) For backup threshold and certificate expiry (critical), enter the **Threshold** in days (from x – y , where x is the minimum number of days and y is the maximum number of days).
- e) To control whether a trap is or is not generated, set the **Event Status**.

Step 3 To save all of your trap changes, click **Save** (below the table).

Step 4 If you want to configure receivers for the server internal SNMP traps, refer to the procedures in the following topics, depending on whether you want to send the information as an email or trap notification.

- [Forward Alarms and Events as Email Notifications \(Administrator Procedure\)](#)
- [Forward Alarms and Events as SNMP Trap Notifications](#)

Troubleshoot Server Internal SNMP Traps

provides a complete list of server internal SNMP traps, their probable cause, and recommended actions to remedy the problem. If that document does not provide the information you need, follow this procedure to troubleshoot and get more information about server issues.

Step 1 Ping the notification from the server to ensure that there is connectivity between and your management application.

Step 2 Check if any firewall ACL settings are blocking port 162, and open communications on that port if needed.

Step 3 Log in to with a user ID that has Administrator privileges. Select **Administration > Logging** and download the log files. Then compare the activity recorded in these log files with the activity you are seeing in your management application:

- ncs_nbi.log: This is the log of all the northbound SNMP trap messages has sent. Check for messages you have not received.
- ncs-#-#.log: This is the log of most other recent activity. Check for hardware trap messages you have not received.
- hm-#-#.log: This is the log of all Health Monitor activity. Check for recent messages about High Availability state-changes and application-process failures that you have not received.

The messages you see in these logs should match the activity you see in your management application. If you find major differences, open a support case with Cisco Technical Assistance Center (TAC) and attach the suspect log files with your case. See [Open a Cisco Support Case, on page 229](#).

Set Up Defaults for Cisco Support Requests

By default, users can create Cisco support requests from different parts of the GUI. If desired, you can configure the sender e-mail address and other e-mail characteristics. If you do not configure them, users can supply the information when they open a case.

If you do not want to allow users to create requests from the GUI client, you can disable that feature.

- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Account Settings**.
- Step 2** Click the **Support Request** tab.
- Step 3** Select the type of interaction you prefer:
- Enable interactions directly from the server—Specify this option to create the support case directly from the server. E-Mails to the support provider are sent from the e-mail address associated with the server or the e-mail address you specify.
 - Interactions via client system only—Specify this option to download the information required for your support case to a client machine. You must then e-mail the downloaded support case details and information to the support provider.
- Step 4** Select your technical support provider:
- Click **Cisco** to open a support case with Cisco Technical Support, enter your Cisco.com credentials, then click **Test Connectivity** to check the connectivity to the following servers:
 - mail server
 - Cisco support server
 - Forum server
 - Click **Third-party Support Provider** to create a service request with a third-party support provider. Enter the provider's e-mail address, the subject line, and the website URL.
-

Configure Cisco Product Feedback Settings

To help Cisco improve its products, collects the following data and sends it to Cisco:

- Product information—Product type, software version, and installed licenses.
- System information—Server operating system and available memory.
- Network information—Number and type of devices on your network.

This feature is enabled by default. Data is collected on a daily, weekly, and monthly basis and is posted to a REST URL in the Cisco cloud using HTTPS. Choose **Administration > Settings > System Settings**, then choose **General > Help Us Improve**, and:

- To view the types of data Cisco collects, click **What data is Cisco collecting?**
- To disable this feature, select **Not at this time, thank you**, then click **Save**.

Migrating Data from Prime Infrastructure to Cisco Digital Network Architecture Center

You can now integrate Cisco Prime Infrastructure with Cisco Digital Network Architecture (DNA) Center and utilize the intent-based networking solution for managing application user experience in the enterprise.

Cisco DNA Center supports the expression of intent for multiple use cases, including base automation capabilities, fabric provisioning, and policy-based segmentation in the enterprise network. Cisco DNA Center adds context to this journey through the introduction of Analytics and Assurance. To know more about Cisco DNA Center, visit <http://cisco.com/go/dna>

You can migrate devices, location groups, associated site maps and cmx data from Prime Infrastructure to Cisco DNA Center and manage your enterprise network over a centralized dashboard.

Before you begin

Ensure that:

You have Root and Super Users access privileges of Prime Infrastructure server.

You have access credentials of Cisco DNA Center server.

You use Prime Infrastructure server version 3.5 is compatible with the Cisco DNA Center servers 1.2.1, 1.2.2, 1.2.3, 1.2.4, 1.2.5, and 1.2.6.

You use a single session of the migration at a time for the same Prime Infrastructure Cisco DNA Center server pair.

Step 1 You can access the Prime Infrastructure to Cisco DNA Center migration by logging in to Prime Infrastructure, selecting **Administration > Settings > System Settings > General > Cisco DNA Center coexistence**, and then click **Launch Cisco DNA Center coexistence** to open **Prime Infrastructure - Cisco DNA Center Coexistence** page.

Step 2 Click **Add Cisco DNA Center Server**.

Step 3 Enter the following Cisco DNA Center server details:

Note You can integrate only one Cisco DNA Center server at a time.

- a) Server IP Address or HostName.
- b) Username.
- c) Password
- d) Confirm Password

Step 4 Click **Save**, to check server reachability.

Step 5 Click **Next** to go to **Sync Settings**.

Step 6 In the **Sync Settings** window:

- a) Select the **Enables automatic synchronization of data integrated with Cisco DNA Center** checkbox to move modifications of already migrated set of data from Prime Infrastructure to Cisco DNA Center automatically post modification.
- b) Select the **Include newly added data during dynamic synchronization** checkbox to move the additions in the migrated hierarchy during dynamic synchronization, if any, from Prime Infrastructure to Cisco DNA Center automatically post addition.

Note This checkbox is enabled only if you select the **Select the Enables automatic synchronization of data integrated with Cisco DNA Center** checkbox.

Step 7 Click **Next** to go to **Select Groups** page.

Step 8 In the **Select Groups** window:

- a) Select the location groups from **Prime Infrastructure Selector** pane. Upon selecting location groups, by default the buildings, floors and associated maps also get selected.

Before adding Prime Infrastructure location groups to Cisco DNA Center, you can check the limitation status bar for the available devices and site groups of Cisco DNA Center.

The Prime Infrastructure groups selector pane lists all the Prime Infrastructure groups irrespective of any virtual domain

- Note**
- Any legacy device which are not supported by Cisco DNA Center chosen for migration will be added to Cisco DNA Center inventory under Device Type column -“Unsupported Cisco Device”.
 - Any device which falls under "Default" group category cannot be migrated to Cisco DNA Center.
 - Any devices managed only with SNMP V1 credentials in Prime Infrastructure cannot be migrated to Cisco DNA Center. Whereas SNMP V2 and V3 can be migrated to Cisco DNA Center.

Step 9 Click **Next**.

Step 10 In the CMX Credentials window:

- a) You can view the list of associated CMX for selected groups with the following details:

- Credential Status
- Server IP
- Device Name
- Username
- Password
- SSH Username
- SSH password

- b) You must update the **SSH Username** and **SSH Password**, if it is not available for the respective CMX.

Note Once the CMX is migrated to Cisco DNA Center, it will not be managed by Prime Infrastructure.

- c) If associated CMX is not found, then click Next.

Note CMX should be reachable. If not, the unreachable CMX must be removed from Prime Infrastructure before migrating to Cisco DNA Center.

Step 11 In the Summary window:

- a) You can view the overall summary of selected location groups, devices, associated maps and cmx. before migrating to Cisco DNA Center
- b) You can also view the groups, devices, maps and cmx which is added, updated and deleted under each respective tabs.
- c) You can also view the status of last synced date and time.

Step 12 Click **Submit**, to migrate all the Location Groups, Devices, Maps and CMX from Prime Infrastructure to Cisco DNA Center.

Step 13 Click **Force Sync** to push data to Cisco DNA Center server after the first migration.

Note When you migrate to eWLC from the Prime Infrastructure-Cisco DNA Center co-existence tool, the eWLC support aided for Cisco DNA Center 1.2.8 and above moves the WLC to Cisco DNA Center and the devices to the collection failure sync state on Netconf feature failure. This is because the eWLC support expects you to enter a value for the **Netconf Port** field so as to be managed by Cisco DNA Center. You can manage the eWLC manually by entering a value for the **Netconf Port** field in Cisco DNA Center and then re-sync.



CHAPTER 5

Maintain Prime Infrastructure Server Health

- [Overview Dashboard, on page 97](#)
- [Performance Dashboard, on page 98](#)
- [Admin Dashboard, on page 98](#)
- [How to Evaluate OVA Size and System Resources, on page 99](#)
- [How to Improve the Performance of Prime Infrastructure, on page 101](#)
- [Optimize Memory for Assurance Processing, on page 106](#)
- [Manage Data Sources, on page 108](#)
- [Special Administrative Tasks, on page 110](#)
- [How to Update Prime Infrastructure With Latest Software Updates, on page 122](#)
- [How to Configure Support Request Settings, on page 127](#)
- [How to Manage Disk Space Issues, on page 128](#)

Overview Dashboard

The following table describes the information displayed on the **Administration > Dashboards > System Monitoring Dashboard > Overview** dashboard.

Table 7: Administration Dashboards System Monitoring Dashboard Overview Information

To view this information...	See this dashlet
PI server's hardware and software server details.	System Information
The trend over time in CPU/Memory/Disk utilization	Live Trend Information
Status of the data cleanup jobs over the selected period.	Data Cleanup
Status of backup jobs, available server backups, and alarms on server backup over the selected period.	Backup Information
Total memory and swap memory utilization displaying the set threshold limit. Also provides information on threads utilizing the memory when the threshold is breached.	Memory Utilization
CPU utilization and the set threshold limit. Also provides information on the processes and the jobs running in Prime Infrastructure that consumes more CPU when the threshold is breached.	CPU Utilization
Disk utilization and the set threshold limit. Also provides information on the files and the tablespaces using the disk when the threshold is breached.	Disk Utilization

To view this information...	See this dashlet
Available disk space.	Disk Statistics
The successful restore information over the selected period, the backup name and the restoration time.	Restore Information

Choose **Administration > System Settings > System Event Configuration** to set the threshold limit for CPU/Disk/Memory utilization and to configure the alarm generation and clearance monitor settings.

Related Topics

[Performance Dashboard](#), on page 98

[Admin Dashboard](#), on page 98

Performance Dashboard

The following table describes the information displayed on the **Administration > Dashboards > System Monitoring Dashboard > Performance Performance** dashboard.

Table 8: Administration Dashboards System Monitoring Dashboard Performance Information

To view this information...	See this dashlet
Incoming syslogs over the set collection time frame.	Syslog
Incoming traps over the set collection time frame.	Trap
Disk read and write over the set collection time frame.	System Disk Throughput
Number of read/write requests that were issued to the server per second.	System Disk IOPS
Number of requests waiting in the server queue.	System Disk Outstanding I/O
The speed at which data is currently being transferred based on the traffic flowing through available network interfaces such as eth0, eth1, and I/O interfaces.	Network Interface Traffic
Collective information on the CPU usage, disk usage, and memory usage.	Composite View

Admin Dashboard

The following table describes the information displayed on the **Administration > Dashboards > System Monitoring Dashboard > Admin** dashboard.

Table 9: Administration Dashboards System Monitoring Dashboard Admin Information

To view this information...	Choose this tab...	And see this dashlet
Alarms and events issued against the Prime Infrastructure server itself, including a list of events, times events occurred, and their severities.	Health	System Alarms
General health statistics for the Prime Infrastructure server, such as the number of jobs scheduled and running, the number of supported MIB variables, how much polling the server is doing, and the number of users logged in.		System Information
The relative proportion of the Prime Infrastructure server database taken up by data on discovered device inventory (“Lifecycle Clients”), their current status and performance data (“Lifecycle Statistics”), and the server’s own system data (“Infrastructure” and “DB-Index”)		DB Usage Distribution
How quickly the Prime Infrastructure server is responding to user service requests for information, such device reachability, alarms and events, and so on. Shows the maximum, minimum, and average response times for each API underlying a client service.	API Health	API Response Time Summary
The trend over time in how quickly the Prime Infrastructure server is responding to user service requests.	Service Details	API Response Time Trend
The activity level for each of the logged-in Prime Infrastructure users, measured by the number of service requests each is generating.		API Calls Per Client Chart
The trend over time in the total number of service requests logged-in clients are generating,		API Request Count Trend

How to Evaluate OVA Size and System Resources

Your Prime Infrastructure system implementation should match the recommendations on appropriate OVA sizes given in the “System Requirements” section of the [Cisco Prime Infrastructure Quick Start Guide](#) (see Related Topics).

Note that the limits on devices, interfaces, and flow records given in the *Quick Start Guide* are all maximums; an OVA of a given size has been tuned to handle *no more than* this number of devices, interfaces, and flows per second. Also note that the system requirements for RAM, disk space, and processors are all minimums; you can increase any of these resources and either store more data for a longer period, or process incoming flows more quickly.

As your network grows, you will approach the maximum device/interface/flow rating for your OVA. You will want to check on this from time to time. You can do so using the information available to you on the Admin dashboards, as explained in “Monitoring Prime Infrastructure Health”.

If you find Prime Infrastructure is using 80 percent or more of your system resources or the device/interface/flow counts recommended for the size of OVA you have installed, we recommend that you address this using one or more of the following approaches, as appropriate for your needs:

- Recover as much existing disk space as you can, following the instructions in “Compacting the Prime Infrastructure Database”.
- Add more disk space—VMware OVA technology enables you to easily add disk space to an existing server. You will need to shut down the Prime Infrastructure server and then follow the instructions provided by VMware to expand the physical disk space (see “VMware vSphere Documentation” in Related Topics). Once you restart the virtual appliance, Prime Infrastructure automatically makes use of the additional disk space.
- Limit collection—Not all data that Prime Infrastructure is capable of collecting will be of interest to you. For example, if you are not using the system to report on wireless radio performance statistics, you need not collect or retain that data, and can disable the Radio Performance collection task. Alternatively, you may decide that you need only the aggregated Radio Performance data, and can disable retention of raw performance data. For details on how to do this, see “Specifying Data Retention by Category”.
- Shorten retention—Prime Infrastructure defaults set generous retention periods for all of the data it persists and for the reports it generates. You may find that some of these periods exceed your needs, and that you can reduce them without negative effects. For details on this approach, see “Controlling Report Storage and Retention”, “Specifying Data Retention by Category”, and “Specifying Data Retention By Database Table.”
- Off load backups and reports—You can save space on the Prime Infrastructure server by saving reports and backups to a remote server. For details, see “Using Remote Backup Repositories”.
- Migrate to a new server—Set up a new server that meets at least the minimum RAM, disk space, and processor requirements of the next higher level of physical or virtual appliance. Back up your existing system, then restore it to a virtual machine on the higher-rated server. For details, see “Migrating to Another OVA Using Backup and Restore”.

For more details, see "[System Requirements](#)", "[Cisco Prime Infrastructure Quick Start Guide](#)" and, "[VMware vSphere Documentation](#)".

Related Topics

[Overview Dashboard](#), on page 97

[Compact the Prime Infrastructure Database](#), on page 102

[How Data Retention Settings Affect Web GUI Data](#), on page 131

[Specify Data Retention By Database Table](#), on page 134

[Control Report Storage and Retention](#), on page 136

[Use a Remote Backup Repository](#), on page 51

[Migrate to Another Virtual Appliance Using Backup and Restore](#), on page 60

View the Number of Devices Prime Infrastructure Is Managing

To check the total number of devices and interfaces that Prime Infrastructure is managing, choose **Administration > Licenses and Software Updates > Licenses**.

To check the total system disk space usage, choose **Administration > Settings > Appliance**, then click the **Appliance Status** tab. Then under **Inventory**, expand **Disk Usage**.

Related Topics

[How to Evaluate OVA Size and System Resources](#), on page 99

[How to Improve the Performance of Prime Infrastructure](#), on page 101

How to Improve the Performance of Prime Infrastructure

You can improve Prime Infrastructure's speed and scalability using several techniques.

Related Topics

- [Tune the Server](#), on page 101
- [Compact the Prime Infrastructure Database](#), on page 102
- [Configure Client Performance Settings](#), on page 102
- [Optimize Memory for Assurance Processing](#), on page 106
- [Monitor Assurance Memory Allocation and Demand](#), on page 106

Tune the Server

You can improve Prime Infrastructure's performance and scalability by increasing the amount of RAM, CPU, and disk space allocated to the Prime Infrastructure server and its virtual machine (or VM).

Successful server tuning requires you to complete the following workflow:

1. Changes to the VM include a risk of failure. Take an application backup before making any changes to the VM (for details, see "Perform an Immediate Application Backup Using the Web GUI" in Related Topics).
2. Perform the resource modifications in the VM, then restart the VM and the server (see "Modify VM Resource Allocation Using VMware vSphere Client").

Related Topics

- [Modify VM Resource Allocation Using VMware vSphere Client](#), on page 101
- [How to Improve the Performance of Prime Infrastructure](#), on page 101
- [Perform an Immediate Application Backup Using the Web GUI](#), on page 56

Modify VM Resource Allocation Using VMware vSphere Client

Use the following steps to make changes to the virtual appliance RAM, CPU or disk space resource allocations.

Be sure to back up the Prime Infrastructure server before attempting these types of changes (see "Backing Up and Restoring Prime Infrastructure" in Related Topics).

Please note that Compliance Services features will not work if you expand the RAM, CPU or disk space resource allocations after installation.



Tip For better performance: If you are changing RAM and CPU resource allocations for the virtual machine on which you run Prime Infrastructure, and you have more than one virtual machine running on the same hardware, you may also want to change your RAM and CPU resource *reservations* using the vSphere Client's **Resource Allocation** tab. For details, see "VMware vSphere documentation" in Related Topics.

-
- Step 1** Open a CLI session with the Prime Infrastructure server (see "Connecting Via CLI").
 - Step 2** Stop Prime Infrastructure using the **ncs stop** command (see "Stopping Prime Infrastructure").
 - Step 3** Halt the VMware virtual appliance:

```
PIServer/admin# halt
```

- Step 4** Launch the vSphere Client, right-click the virtual appliance, then click **Edit Settings**.
- Step 5** To change the RAM allocation, select **Memory** and change the **Memory Size** as needed. Then click **OK**.
- Step 6** To change the CPU allocation, select **CPUs** and select the **Number of Virtual Processors** from the drop-down list. Then click **OK**.
- Step 7** To add a new disk (you cannot expand the space of the existing disk):
- Click **Add**.
 - Select **Hard Disk**, then click **Next**.
 - Check **Create a new virtual disk**, then click **Next**.
 - Enter the desired **Disk Size** and specify a **Location** for the new virtual disk, then click **Next**.
 - With the Advanced Options displayed, click **Next**, then click **Finish**.
- Step 8** Power on the virtual appliance (see “Restarting Prime Infrastructure”)
- For more details, see "Backing Up and Restoring Prime Infrastructure" and [VMware vSphere Documentation](#).

Related Topics

- [How to Connect Via CLI](#), on page 111
- [Stop Prime Infrastructure](#), on page 113
- [Restart Prime Infrastructure Using CLI](#), on page 113
- [How to Improve the Performance of Prime Infrastructure](#), on page 101

Compact the Prime Infrastructure Database

You can reclaim disk space by compacting the Prime Infrastructure database.

- Step 1** Open a CLI session with the Prime Infrastructure server (see “How to Connect Via CLI” in related topics).
- Step 2** Enter the following command to compact the application database:
- ```
PIServer/admin# ncs cleanup
```
- Step 3** When prompted, answer **Yes** to the deep cleanup option.

---

#### Related Topics

- [How to Connect Via CLI](#), on page 111
- [How to Improve the Performance of Prime Infrastructure](#), on page 101

## Configure Client Performance Settings

You can configure many client processes to improve Prime Infrastructure performance and scalability (see Related Topics).

#### Related Topics

- [Enable Automatic Client Troubleshooting](#), on page 103
- [Enable DNS Hostname Lookup](#), on page 103
- [Specify How Long to Retain Client Association History Data](#), on page 104

- [Poll Clients When Receiving Client Traps/Syslogs](#), on page 104
- [Save Client Traps as Events](#), on page 105
- [Save 802.1x and 802.11 Client Traps as Events](#), on page 105
- [How to Improve the Performance of Prime Infrastructure](#), on page 101

## Enable Automatic Client Troubleshooting

The **Administration > Settings > System Settings > Client and User > Client** page allows you to enable automatic client troubleshooting on a diagnostic channel for your third-party wireless clients running Cisco Compatible Extensions (CCX).

With this feature enabled, Prime Infrastructure will process the client ccx test-association trap that invokes a series of tests on each CCX client. Clients are updated on all completed tasks, and an automated troubleshooting report is produced (it is located in dist/acs/win/webnms/logs). When each test is complete, the location of the test log is updated in the client details pages, in the V5 or V6 tab, in the Automated Troubleshooting Report area. Click **Export** to export the logs.

When this feature is not enabled, Prime Infrastructure still raises the trap, but automated troubleshooting is not initiated.

Automatic client troubleshooting is only available for clients running CCX Version 5 or 6. For a list of CCX-certified partner manufacturers and their CCX client devices, see the Cisco Compatible Extensions Client Devices page, linked under Related Topics, below.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Client**. The Client page appears.
  - Step 2** In the **Process Diagnostic Trap** area, select the Automatically troubleshoot client on diagnostic channel check box, then click **Save**. For more details, see [Cisco Compatible Extensions Client Devices page](#).

---

### Related Topics

- [Configure Client Performance Settings](#), on page 102
- [How to Improve the Performance of Prime Infrastructure](#), on page 101

## Enable DNS Hostname Lookup

DNS lookup can take a considerable amount of time, so Prime Infrastructure has it disabled by default.

You can enable or disable the DNS lookup for client hostnames, and change how long Prime Infrastructure retains the results of previous DNS lookups in its cache.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Client**.
  - Step 2** Select the Lookup client host names from DNS server check box.
  - Step 3** Enter the number of days that you want the hostname to remain in the cache, then click **Save**.

---

### Related Topics

- [Configure Client Performance Settings](#), on page 102
- [How to Improve the Performance of Prime Infrastructure](#), on page 101

## Specify How Long to Retain Client Association History Data

Client association history can take a lot of database and disk space. This can be an issue for database backup and restore functions. The retention duration of client association history can be configured to help manage this potential issue.

---

**Step 1** Choose **Administration > Settings > System Settings > Client and User > Client**.

**Step 2** Under Data Retention, change the following parameters as needed:

- **Dissociated Clients**—Enter the number of days that you want Prime Infrastructure to retain the data. The valid range is 1 to 30 days.
- **Client session history**—Enter the number of days that you want Prime Infrastructure to retain the data. The valid range is 7 to 365 days.
- **Number of Rows To Keep**—Enter the maximum number of client session records to maintain. The default is 8,000,000.

**Step 3** Click **Save**.

---

### Related Topics

[Configure Client Performance Settings](#), on page 102

[How to Improve the Performance of Prime Infrastructure](#), on page 101

## Poll Clients When Receiving Client Traps/Syslogs

Under normal circumstances, Prime Infrastructure polls clients on a regular schedule, every few minutes, identifying session information during the poll. You can also choose to have Prime Infrastructure poll clients immediately whenever traps and syslogs are received from them. This helps you discover new clients and their sessions quickly.

This option is disabled by default, as it can affect Prime Infrastructure performance. Busy networks with many clients can generate large amounts of traps and syslogs, especially during peak periods when clients are roaming and associating/disassociating often. In this case, polling clients every time you receive a trap or syslog may be an unnecessary processing burden.

If you enable the Wireless Polling Clients when Receiving Client Traps/Syslogs option, Prime Infrastructure enables Client Authentication, Client Deauthentication, and Client Disassociate Traps on the WLC even if you previously disabled the traps on the WLC. Prime Infrastructure triggers the WLC Sync operation, which enables the client traps on WLC.

---

**Step 1** Choose **Administration > Settings > System Settings > Client**.

**Step 2** Select the Poll clients when client traps/syslogs received check box. Prime Infrastructure will poll clients as soon as a trap or syslog is received, to identify client sessions.

**Step 3** Click **Save**.

---

### Related Topics

[Configure Client Performance Settings](#), on page 102

[How to Improve the Performance of Prime Infrastructure](#), on page 101

## Save Client Traps as Events

In some deployments, Prime Infrastructure might receive large amounts of client association and disassociation traps. Saving these traps as events can cause slow server performance. In addition, other events that might be useful could be aged out sooner than expected because of the amount of traps being saved.

Follow the steps below to ensure that Prime Infrastructure does not save client association and disassociation traps as events.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client**.
  - Step 2** Unselect the **Save client association and disassociation traps as events check box**.
  - Step 3** Click **Save** to confirm this configuration change. This option is disabled by default.

---

### Related Topics

- [Configure Client Performance Settings](#), on page 102
- [How to Improve the Performance of Prime Infrastructure](#), on page 101

## Save 802.1x and 802.11 Client Traps as Events

You must enable **Save 802.1x and 802.11 client authentication failed traps as events** for debugging purposes.

- 
- Step 1** Choose **Administration > Settings > System Settings > Client**.
  - Step 2** Select the **Save 802.1x and 802.11 client authentication fail traps as events** check box.
  - Step 3** Click **Save** to confirm this configuration change.

---

### Related Topics

- [Configure Client Performance Settings](#), on page 102
- [How to Improve the Performance of Prime Infrastructure](#), on page 101

## Enable Enhanced Client Traps

To enable enhanced client traps:

- 
- Step 1** Choose **Administration > Settings > System Settings > Client and User > Client**.
  - Step 2** Select the **Discover Clients from enhanced client traps** check box.
  - Step 3** Make sure that the Prime Infrastructure server is registered as a Trap receiver on Cisco WLC for receiving Client traps. The following trap flags need to be enabled on the devices for enhanced client trap to work:
    - config trapflags client enhanced-802.11-associate enable
    - config trapflags client enhanced-802.11-deauthenticate enable
    - config trapflags client enhanced-authentication enable
    - config trapflags client enhanced-802.11-stats enable

**Step 4** To log the incoming enhanced client traps on the Prime Infrastructure side, you can enable client trap logging via ssh to root shell. This generates clientTraps.log file under the /opt/CSCOLumos/logs file.

- /opt/CSCOLumos/bin/setLogLevel.sh com.cisco.client.traps TRACE

**Note** Enhanced clients traps from Prime Infrastructure is supported from WLC version 8.0 onwards.

## Optimize Memory for Assurance Processing

Prime Infrastructure's Assurance features depend heavily on high-volume NetFlow data forwarded to the Prime Infrastructure server by devices, including NAMs. Because Prime Infrastructure always aggregates NetFlow data before storing it, supporting Assurance features with appropriate data is a memory-intensive process.

With more working memory to hold NetFlow data during aggregation, Prime Infrastructure can get this job done faster and more efficiently. This can lead to important performance improvements if your organization licenses Assurance features and makes heavy use of them.

Prime Infrastructure offers features to help you:

- Determine how much memory is currently allocated to Assurance-related data processing, and how completely individual Assurance features are using that memory pool.
- Increase the default pool of memory used to process Assurance-related data.
- Balance the memory allocated to individual Assurance features, so those with the greatest demand for memory get what they need.

The amount of performance improvement you can get from using these features depends on the memory available and how you use Assurance features, but can be substantial. For example: Given a Prime Infrastructure Professional implementation with the recommended minimum hardware Prime Infrastructure can process up to 414,000 NetFlow host records in a single five-minute aggregation cycle. With Assurance memory optimization, maximum processing for the same type of data is closer to 800,000 records per cycle.

You can increase the Assurance memory pool without balancing Assurance memory allocations, and vice versa. But using these two optimization options together is the best way to improve Prime Infrastructure performance when Assurance features are used.

### Related Topics

[Monitor Assurance Memory Allocation and Demand](#), on page 106

[Increase the Assurance Memory Pool Via CLI](#), on page 107

[How to Balance the Assurance Memory Allocation](#), on page 107

[Reset Assurance Memory Allocation](#), on page 108

[Reset the Assurance Memory Pool](#), on page 108

## Monitor Assurance Memory Allocation and Demand

You can quickly see Prime Infrastructure's current Assurance-related memory allocation and usage.

**Step 1** Select **Services > Application Visibility & Control > Data Sources**.

- Step 2** Select the text link **Assurance Memory Statistics** (in the upper right corner of the page). Prime Infrastructure displays:
- The current memory allocation in megabytes for each of the main Assurance feature categories, including Traffic, Performance Routing, Applications, Voice-Video data, Device Health, Lync and other data.
  - The usage of each area’s memory allocation over the last 24 hours. The percentage represents the peak memory usage over that period (that is, if 100 percent of the memory allocation is used at any point in the past 24 hours, the usage percentage shown will be 100 percent).

---

#### Related Topics

- [Optimize Memory for Assurance Processing](#), on page 106
- [Increase the Assurance Memory Pool Via CLI](#), on page 107
- [How to Balance the Assurance Memory Allocation](#), on page 107

## Increase the Assurance Memory Pool Via CLI

You can use the Prime Infrastructure command line to allocate more memory to all types of Assurance-related data processing. Note that using the **ncs tune-resources assurance** command requires a server restart. Once restarted, the server will increase the total pool of memory allocated to all Assurance-related data processing.

- 
- Step 1** Open a CLI session with the Prime Infrastructure server (see “How to Connect Via CLI”).
- Step 2** Enter the following command:
- ```
PIServer/admin# ncs tune-resources assurance
```
- Step 3** Restart the Prime Infrastructure server (see “Restart Prime Infrastructure”).

Related Topics

- [How to Connect Via CLI](#), on page 111
- [Restart Prime Infrastructure Using CLI](#), on page 113
- [Optimize Memory for Assurance Processing](#), on page 106

How to Balance the Assurance Memory Allocation

You can use the Prime Infrastructure interface to automatically balance the allocation of the total Assurance memory pool to individual categories of Assurance-related data processing, ensuring that those Assurance features that need memory the most are getting it.

-
- Step 1** Select **Services > Application Visibility & Control > Data Sources**.
- Step 2** Select the text link **Assurance Memory Statistics** (in the upper right corner of the Data Sources page).
- Step 3** Click **Rebalance**.
- Prime Infrastructure will change Assurance memory allocations to individual features as needed, reducing allocations for less-used features and increasing allocations for features where usage over the past 24 hours was at or near 100 percent.
-

Related Topics

[Optimize Memory for Assurance Processing](#), on page 106

Reset Assurance Memory Allocation

You can use the Prime Infrastructure interface to cancel Assurance memory balancing, returning the allocation for each Assurance-related feature to its default value.

-
- Step 1** Select **Services > Application Visibility & Control > Data Sources**.
 - Step 2** Select the text link **Assurance Memory Statistics** (in the upper right corner of the Data Sources page).
 - Step 3** Click **Reset**.

Related Topics

[Optimize Memory for Assurance Processing](#), on page 106

Reset the Assurance Memory Pool

You can use the Prime Infrastructure command line to return the Assurance memory pool to the default allocation, disabling all changes created using the **ncs tune-resources assurance** command explained in “Increase the Assurance Memory Pool Via CLI”.

-
- Step 1** Open a CLI session with the Prime Infrastructure server (see “How to Connect Via CLI”).
 - Step 2** Enter the following command:

```
PIServer/admin# ncs tune-resources default
```
 - Step 3** Restart the Prime Infrastructure server (see “Restart Prime Infrastructure”).

Related Topics

[Increase the Assurance Memory Pool Via CLI](#), on page 107
[How to Connect Via CLI](#), on page 111
[Restart Prime Infrastructure Using CLI](#), on page 113
[Optimize Memory for Assurance Processing](#), on page 106

Manage Data Sources

Prime Infrastructure 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.

For details on the data sources used in dashlets, see “Advanced Monitoring” in Related Topics. For details on setting up individual data sources, see the data-source configuration sections of “Administrator Setup Tasks”, also listed in Related Topics.

Related Topics

- [View Current Data Sources](#), on page 109
- [Delete Data Sources](#), on page 110
- [Advanced Monitoring](#)
- [Administrator Setup Tasks](#), on page 4
- [Configure Data Sources for With Assurance](#), on page 9
- [Enable Medianet NetFlow](#), on page 11
- [Enable NetFlow and Flexible NetFlow](#), on page 13
- [Deploy Network Analysis Modules NAMs](#), on page 14
- [Enable Performance Agent](#), on page 15

View Current Data Sources

Use the Data Sources page to review Prime Infrastructure’s current data sources. Access to this page requires administrator privileges

Select **Services > Application Visibility & Control > Data Sources**. Prime Infrastructure displays a summary page that lists each device 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 Prime Infrastructure (e.g., “Netflow”).
- **Exporting Device**—The IP address of the device exporting the data to Prime Infrastructure.
- **Last 5 min Flow Read Rate**—The amount of data Prime Infrastructure has received from this source during the last five minutes.
- **Last Active Time**—The latest date and time that Prime Infrastructure received data from this source.

For each Cisco NAM data collector sources, the page lists:

- **Name**—The host name of the NAM.
- **Type**—The type of data the NAM is collecting and sending to Prime Infrastructure (e.g., “Cisco Branch Routers Series Network Analysis Module”).
- **Host IP Address**—The IP address of the NAM.
- **Data Usage in System**—Whether the data forwarded by this NAM is enabled for use in Prime Infrastructure.
- **Last Active Time**—The latest date and time that Prime Infrastructure received data from this NAM.

Related Topics

- [Special Administrative Tasks](#), on page 110

[Delete Data Sources](#), on page 110

Delete Data Sources

Use the Data Sources page to delete inactive Prime Infrastructure data sources. Access to this page requires administrator privileges.

Note that you cannot delete a NetFlow data source until seven full days have elapsed without receipt of any data from that data source. This delay helps protect the integrity of NetFlow data (which Prime Infrastructure identifies and aggregates according to the source) by giving network operators a full week to ensure that the data source has been retired. If the source remains active during that period and sends data to Prime Infrastructure, data from that source will still be identified and aggregated properly with other data from the same source (instead of being identified as a new source).

-
- Step 1** Select **Services > Application Visibility & Control > Data Sources**.
- Step 2** Select the checkbox next to the inactive data source you want to delete.
- Step 3** Click **Delete**.
- Step 4** Click **OK** to confirm the deletion.
-

Related Topics

- [Special Administrative Tasks](#), on page 110
- [View Current Data Sources](#), on page 109

Special Administrative Tasks

Prime Infrastructure provides administrators with special access in order to perform a variety of infrequent tasks, including

- Connecting to the server via an SSH command-line interface (CLI) session.
- Changing server hardware setup and resource allocations.
- Starting, stopping, and checking on the status of Prime Infrastructure services.
- Running Prime Infrastructure processes accessible only via the CLI.
- Managing access rights, including changing passwords for user IDs with special tasks.
- Removing or resetting Prime Infrastructure.

Related Topics

- [How to Connect Via CLI](#), on page 111
- [Start Prime Infrastructure](#), on page 111
- [Check Prime Infrastructure Server Status](#), on page 112
- [Check Prime Infrastructure Version and Patch Status](#), on page 112
- [Stop Prime Infrastructure](#), on page 113
- [Restart Prime Infrastructure Using CLI](#), on page 113
- [How to Remove Prime Infrastructure](#), on page 114
- [Reset Prime Infrastructure to Defaults](#), on page 114
- [Change the Prime Infrastructure Host Name](#), on page 115
- [Enable the FTP User](#), on page 115

[Change the Root User Password](#), on page 116

[How to Recover Administrator Passwords on Virtual Appliances](#), on page 117

[How to Recover Administrator Passwords on Physical Appliances](#), on page 118

[How to Get the Installation ISO Image](#), on page 121

[Check High Availability Status](#), on page 277

How to Connect Via CLI

Administrators can connect to the Prime Infrastructure server via its command-line interface (CLI). CLI access is required when you need to run commands and processes accessible only via the Prime Infrastructure CLI. These include commands to start the server, stop it, check on its status, and so on.

Before you begin

Before you begin, make sure you:

- Know the user ID and password of an administrative user with CLI access to that server or appliance. Unless specifically barred from doing so, all administrative users have CLI access.
- Know the IP address or host name of the Prime Infrastructure server.

Step 1 Start up your SSH client, start an SSH session via your local machine's command line, or connect to the dedicated console on the Prime Infrastructure physical or virtual appliance.

Step 2 Log in as appropriate: If you are using a GUI client: Enter the ID of an active administrator with CLI access and the IP address or host name of the Prime Infrastructure server. Then initiate the connection. If you are using a command-line client or session: Log in with a command like the following: `[localhost]# ssh username@IPHost` -Where username is the user ID of a Prime Infrastructure administrator with CLI access to the server. IPHost is the IP address or host name of the Prime Infrastructure server or appliance. If you are using the console: A prompt is shown for the administrator user name. Enter the user name.

Prime Infrastructure will then prompt you for the password for the administrator ID you entered.

Step 3 Enter the administrative ID password. Prime Infrastructure will present a command prompt like the following: `PIServer/admin#`.

Step 4 If the command you need to enter requires that you enter "configure terminal" mode, enter the following command at the prompt:

```
PIServer/admin# configure terminal
```

The prompt will change from `PIServer/admin#` to `PIServer/admin/conf#`.

Related Topics

[Special Administrative Tasks](#), on page 110

Start Prime Infrastructure

To start Prime Infrastructure:

Step 1 Open a CLI session with the Prime Infrastructure server (see "How to Connect Via CLI").

Step 2 Enter the following command to start the Prime Infrastructure server or appliance:

```
PIServer/admin# ncs start
```

Related Topics

- [How to Connect Via CLI](#), on page 111
- [Stop Prime Infrastructure](#), on page 113
- [Restart Prime Infrastructure Using CLI](#), on page 113
- [Special Administrative Tasks](#), on page 110

Check Prime Infrastructure Server Status

You can check on the status of all Prime Infrastructure server or appliance processes at any time, without stopping the server. Technical Assistance personnel may ask you to perform this task when troubleshooting a problem with Prime Infrastructure.

You can also check on the current health of the server using the dashlets on the Admin Dashboard (see “Monitoring Prime Infrastructure Health”).

You can check on the status of High Availability options enabled on the server using the command **ncs ha status** (see “Checking High Availability Status”).

Step 1 Open a CLI session with the Prime Infrastructure server (see “Connecting Via CLI”).

Step 2 Enter the following command to display the current status of Prime Infrastructure processes and services:

```
PIServer/admin# ncs status
```

For more details, see "Checking High Availability Status".

Related Topics

- [How to Connect Via CLI](#), on page 111
- [Overview Dashboard](#), on page 97
- [Special Administrative Tasks](#), on page 110

Check Prime Infrastructure Version and Patch Status

You can check on the version of a Prime Infrastructure server and the patches applied to it at any time, without stopping the server. You will usually need to do this when upgrading or patching the server software.

Step 1 Open a CLI session with the Prime Infrastructure server (see “How to Connect via CLI”).

Step 2 Enter the following command to display the current status of Prime Infrastructure processes and services:

```
PIServer/admin# show version
```

Related Topics

- [How to Connect Via CLI](#), on page 111

[Special Administrative Tasks](#), on page 110

Stop Prime Infrastructure

You can stop a Prime Infrastructure server or appliance at any time using the command line interface. Any users logged in at the time you stop Prime Infrastructure will have their sessions stop functioning.

Step 1 Open a CLI session with the Prime Infrastructure server (see “How to connect via CLI”).

Step 2 Enter the following command to stop the Prime Infrastructure server or appliance:

```
PIServer/admin# ncs stop
```

Related Topics

[How to Connect Via CLI](#), on page 111

[Special Administrative Tasks](#), on page 110

Restart Prime Infrastructure Using CLI

Step 1 Open a CLI session with the Prime Infrastructure server (see “How to Connect via CLI”).

Step 2 Enter the following command to stop the Prime Infrastructure server or appliance:

```
PIServer/admin# ncs stop
```

Step 3 Wait for the previous command to complete.

Step 4 Enter the following command to restart the Prime Infrastructure server or appliance:

```
PIServer/admin# ncs start
```

Related Topics

[How to Connect Via CLI](#), on page 111

[Special Administrative Tasks](#), on page 110

[Restart Prime Infrastructure Using GUI](#), on page 113

Restart Prime Infrastructure Using GUI

To restart the server from the server GUI, do the following.

Before you begin

You must have Root or Super User privilege to restart the server using GUI.

Step 1 Choose **Administration > System Settings > Server**.

Step 2 Click **Restart Prime Infrastructure**.

Step 3 Check the Restart acknowledgment check box in the pop-up window and click **Restart**.

Related Topics

[Restart Prime Infrastructure Using CLI](#), on page 113

How to Remove Prime Infrastructure

You may need to remove Prime Infrastructure in preparation for a clean “from scratch” re-installation. You can do so by following the steps below

Note that this procedure will delete all your existing data on the server, including all server settings and local backups. You will be unable to restore your data unless you have a remote backup or access to disk-level data recovery methods.

-
- Step 1** Stop the server (see “Stop Prime Infrastructure”).
- Step 2** In the VMware vSphere client, right-click the Prime Infrastructure virtual appliance.
- Step 3** Power off the virtual appliance.
- Step 4** Right click on the powered-off virtual appliance and select **Delete from Disk option**.

Related Topics

[Stop Prime Infrastructure](#), on page 113

[Special Administrative Tasks](#), on page 110

Reset Prime Infrastructure to Defaults

You may need to reset the installed Prime Infrastructure server to factory defaults, removing all user data and customizations, but preserving the installation itself. You can do so by following the steps below.

Note that this procedure will delete all your existing data on the server host except for the default settings supplied with Prime Infrastructure. You will be unable to restore your data unless you have a remote backup or access to disk-level data recovery methods.

-
- Step 1** Stop the server (see “Stop Prime Infrastructure”).
- Step 2** Download the installation ISO image appropriate for your installed version of the Prime Infrastructure virtual or physical appliance server software and burn it to DVD (see “How to Get the Installation ISO Image”).
- Step 3** Power off the virtual appliance.
- Step 4** Reinstall the appliance or OVA by booting the host from the DVD.

Related Topics

[Stop Prime Infrastructure](#), on page 113

[How to Get the Installation ISO Image](#), on page 121

[Special Administrative Tasks](#), on page 110

Change the Prime Infrastructure Host Name

Prime Infrastructure prompts you for a host name when you install the server. For a variety of reasons, you may find there is a mismatch between the host name on the Prime Infrastructure server and the host name elsewhere. If so, you can recover without reinstalling by changing the host name on the server.

Step 1 Open a CLI session with the Prime Infrastructure server (see “How to Connect Via CLI”). Be sure to enter “configure terminal” mode.

Step 2 Enter the following command:

```
PIServer/admin(config)# hostname newHostName
```

Where *newHostName* is the new host name you want to assign to the Prime Infrastructure server.

Step 3 Restart the Prime Infrastructure server using the **ncs stop** and **ncs start** commands, as explained in "Restart Prime Infrastructure" .

Related Topics

[How to Connect Via CLI](#), on page 111

[Restart Prime Infrastructure Using CLI](#), on page 113

[Special Administrative Tasks](#), on page 110

Enable the FTP User

To use Prime Infrastructure as an FTP server for file transfers and software image management, an administrator must configure an FTP account. Use the steps below to enable the account and set a password for it.

After you enable the ftp-user, you can FTP files to and from the /localdisk/ftp folder on standalone or, if configured, High Availability primary servers only. You cannot use change directory (cd) or list directory (ls) functionality with ftp-user.

Step 1 Open a CLI session with the Prime Infrastructure server (see “How to Connect Via CLI”).

Step 2 Enter the following command:

```
PIServer/admin#ncs password ftpuser ftp-user password password
```

Where:

- **ftp-user** is the username for FTP operation.
- **password** is the login password for **ftp-user**.

Note The username for FTP must be **ftp-user**.

For example:

```
pi-system-999/admin# ncs password ftpuser root password MyPassword
```

Updating FTP password.

Saving FTP account password in credential store

Syncing FTP account password to database store - location-ftp-user

Syncing FTP account password to system store

Completed FTP password update

pi-system-999/admin#

Related Topics

[How to Connect Via CLI](#), on page 111

[Special Administrative Tasks](#), on page 110

Change the Root User Password

Administrators can change the password associated with this special administrative ID.

Step 1 Open a CLI session with the Prime Infrastructure server (see “How to Connect Via CLI”) in Related Topics.

Step 2 Enter the following command:

```
PIServer/admin# ncs password root password password
```

Where *password* is the root user login password. You can enter a password not exceeding 80 characters.

For example:

```
PIServer/admin# ncs password root password #password#
```

```
pi-system-198/admin# ncs password root password #password#
```

Password updated for web root user

```
pi-system-198/admin#
```

Related Topics

[How to Connect Via CLI](#), on page 111

[Special Administrative Tasks](#), on page 110

Change the Admin Password using CLI

A new Cli command “change-password” is introduced. Using this user can change their own passwords. This command is available for all roles.

The following CLI users roles are applicable:

- Super-user (admin): Only one super-user is allowed which is created during the initial setup.
- Security-admin: Has highest privilege after super user.
- Network-admin: Has privileges to do network related configuration
- User: Has privileges for read only permissions.

Step 1 Open a CLI session with the Prime Infrastructure.

Step 2 Enter the following command:

```
pi-cluster-54/admin# change-password
```

Changing password for user admin
Changing password for admin.
(current) UNIX password

Note When upgrading from previous 3.5 releases:

- User with name "admin" is converted to Super-user (admin).
- Users name which does not contain "admin" account from which upgrade is performed gets converted to super-user(admin).
- All the other admin users are converted to security-admin.

How to Recover Administrator Passwords on Virtual Appliances

You can recover (that is, reset) administrator passwords on Prime Infrastructure virtual machines (also known as OVAs) installed on your own hardware.

Before you begin

Ensure that you have:

- Physical access to the Prime Infrastructure server.
- A copy of the installation ISO image appropriate for your version of the software. See “How to Get the Installation ISO Image” in Related Topics.
- Access to the VMware vSphere client, and to the vSphere inventory, Datastores and Objects functions. If you do not have such access, consult your VMware administrator. You should avoid accessing ESX directly from the vSphere client.

Step 1 Launch your VMware vSphere Client and connect to the ESXi host or vCenter server.

Step 2 Upload the installation ISO image to the data store on the OVA virtual machine, as follows:

- a) In the vSphere Server, click **Inventory > Summary > Datastores**.
- b) On the **Objects** tab, select the datastore to which you will upload the file.
- c) Click the **Navigate to the datastore file browser** icon.
- d) If needed, click the **Create a new folder** icon and create a new folder.
- e) Select the folder that you created or select an existing folder, and click the **Upload a File** icon.

If the Client Integration Access Control dialog box appears, click **Allow** to allow the plug-in to access your operating system and proceed with the file upload.

- f) On the local computer, find the ISO file and upload it.
- g) Refresh the datastore file browser to see the uploaded file in the list.

Step 3 With the ISO image uploaded to a datastore, make it the default boot image, as follows:

- a) Using the VMware vSphere client, right-click the deployed OVA and choose **Power > Power Off**.
- b) Select **Edit Settings > Hardware**, then select **CD/DVD drive 1**.
- c) Under **Device Type**, select **Datastore ISO File**, then use the **Browse** button to select the ISO image file you uploaded to the datastore.
- d) Under **Device Status**, select **Connect at power on**.
- e) Click the **Options** tab and select **Boot Options**. Under **Force BIOS Setup**, select **Next time VM boots, force entry into BIOS setup Screen**. This will force a boot from the virtual machine BIOS when you restart the virtual machine.
- f) Click **OK**.
- g) In the VMware vSphere client, right-click the deployed OVA and choose **Power > Power On**.
- h) In the BIOS setup menu, find the option that controls the boot order of devices and move **DVD/CDROM** to the top.

Step 4 Follow the steps below to reset a server administrator password:

- a) Save your BIOS settings and exit the BIOS setup menu. The virtual machine will boot from the ISO image and display a list of boot options.
- b) Enter **3** if you are using the keyboard and monitor to access the OVA, or **4** if you are accessing via command line or console. The vSphere client displays a list of administrator user names.
- c) Enter the number shown next to the administrator username for which you want to reset the password.
- d) Enter the new password and verify it with a second entry.
- e) Make sure to disconnect ISO image before confirming the changes using the vSphere client.
- f) Click the CD icon and select **Disconnect ISO image**.
- g) Enter **Y** to save your changes and reboot.

Step 5 Log in with the new administrator password.

Related Topics

- [How to Get the Installation ISO Image](#), on page 121
- [Special Administrative Tasks](#), on page 110

How to Recover Administrator Passwords on Physical Appliances

You can recover (reset) administrator passwords on Prime Infrastructure physical appliances.

Before You Begin

Ensure that you have:

- Physical access to the Prime Infrastructure appliance.
- A copy of the appliance recovery CD that was supplied with the shipped appliance.

If you have lost the appliance recovery CD, download and burn a DVD copy of the ISO image, as explained in “How to Get the Installation ISO Image”. You can then use the DVD to reset administrator passwords on the appliance (see “How to Recover Administrator Passwords on Virtual Appliances” for detailed steps).

You can reset the password using,

- **Console:** KVM Console (Other console options are VGA Console and Serial Console/Serial Over Lan-SOL)
- **DVD mount option:** KVM mapped DVD (Other mount options are CIMC mapped DVD and Physical External DVD)

See [Cisco Prime Infrastructure Hardware Installation Guide](#) for additional information.

To recover the password using KVM Console, follow these steps:

-
- Step 1** Launch Cisco Integrated Management Controller .
 - Step 2** Choose **Server > Summary** from the left navigation pane.
 - Step 3** Under **Actions**, click **Launch KVM Console**.
 - Step 4** In the console, choose **Virtual Media > Activate Virtual Devices**.
 - Step 5** Select **Accept the session** radio button and click **Apply**.
 - Step 6** In the console, choose **Virtual Media > Map CD/DVD**.
 - Step 7** Browse to the location of the Prime Infrastructure ISO image and click **Map Device**.
 - Step 8** In the console, choose **Power > Reset System(warm boot)**.
 - Step 9** A confirmation message appears. Click **Yes**.
 - Step 10** The machine reboots and prompts to enter F6 for boot option. Press the function-key **F6**.
You may need to press F6 multiple times to see **Enter boot selection menu...** in the screen. You must wait for a few minutes to get the boot device option.
 - Step 11** Select the desired DVD mount option and in this case, you must select **Cisco vKVM-Mapped vDVD1.22**.
 - Step 12** The vSphere client displays a list of boot options. Enter **3** to select the **Recover administrator password (Keyboard/Monitor)** boot option.
Note If you are using Serial Console to recover password, then you must enter **4** to select the **Recover administrator password (Serial Console)** boot option.
 - Step 13** The vSphere client displays a list of administrator user names. Enter the number shown next to the administrator user name for which you want to recover (reset) the password and press **Enter**.
 - Step 14** Enter the new password and verify it with a second entry.
 - Step 15** Enter **Y** to save your changes and reboot the system.
 - Step 16** Login to the admin CLI with the new administrator password.
Note You can follow the same steps to recover password using VGA console and Serial console.

To recover the password using Serial Console/Serial Over Lan-SOL, follow these steps:

- Step 1** Launch Cisco Integrated Management Controller server using SSH .

```
# ssh admin@(server IP)
Enter the admin password
```
- Step 2** Map the ISO image.

```
C220-FCH1840V0BL# scope vmedia
C220-FCH1840V0BL /vmedia # map-www <VOLUME_NAME> <LOCATION> <ISO_FILE>
Server username: anonymous
Server password:
Confirm password:
C220-FCH1840V0BL /vmedia # show mappings
Volume          Map-Status          Drive-Type Remote-Share          Remote-File
Mount-Type
-----
-----
```

```
<VOLUME_NAME> OK CD <LOCATION> <IMAGE_NAME> www
C220-FCH1840V0BL /vmedia #
```

Step 3 Reboot the server:

```
# scope chassis
# power off
This operation will change the server's power state.
Do you want to continue?[y|N]y
#
#
# power on
This operation will change the server's power state.
Do you want to continue?[y|N]y
# exit
```

Step 4 Connect to Serial Over Lan Console.

```
# scope sol
# show detail
Serial Over LAN:
Enabled: yes
Baud Rate(bps): 9600
Com Port: com0
# set enabled yes
# set baud-rate 9600
# commit

# connect host // to connect sol cosole
```

Step 5 The machine reboots and prompts to enter F6 for boot option. Press the function-key **F6**.

You may need to press F6 multiple times to see **Enter boot selection menu...** in the screen. You must wait for a few minutes to get the boot device option.

Step 6 Select the desired DVD mount option and in this case, you must select **Cisco CIMC-Mapped vDVD1.22**.

Step 7 The vSphere client displays a list of boot options. Enter **4** to select the **Recover administrator password (Serial Console)** boot option.

Note To recover administrator password for Gen 3 appliances, it is recommended to use Serial Over Lan (Serial console)

Step 8 The vSphere client displays a list of administrator user names. Enter the number shown next to the administrator user name for which you want to recover (reset) the password and press **Enter**.

Step 9 Enter the new password and verify it with a second entry.

Step 10 Enter **Y** to save your changes and reboot the system.

Step 11 Login to the admin CLI with the new administrator password.

How to Recover Administrator Passwords on Hyper-V Virtual Appliances

You can recover (reset) administrator passwords on Prime Infrastructure Hyper-V Virtual appliances.

Before You Begin

Ensure that you have:

- Physical access to the Prime Infrastructure appliance.
- A copy of the installation ISO image appropriate for your version of the software. See [How to Get the Installation ISO Image, on page 121](#).
- Access to the Hyper-V Machine, and to the Hyper-V manager. If you do not have the access, get help from your Hyper-V administrator.

-
- Step 1** Launch your Hyper-V Machine and make sure ISO image available in your Hyper-V Machine.
- Step 2** Connect to the Hyper-V Manager.
- a) Right-click the virtual machine for which you want to reset the password and select **Connect**. The **Virtual Machine Connection** window opens.
 - b) Choose **Media > DVD Drive > Insert Disk**.
 - c) Browse and select the ISO image.
 - d) Turn Off and Start the virtual machine as follows:
 - Choose **Action > Turn Off**.
 - Click **Turn Off** in the **Turn Off Machine** pop-up.
 - Choose **Action > Start**.
- Step 3** The virtual machine will boot from the ISO image and will display a list of boot options.
- a) Enter 3 (The option for recovering Administrator password)
 - b) Enter the number shown for the administrator username for which you want to reset the password.
 - c) Enter the new password and verify it with a second entry.
 - d) Enter Y to save your changes and reboot.
 - e) Wait until the machine gets rebooted.
- Step 4** Log in with the new administrator password.
-

How to Get the Installation ISO Image

Copies of the Prime Infrastructure installation ISO image are needed for some special maintenance operations, such as resetting administrator passwords.

Prime Infrastructure ISO image files have the format **PI-APL-*version*-K9.iso**, where **version** is the version number of the product. The version number will often contain extended numbering indicating the patch level of the product. For example: If you were using a fully-updated version of Prime Infrastructure 3.5, you would must download the **PI-APL-3.5.0.0.550-1-K9.iso** from [Cisco.com](#).

If you do not have a copy of the ISO image, you can download it from [Cisco.com](#) using the steps below:

-
- Step 1** On a browser with internet access, link to the Cisco Software Download Navigator (see Related Topics).
- Step 2** Use the **Find** box to search for “Cisco Prime Infrastructure”.
- Step 3** From the results list, select the software version you are using.

- Step 4** Select **Prime Infrastructure Software** to display the list of ISOs and other downloadable image files for that software version.
- Step 5** Download the ISO image from the page.
- Step 6** When the download is complete, check that the MD5 checksum of the downloaded file matches the checksum shown for the file on its Cisco.com download page. If the checksums do not match, the file is corrupt, and you will need to download it from Cisco.com again.
- Step 7** If you need the ISO image on disk: Burn the ISO image to a Dual Layer DVD using DVD authoring software. For reliable results, we recommend that you conduct the burn at single (1X) speed and with the “Verify” option turned on. For more details, see <https://software.cisco.com/download/navigator.html> and [Cisco Prime Infrastructure 3.5 Appliance Hardware Installation Guide](#)

Related Topics

[Special Administrative Tasks](#), on page 110

How to Update Prime Infrastructure With Latest Software Updates

Cisco provides updates to Prime Infrastructure software periodically. These updates fall into the following categories:

- **Critical Fixes**—Provide critical fixes to the software. We strongly recommend that you download and apply all of these updates as soon as they are available.
- **Device Support**—Adds support for managing devices which Prime Infrastructure did not support at release time. These updates are published on a monthly basis.
- **Add-Ons**—Provide new features, which can include new GUI screens and functionality, to supplement the Prime Infrastructure version you are using.

For details on how to find these updates, and how to get notifications when they are released, see “View Installed and Available Software Updates” in Related Topics.

The update notifications that Prime Infrastructure displays are based on the Notification Settings you specify using **Administration > Settings > System Settings > Software Update**. For details, see “Configuring Software Update Notifications”.

For details on installing these updates, see “Install Software Updates”.

For details on streamlining your software update notifications and installations using your Cisco.com account, see “How to Use Your Cisco.com Account Credentials with Prime Infrastructure”.

Related Topics

[View Installed and Available Software Updates](#), on page 122

[Configure Software Update Notifications](#), on page 123

[Install Software Updates](#), on page 125

[How to Use Your Cisco.com Account Credentials with Prime Infrastructure](#), on page 126

View Installed and Available Software Updates

Prime Infrastructure allows you to:

- Receive notifications when new software updates become available.
- Modify how and when you are notified that new software updates are available.
- View the details of each update.
- See which software updates have been installed.

The following topics explain how to perform each of these tasks.

Related Topics

- [How to Get Software Update Notifications](#), on page 123
- [Configure Software Update Notifications](#), on page 123
- [View Details of Installed Software Updates](#), on page 124
- [View Installed Updates From the Login Page](#), on page 124
- [View Installed Updates From the About Page](#), on page 124
- [How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

How to Get Software Update Notifications

When properly configured, Prime Infrastructure will notify you automatically when new software updates are available.

-
- Step 1** Choose **Administration > Settings > System settings > Account Settings**.
 - Step 2** Enter a valid Cisco.com user name and password.
 - Step 3** Click **Save**.
 - Step 4** Choose **Administration > Settings > System Settings > General > Software Update**.
 - Step 5** Under Notification Settings, select the categories for which you want updates displayed on the **Administration > Software Update** page.
 - Step 6** Click **Save**.

To see notifications: Click on the notifications icon at the top right, next to the alarms icon.

Related Topics

- [Configure Software Update Notifications](#), on page 123
- [View Installed and Available Software Updates](#), on page 122
- [How to Use Your Cisco.com Account Credentials with Prime Infrastructure](#), on page 126
- [How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

Configure Software Update Notifications

You can modify the update notifications that Prime Infrastructure displays on the **Administration > Software Update** page. For example, if you do not want to install any updates to Prime Infrastructure, you can disable all notification and prevent Prime Infrastructure from displaying notifications of available updates.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Software Update**.
 - Step 2** Under Notification Settings, select the categories for which you want updates displayed on the **Administration > Software Update** page.

Step 3 Click **Save**.

Related Topics

[View Installed and Available Software Updates](#), on page 122

[How to Get Software Update Notifications](#), on page 123

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

View Details of Installed Software Updates

Step 1 Choose **Administration Settings > Licenses and Software Updates > Software Update**.

Step 2 Click the **Updates** tab to see the Name, Type, Version, Status and Date of each installed software update.

To filter this list, click the Filter icon at the right side of the Updates tab and select the categories of installed updates you want to see.

Step 3 Click the **Files** tab to see the list of installed UBF files and downloaded UBF files which have yet to be installed.

To delete a software update file that has not yet been installed, select the file and click **Delete**.

Related Topics

[View Installed and Available Software Updates](#), on page 122

[View Installed Updates From the Login Page](#), on page 124

[View Installed Updates From the About Page](#), on page 124

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

View Installed Updates From the Login Page

Step 1 Launch or log out of Prime Infrastructure. The login page displays.

Step 2 Click **View installed updates**. Prime Infrastructure displays a popup list of the names and versions of all installed software updates.

Step 3 Click the **Close** button to close the popup list.

Related Topics

[View Installed Updates From the About Page](#), on page 124

[View Installed and Available Software Updates](#), on page 122

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

View Installed Updates From the About Page

Step 1 Click the settings icon at the upper right corner of any Prime Infrastructure page.

Step 2 Click **About Prime infrastructure**. The About page appears, listing the version of the product and other details.

Step 3 Click **View installed updates**. Prime Infrastructure displays a popup list of the names and versions of all installed software updates.

Step 4 Click the **Close** button to close the popup list.

Related Topics

[View Installed Updates From the Login Page](#), on page 124

[View Installed and Available Software Updates](#), on page 122

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

Install Software Updates

Prime Infrastructure periodically provides critical fixes, device support, and add-on updates that you can download and install by choosing **Administration > Software Update**. Depending on your connectivity and preference, you can install software updates by:

- Downloading updates directly from [cisco.com](#) to the Prime Infrastructure server.

To use this method, your Prime Infrastructure server must be able to connect externally to [Cisco.com](#). For details, see “Install Software Updates from Cisco.com” in Related Topics.

- Downloading software update files to a client or server with external connectivity,

then uploading them to and installing them on the Prime Infrastructure server. For details, see “Upload and Install Downloaded Software Updates” in Related Topics.

Related Topics

[Install Software Updates from Cisco.com](#), on page 125

[Upload and Install Downloaded Software Updates](#), on page 126

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

Install Software Updates from Cisco.com

The following steps explain how to install software updates directly from [Cisco.com](#). This procedure assumes that Prime Infrastructure has external connectivity to [Cisco.com](#) and that you want to download updates directly from [Cisco.com](#).

Step 1 Choose **Administration > Licenses and Software Updates > Software Update**.

Step 2 Click the **download** link at the top of the page to get the latest updates from [Cisco.com](#).

Step 3 Enter your [Cisco.com](#) login credentials. Prime Infrastructure lists the available updates.

If you receive an error indicating there was a problem connecting to [cisco.com](#), verify your proxy settings by choosing **Administration > Settings > System Settings > General > Account Settings > Proxy**. If your proxy settings are not working, deselect **Enable Proxy**, then click **Save**.

Step 4 Click **Show Details** to see the details about the updates.

Step 5 Click **Download** next to the update you want to install.

Step 6 After the update has been downloaded, click **Install**.

Step 7 Click **Yes** in the pop-up message. The server will restart automatically.

Step 8 When the restart is complete, choose **Administration > Licenses and Software Updates > Software Update**. The Updates table should show the update as “Installed”.

Related Topics

[Install Software Updates](#), on page 125

[Restart Prime Infrastructure Using CLI](#), on page 113

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

Upload and Install Downloaded Software Updates

The following steps explain how to upload and install software updates. This procedure is useful when your Prime Infrastructure server does not have external connectivity, or you prefer to download files on a different server.

-
- Step 1** Choose **Administration > Licenses and Software Updates > Software Update**.
- Step 2** Click the **upload** link at the top of the page.
- Step 3** On the Upload Update window, click **Cisco Download**, which displays Cisco.com’s “Download Software” page.
- Step 4** Select **Products > Cloud and Systems Management > Routing and Switch Management > Network Management Solutions > Prime Infrastructure**.
- Step 5** Select the correct version of Prime Infrastructure.
- Step 6** Select an update software type (such as “Prime Infrastructure Device Packs”).
- Step 7** From the page that appears, click **Download** next to the file containing the updates you want. The file will have a UBF filename extension.
- If you have not already stored your Cisco.com credentials (see “Saving Cisco.com Account Credentials in Prime Infrastructure” in Related Topics), you will be prompted to log in to Cisco.com, and to accept your organization’s active license agreement with Cisco, before you can download the update file.
- Be sure to download software updates that match your Prime Infrastructure version. For example, if you were running Prime Infrastructure 3.5, be sure to download software updates for version 3.5 only.
- Step 8** With the update file downloaded to your client machine, return to the Prime Infrastructure tab and choose **Administration > Licenses and Software Updates > Software Update**.
- Step 9** Click **Upload** and browse to locate and select the update file you downloaded.
- Step 10** Click **Install**.
- Step 11** Click **Yes** in the pop-up message. The server will restart automatically.
- Step 12** When the restart is complete, choose **Administration > Licenses and Software Updates > Software Update**. The Updates table should show the update as “Installed”.

Related Topics

[Install Software Updates](#), on page 125

[Save Cisco.com Account Credentials in Prime Infrastructure](#), on page 127

[Restart Prime Infrastructure Using CLI](#), on page 113

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

How to Use Your Cisco.com Account Credentials with Prime Infrastructure

You can store your Cisco.com account user name and password in Prime Infrastructure. Doing so will allow you to streamline download and installation of software updates, and speed automatic checking and notification of updates.

Note that Prime Infrastructure stores only one set of Cisco.com credentials at a time. The password is stored in secure, encrypted form. It will use this stored user name and password to do all software update notification checks until such time as another user either deletes the stored credentials (as explained in “Deleting Cisco.com Account Credentials” in Related Topics) or overwrites them by entering a new Cisco.com user name and password.

Related Topics

[Save Cisco.com Account Credentials in Prime Infrastructure](#), on page 127

[Deleting Cisco.com Account Credentials](#), on page 127

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

Save Cisco.com Account Credentials in Prime Infrastructure

- Step 1** Choose **Administration > Settings > System settings > Account Settings**
- Step 2** Enter a valid Cisco.com user name and password.
- Step 3** Click **Save**.

Related Topics

[Install Software Updates from Cisco.com](#), on page 125

[Restart Prime Infrastructure Using CLI](#), on page 113

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

Deleting Cisco.com Account Credentials

- Step 1** Choose **Administration > Settings > System settings > Account Settings**.
- Step 2** Click **Delete**.
- Step 3** Click **Yes** to confirm the deletion.

Related Topics

[Install Software Updates](#), on page 125

[Restart Prime Infrastructure Using CLI](#), on page 113

[How to Update Prime Infrastructure With Latest Software Updates](#), on page 122

How to Configure Support Request Settings

The Support Request Settings page allows you to configure the general support and technical support information.

- Step 1** Choose **Administration > Settings > System Settings > Support Request**. The Support Request Settings page appears.
- Step 2** Configure the following parameters:
- General Support Settings:

- Enable interactions directly from the server—Select this check box to allow interactions for support requests directly from the server.
- Sender E mail Address—Enter the email address of the support request sender.
- Interactions via client system only—Select this check box to allow interactions for support requests only through client system.
- Technical Support Provider Information:
 - Cisco—Select this check box if the technical support provider is Cisco.
 - Default Cisco.com Username—Enter a default username to log in to Cisco.com. Click **Test Connectivity** to test the connections to the mail server, Cisco support server, and forum server.
 - Third-Party Support Provider—Select this check box if the technical support provider is a third party other than Cisco. Enter the email address, email subject line format, and website URL of the support provider.

Step 3 Click **Save Settings**.

Related Topics

[Open a Cisco Support Case](#), on page 229

[Join the Cisco Support Community](#), on page 230

How to Manage Disk Space Issues

Whenever disk space on the physical or virtual Prime Infrastructure server reaches 90 percent, the server will trigger a Major alert indicating that the server is low on disk space.

Threshold crossings for these alarms are calculated based on the usage of the Prime Infrastructure `optvol` and `localdiskvol` partitions only. The `optvol` partition contains the Oracle database used to store all of Prime Infrastructure’s inventory and network data, while `localdiskvol` stores local application backups, WLC and MSE backups, and reports. The settings that trigger the alarms are defined in the file `PackagingResources.properties`, which you can find in the Prime Infrastructure server in the folder `/opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging`.

We recommend that administrators take action to increase disk space immediately upon receiving the Major alert. You can do this using any combination of the following methods:

- Free up existing database space as explained in “Compacting the Prime Infrastructure Database”.
- Reduce the storage load on the `localdiskvol` partition by setting up and using remote backup repositories, as explained in “Using Remote Backup Repositories”.
- Reduce the storage load on the `optvol` partition by reducing the amount and storage period for which you retain inventory and network data:
 - Reduce the length of time you store client association data and related events, as explained in “Specifying How Long to Retain Client Association History Data” and “Saving Client Traps as Events”.
 - Reduce the length of time you store reports, as explained in “Controlling Report Storage and Retention”.
 - Reduce the retention period for network inventory, performance, and other classes of data, as explained in “Specifying Data Retention by Category” and “Enabling DNS Hostname Lookup”.

- Increase the amount of existing virtual disk space allocated to Prime Infrastructure, as explained in “Modifying VM Resource Allocation Using VMware vSphere Client”. If you are using VMware ESXi 5.5 or later, use the vSphere Web Client to adjust disk space allocation (for details, see the “VMware vSphere documentation” in Related Topics). You can also install additional physical disk storage and then use VMware Edit Settings or the vSphere Web Client to allocate the additional storage to Prime Infrastructure.
- Move the Prime Infrastructure server installation to a server with adequate disk space, as explained in “Migrating to Another OVA Using Backup and Restore” and “Migrating to Another Appliance Using Backup and Restore”. For more details, see "[VMware vSphere Documentation](#)".

Related Topics

[Compact the Prime Infrastructure Database](#), on page 102

[Use a Remote Backup Repository](#), on page 51

[Specify How Long to Retain Client Association History Data](#), on page 104

[Save Client Traps as Events](#), on page 105

[How Data Retention Settings Affect Web GUI Data](#), on page 131

[Specify Data Retention By Database Table](#), on page 134

[Enable DNS Hostname Lookup](#), on page 103

[Modify VM Resource Allocation Using VMware vSphere Client](#), on page 101

[Migrate to Another Virtual Appliance Using Backup and Restore](#), on page 60

[Migrate to Another Physical Appliance Using Backup and Restore](#), on page 61



CHAPTER 6

Data Collection and Background Tasks

This section contains the following topics:

- [Control Data Collection Jobs, on page 131](#)
- [How Data Retention Settings Affect Web GUI Data, on page 131](#)
- [About Historical Data Retention, on page 132](#)
- [Performance and System Health Data Retention, on page 133](#)
- [Alarm, Event, and Syslog Purging, on page 139](#)
- [Log Purging, on page 139](#)
- [Report Purging, on page 139](#)
- [Backup Purging, on page 140](#)
- [Device Configuration File Purging, on page 140](#)
- [Software Image File Purging, on page 140](#)
- [Control System Jobs, on page 140](#)
- [Migrate Data from Cisco Prime LMS to Cisco Prime Infrastructure, on page 150](#)

Control Data Collection Jobs

All data collection tasks (and data purging tasks) are controlled from the Jobs Dashboard. See . Data collection jobs are listed under .

How Data Retention Settings Affect Web GUI Data

Changes you make on the Data Retention page determine the information that is displayed in the web GUI. You can open the data retention page by choosing **Administration > Settings > System Settings**, then choosing **General > Data Retention**.

For example, if you do not need any historical performance data older than 7 days, you can modify the performance data retention values as follows:

- Short-term Data Retention Period—1 day
- Medium-term Data Retention Period—3 days
- Long-term Data Retention Period—7 days

If you specify these settings, all data displayed in performance reports and on performance dashboards will be for the previous 7 days only. When you generate a performance report, even if you select a reporting period longer than the last 7 days, the report will contain data from the last 7 days only (because that is all of the data you selected to retain).

Similarly, if you view a performance dashboard and select a time frame longer than one week, the dashboard will contain data from the last 7 days only.

When you create the monitoring policy for interfaces, you can define the polling interval for every 15 minutes or every 5 minutes or every 1 minute. According to the selected polling interval, the device data is polled and stored in Oracle Data base. The data is aggregated every 1 hour into the AHxxx table; once a day into the ADxxx table irrespective of the polling interval is set to 1/5/15 minutes.

In the Interface Health Policy tab, if the frequency is set at 5 mins, you can view 12 samples for each hour. Every hour the data moves to the aggregated table and an average or mean interface statistics is calculated, and there will be one entry in the hourly aggregated table. The aggregation is the same for all the policies no matter what the polling interval is.

You can view data retention details and the age of the data storage, the event time in milliseconds and for each data base the entity ID and the event time. View the performance data and aggregate data in the Performance Dashlet, > Interfaces > Traffic Utilization tab.

About Historical Data Retention

Prime Infrastructure retains two types of historical data:

1. Non-aggregated historical data—Numeric data that cannot be gathered as a whole or aggregated. Client association history is one example of non-aggregated historical data.

You can define a retention period (and other settings) for each non-aggregated data collection task. For example, you can define the retention period for client association history in **Administration > Settings > System Settings > Client**. By default, the retention period for all non-aggregated historical data is 31 days or 1 million records. This retention period can be increased to 365 days.

1. Aggregated historical data—Numeric data that can be gathered as a whole and summarized as minimums, maximums, or averages. Client count is one example of aggregated historical data.

Types of aggregated historical data include:

- Trend: This includes wireless-related historical information such as client history, AP history, AP utilization, and client statistics.
- Device health: This includes SNMP polled data for wired and wireless devices, such as device availability, and CPU, memory, and interface utilization, and QoS.
- Network audit records: This includes audit records for configuration changes triggered by users, and so on.
- Performance: This includes Assurance data such as traffic statistics, application metrics, and voice metrics.
- System health records: This includes most data shown on Prime Infrastructure administrator dashboards.

The retention periods for these aggregation types are defined as Default, Minimum, and Maximum (see the table below). Use the **Administration > Settings > System Settings > General > Data Retention** page to define aggregated data retention periods. Aggregation types include hourly, daily, and weekly.

Table 10: Retention Periods for Aggregated Historical Data

Trend Data Retention Periods

Period	Default	Minimum	Maximum
Hourly	7 days	1 days	31 days
Daily	90 days	7 days	365 days
Weekly	54 weeks	2 weeks	108 weeks
Device Health Data Retention Periods			
Hourly	15 days	1 day	31 days
Daily	90 days	7 days	365days
Weekly	54 weeks	2 weeks	108 weeks
Performance Data Retention Periods			
Short-Term Data	7 days	1 day	31 days'
Medium-Term Data	31 days	7 days	365 days
Long-Term Data	378 days	2 days	756 days
Network Audit Data Retention Period			
All audit data	7 days	7 weeks	365 days
System Health Data Retention Periods			
Hourly	7 days	1 day	31 days
Daily	31 days	7 days	365 days
Weekly	54 weeks	7 weeks	365 days
User Job Data Retention Periods			
Weekly	7 days	7 days	7 days

The performance data is aggregated as follows:

- Short-term data is aggregated every 5 minutes.
- Medium-term data is aggregated every hour.
- Long-term is aggregated daily.

Performance and System Health Data Retention



Note Cisco recommends you do not change the retention periods for trend, device health, system health, and performance data because the default settings are optimized to get the most helpful information from interactive graphs.

The following table describes the information shown on the Data Retention page.

Type of Data	Description	Default Retention Settings
Trend Data Retain Periods	Device-related historical information. Trend data is gathered as a whole and summarized as minimums, maximums, or averages.	Hourly data retain period: 15 (days) Daily data retain period: 90 (days) Weekly data retain period: 54 (weeks)
Device Health Data Retain Periods	SNMP-polled device data such as device reachability, and utilization for CPU, memory, and interfaces.	Hourly data retain period: 15 (days) Daily data retain period: 90 (days) Weekly data retain period: 54 (weeks)
Performance Data Retain Periods	Assurance data such as traffic statistics. <ul style="list-style-type: none"> • Short-term data is aggregated every 5 minutes. • Medium-term data is aggregated every hour. • Long-term is aggregated daily. 	Short term data retain period: 7 (days) Medium term data retain period: 31 (days) Long term data retain period: 378 (days)
Network Audit Data Retain Period	Audit records for configurations triggered by users, and so on.	Audit data retain period: 90 (days)
System Health Data Retain Periods	Includes most data shown on the Admin dashboards	Hourly data retain period: 1 (days) Daily data retain period: 7 (days) Weekly data retain period: 54 (weeks)

Specify Data Retention By Database Table

Administrators can use the “Other Data Retention Criteria” section of the Data Retention page to configure retention periods for specific Prime Infrastructure database tables. You specify the retention period using the following attributes:

- **Age (in hours):** Specifies the maximum data retention period in hours for all records in the database.
- **Max Records:** Specifies the maximum number of records to retain in a particular database table. A Max Records value of NA means that the only retention criteria considered is the Age attribute.

The section is categorized into multiple subsections. Each subsection list each database table name, along with the current Age and Max Records used to determine whether an individual record in the table will be retained or discarded. The page also lists the table Age Attribute used to compute the age of the data in the table. The Optical Devices category is not applicable for Prime Infrastructure.

We strongly recommend you to consult with Cisco Technical Assistance Center before changing the values for any of the tables in this section. Doing so without help may affect system performance negatively.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Data Retention**.
- Step 2** Expand the **Other Data Retention Criteria** section.
- Step 3** Expand the database table subsection for which you want to specify Age and Max Records values.

Step 4 Click on the database table listing and enter the new values as needed.

Step 5 Click Save.

Specify Client Data Retrieval and Retention

Administrators can use Prime Infrastructure's Client page to configure parameters affecting retention of data on network clients, including:

- Data on disassociated clients. The default is seven days, and this applies irrespective of whether the clients will ever attempt to associate again.
- Data on client session histories. You can also specify the maximum number of session entries to keep, specified as rows in the Prime Infrastructure database.
- Cached client host names retrieved from a DNS server.

In addition to these data-retention options, the page allows you to enable and disable options to:

- Automatically troubleshoot clients using a diagnostic channel when traps are received from these clients.
 - Automatically retrieve client host names from a DNS server.
 - Poll clients when traps or syslogs are received from these clients
 - Discover clients from enhanced client traps.
 - Discover wired clients on trunk ports .
 - Save as Prime Infrastructure events routine client association and disassociation traps and syslogs. This option is disabled by default, to avoid Prime Infrastructure performance problems on large networks during periods (such as network setup) when these kinds of traps and syslogs may be numerous. You may want to enable this option at all other times.
 - Save all 802.1x and 802.11 client authentication-failure traps as Prime Infrastructure events. This option is disabled by default, to avoid Prime Infrastructure performance problems on large networks during periods (such as network setup) when these kinds of traps and syslogs may be numerous. You may want to enable this option if your network is stable.
-

Step 1 Choose **Administration > Settings > System Settings > Client and User > Client**.

Step 2 Under Data Retention, modify the values as required.

Step 3 Click Save.

Enable Data Deduplication

Data deduplication allows you to identify authoritative sources for each of the following classes of application data:

- Application Response Time data for TCP applications
- Traffic analysis data for all applications
- Voice/Video data for RTP applications

Prime Infrastructure stores all data it receives about network elements and protocols, including any duplicate data that it may receive from multiple sources. When you specify authoritative data sources, only the data from the specified sources is displayed when you view a particular location or site.

The Data Deduplication page allows you to specify one or more authoritative data sources at a specific location. For example, if you have a Network Analysis Module (NAM) at a branch office as well as NetFlow data that is sent from the same branch, you can choose to have Prime Infrastructure display only the NAM or the NetFlow data for that location.

-
- Step 1** Choose **Services > Application Visibility & Control > Data Deduplication**.
- Step 2** Select the **Enable Data Deduplication** checkbox and click **Apply**. The Data Deduplication page displays the list of your defined location groups.
- Step 3** To automatically detect authoritative sources at all locations, click **Auto-Detect**. If it can identify them, Prime Infrastructure will fill in the address of an authoritative source in the list box under the column listing sources for each of the classes of application data.
- Step 4** To specify authoritative sources for a class of application data at a specific location:
- Click the location group name.
 - Click the drop-down list box under the class of application data for which you want to specify an authoritative source (for example: click in the list box under “Application Response Time”).
 - From the drop-down list, select the data sources you want to specify as authoritative for that location and application data type. Then click **OK**.
 - Click **Save** to save your selections.
- Repeat this step as needed for each location and application data type for which you want to specify authoritative data source.
- Step 5** When you are finished, click **Apply** to save your changes.
-

Control Report Storage and Retention

All scheduled reports are stored in the Scheduled Reports Repository. You will want to ensure that scheduled reports are retained in the report repository for reasonable lengths of time only, and deleted on a regular basis.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Report**. The Report page appears.
- Step 2** In **Repository Path**, specify the report repository path on the Prime Infrastructure server.
- Step 3** In **File Retain Period**, specify the maximum number of days reports should be retained.
- Step 4** Click **Save**.
-

Specify Inventory Collection After Receiving Events

The Inventory page allows you to specify if Prime Infrastructure must collect inventory when a syslog event is received for a device.

-
- Step 1** Choose **Administration > Settings > System Settings > Inventory**. The Inventory page appears.
- Step 2** Select the **Enable event based inventory collection** check box to allow Prime Infrastructure to collect inventory when it receives a syslog event for a device.

Step 3 Select the **Enable Syslog and Traps on device** check box to allow Prime Infrastructure to enable syslog and trap notifications on newly added devices.

Note This feature is not supported on the Cisco Nexus devices.

Step 4 Click **Save**.

Control Configuration Deployment Behavior

Administrators can choose to have device configurations backed up or rolled back whenever Prime Infrastructure users deploy new device configuration templates. They can also control how Cisco WLC configurations are archived, as explained in the following related topics.

Related Topics

[Archive Device Configurations Before Template Deployment](#), on page 137

[Roll Back Device Configurations on Template Deployment Failure](#), on page 137

[Specify When and How to Archive WLC Configurations](#), on page 137

Archive Device Configurations Before Template Deployment

With Backup Device Configuration enabled, Prime Infrastructure automatically backs up all device running and startup configurations before deploying new configuration templates.

Step 1 Choose **Administration > Settings > System Settings > Inventory > Configuration**.

Step 2 Select the **Backup Device Configuration** check box.

Step 3 Click **Save**.

Related Topics

[Roll Back Device Configurations on Template Deployment Failure](#), on page 137

Roll Back Device Configurations on Template Deployment Failure

With **Rollback Configuration** enabled, Prime Infrastructure automatically rolls back each device to its last archived running and startup configurations when any attempt to deploy a new configuration template to the device has failed.

Step 1 Choose **Administration > Settings > System Settings > Configuration**.

Step 2 Select the **Rollback Configuration** check box.

Step 3 Click **Save**.

Specify When and How to Archive WLC Configurations

By default, Prime Infrastructure keeps a backup archive of startup configurations for each device running Cisco Wireless LAN Controller (WLC) software whenever it:

- Collects initial out-of-box inventory for these devices

- Receives notification of a configuration change event for these devices

Prime Infrastructure provides configuration archive support for devices running Cisco WLC software. The configuration archive includes only startup configurations. The running configurations are excluded from configuration archive.

You can change many of the basic parameters controlling Cisco WLC configuration archiving, including:

- The maximum timeout on all Cisco WLC configuration operations (fetch, archive or rollback).
- The maximum time to wait before updating the Cisco WLC configuration archive summary information.
- Whether or not to archive configurations at initial inventory collection, after each inventory synchronization, and on receipt of configuration change events.
- Whether or not to mask security information when exporting archived configurations to files.
- The maximum number of archived configurations for each device and the maximum number of days to retain them.
- The maximum number of thread pools to devote to the archive operation. Increasing the default can be helpful with Prime Infrastructure performance during archiving of changes involving more than 1,000 devices.

You can also tell Prime Infrastructure to ignore for archive purposes any change that involves specified commands on devices of a given family, type, or model. This is useful when you want to ignore insignificant or routine changes in a few parameters on one or many devices.

Step 1 Choose **Administration > Settings > System Settings > Configuration Archive**.

Step 2 On the **Basic** tab, change the basic archive parameters as needed.

Note The option of masking the security content while exporting is included in the **Inventory > Device Management > Configuration Archive** page. See [Download Configuration Files](#) for more information.

Step 3 To specify devices and configuration commands to exclude from archived configurations:

- Click the **Advanced** tab.
- In the **Product Family** list, choose the device(s) for which you want to specify configuration commands to exclude.

Use the List/Tree View dropdown, or click the > icons to drill down to individual product types and models for which you want to specify exclude commands.

- In the **Command Exclude List**, enter (separated by commas) the configuration commands you want to exclude for the currently selected device family, type, or model.

If the device(s) you select has configuration changes and Prime Infrastructure detects that the change is one of the specified commands in the Exclude List, Prime Infrastructure will not create an archived version of the configuration with this change.

- Click **Save**.
 - To remove a specified set of command exclusions for a device family, type or model, select the device(s) in the Product Family list and click **Reset**.
-

Alarm, Event, and Syslog Purging



Note These default purging settings are provided to ensure optimal performance. Use care when adjusting these settings, especially if you are managing a very large network (where increasing these settings may have an adverse impact).

stores a maximum of 8000000 events and 2000000 syslogs in the database.

To protect system performance, purges alarms, events, and syslogs according to the settings in the following table. All of these settings are enabled by default. Data is deleted on a daily basis. Alarm tables are checked hourly, and if the alarm table exceeds the 300,000 limit, deletes the oldest cleared alarms until the alarms table size is within the limit.

Data Type	Deleted after:	Default Setting
Alarms—Cleared security alarms	30 days	Enabled
Alarms—Cleared non-security alarms	7 days	Enabled
Events	60 days	Enabled
Syslogs	30 days	Enabled
Alarms	30 days	Disabled

To change the settings, choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarms and Events** and modify the settings in the Alarm and Event Cleanup Options area.

Log Purging

You can adjust the purging settings for logs by choosing **Administration > Settings > Logging**. Logs are saved until they reach the maximum size. At that point, a number is appended to the log file and a new log is started. When the number of logs exceeds the maximum, the oldest log is deleted.

The following table lists the default purging values for General and SNMP logs.

Log Type	Size of Logs	Number of Logs	To change the setting, see:
General	10 MB	10	Adjust General Log File Settings and Default Sizes, on page 234
SNMP	10 MB	5	View and Manage General System Logs, on page 234

Report Purging

By default, reports are stored in a repository named `/localdisk/ftp/reports` and are deleted after 31 days from that directory. Reports filters that you set from the filters page are saved in the database and are not purged.

-
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Reports**.
- Step 2** If required, adjust the location for the reports repository on the server. The repository must reside under the FTP root partition.
- Step 3** If you want to change the default purging age, enter a new value in the **File Retain Period** field.
- Step 4** Click **Save**.
-

Backup Purging

By default, 2 backups are saved for backups in local repositories. If you are using remote repositories, there is no automatic backup purging mechanism; you must manually delete old backups. See [Change the Number of Automatic Application Backups That Are Saved, on page 55](#).

Device Configuration File Purging

For each device, 5 configuration files are saved in the configuration archive. Any file that is older than 30 days is purged. Device configuration files cannot be manually deleted. .

Software Image File Purging

Device software image files are not automatically purged from the database. They must be manually removed using the GUI client.

Control System Jobs

Prime Infrastructure performs scheduled data collection jobs on a regular basis. You can change each job's schedule, pause or resume it, or execute it immediately.

Disabling or limiting these System jobs can have a direct impact on how you use Prime Infrastructure, especially for reporting. To help you consider these impacts, take note of the reports this data is used in.

Related Topics

- [Schedule Data Collection Jobs](#), on page 140
- [Resume Data Collection Jobs](#), on page 141
- [Run Data Collection Jobs Immediately](#), on page 141
- [About System Jobs](#), on page 141

Schedule Data Collection Jobs

System jobs run on a regular default schedule, as described in [About System Jobs](#) . You can re-schedule them as needed.

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard > System Jobs**.
- Step 2** Select the category of data collection job you want to re-schedule (e.g., **APIC-EM Integration, Assurance and Health Summary, Infrastructure, Inventory and Discovery, or Status and Wireless Monitoring**).
- Step 3** Click the check box next to the system job you want to re-schedule.
- Step 4** Click **Edit Schedule** and specify the schedule you want the job to run on.
- You can select the date and time the job is executed. You can choose to have the job recur on a minute, hourly, daily, weekly, monthly or annual basis. No end time has been specified by default.
- Step 5** When you are finished, click **Submit**.
-

Resume Data Collection Jobs

You can pause any scheduled data collection job, and resume it if already paused.

- Step 1** Choose **Administration > Dashboards > Job Dashboard > System Jobs**.
- Step 2** Select the category of data collection job you want to pause or resume (e.g., **APIC-EM Integration, Assurance and Health Summary, Infrastructure, Inventory and Discovery, or Status and Wireless Monitoring**).
- Step 3** Click the check box next to the system job you want.
- Step 4** Click **Pause Series** to stop the job from executing.
- If the job is already paused, click **Resume Series** to resume execution on the current schedule.
-

Run Data Collection Jobs Immediately

In addition to the steps below, you can run a job immediately by rescheduling it and selecting the time to execute as **Now** and submit. Then select the job and click run.

- Step 1** Choose **Administration > Dashboards > Job Dashboard > System Jobs**.
- Step 2** Select the category of data collection job you want to run (e.g., **APIC-EM Integration, Assurance and Health Summary, Infrastructure, Inventory and Discovery, or Status and Wireless Monitoring**).
- Step 3** Click the check box to select the system job you want to run immediately.
- Step 4** Click **Run**.
-

About System Jobs

The following table describes the background data collection jobs Prime Infrastructure performs.

Table 11: Inventory Data Collection Jobs

Task Name	Default Schedule	Description	Editable options
APIC EM Integration Jobs			
APIC-EM Site Sync	6 hours	Schedules synchronization of sites and devices between APIC-EM and Prime Infrastructure.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
APIC Server Status Periodic	5 minutes	Schedules checks on APIC-EM server reachability.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
PnP Bulk Import	5 minutes	Schedules bulk import of device profiles from APIC-EM to Prime Infrastructure.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
PnP Status Polling	5 minutes	Tracks the status of the PnP devices created on APIC-EM and adds them to Prime Inventory when successful.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Post PnP Job		Schedules validation of post-PnP configurations on devices.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Assurance and Health Summary Jobs			
AGGREGATION_HEALTH_SUMMARY	Disabled	Aggregates the health scores of device metrics (Routers, Switches and Access Points).	Non Editable
Assurance DataSource Update	Disabled	Synchronizes the list of data sources between two different processes in PI.	Non Editable
Assurance License Update	Disabled	Fetches the devices and AP which netflow associated with it every 12 hours.	Non Editable
Assurance Lync Aggregation	Disabled	Computes the Lync call statistics.	Non Editable
BASELINE_DAILY	Disabled	Aggregates the hourly baseline values to daily values for the application data.	Non Editable

Task Name	Default Schedule	Description	Editable options
BASELINE_HOURLY	Disabled	Computes hourly baseline data points for application data.	Non Editable
DAHealth_SITE	Disabled	Synchronizes the site rules between two different processes in PI.	Non Editable
HEALTH_SUMMARY_5MIN	Disabled	Computes the health scores for applications.	Non Editable
PushCollectionPlanToDA	Disabled	Pushes the collection plan to DA.	Non Editable
WUserSyncJob_USER	Disabled	Fetches the list of current clients from the Station Cache to update the netflow user cache.	Non Editable
Infrastructure jobs			
Bulk Recompute RF Prediction	15 days	Schedules status polling of Bulk Recompute RF Prediction.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Connected Mobility Reachability Status	5 minutes	Schedules status polling of Connected Mobility Reachability	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Controller Configuration Backup	1 day	Displays the controller configuration backup activities.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Data Cleanup	2 hours	Schedules daily data file cleanup.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Device Config Backup-External	15 minutes	Transfers 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).	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job. Click the edit icon, and check the Export only Latest Configuration check box, to transfer only the latest configuration. You can edit the job properties based on the user permission set in Role Based Access Control (RBAC).
Guest Accounts Sync	1 day	Schedules guest account polling and synchronization.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Index serach Entities	3 hours	Schedules the Index Search Entities job.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Mobility Service Backup	7 days	Schedules automatic mobility services backups.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Mobility Service Status	5 minutes	Schedules mobility services status polling.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Mobility Service Synchronization	1 hour	Schedules mobility services synchronization.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
On Demand Reports Cleanup	6 hours	Schedules reports cleanup.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Server Backup	1 day	Schedules automatic Prime Infrastructure server backups. The backups created are application backups.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Smart License Compliance Status	Disabled	Runs for Smart License for the default schedule.	Non Editable.
wIPS Alarm Sync	2 hours	Schedules wIPS alarm synchronization.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Inventory and Discovery Jobs			
Autonomous AP Inventory	1 day	Collects inventory information for autonomous APs.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Switch Inventory	1 day	Collects inventory information for Switches.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Wireless Controller Inventory	1 day	Collects inventory information for Wireless Controllers.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Status Jobs			
Appliance Status	5 minutes	Schedules appliance polling. This task populates the appliance polling details from the Administration > Appliance > Appliance Status page. It also populates information like the performance and fault checking capabilities of the appliance.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Autonomous Client Status	5 minutes	Lets you schedule status polling of autonomous AP clients.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Autonomous AP Operational Status	5 minutes	Schedules status polling of autonomous wireless access points.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Controller Operational Status	5 minutes	Schedules controller operational status polling.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Device Data Collector	30 minutes	Schedules data collection based on specified command-line interface (CLI) commands at a configured time interval.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Identity Services Engine Status	15 minutes	Schedules Identity Services Engine polling.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Interferers	15 minutes	Schedules interferer information collection.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Learn Unified AP Ping Capability	This Job remains suspended and runs on-demand.	Schedules Unified AP Ping Capability information collection.	Non-Editable.
License Status	4 hours	Schedules the license-status information collection.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Lightweight AP Ethernet Interface Status	1 minute	Schedules Lightweight AP Ethernet Interface Status information collection.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Lightweight AP Operational Status	5 minutes	Schedules Lightweight AP Operational Status information collection.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Lightweight Client Status	5 minutes	Schedules information collection for Lightweight AP Clients from Network.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Mobility Service Performance	15 minutes	Schedules status polling of mobility services performance.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Mobility Status Task	15 minutes	Schedules status polling of mobility services engines.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
OSS Server Status	5 minutes	Schedules status polling of OSS Servers.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Redundancy Status	1 hour	Schedules redundancy status polling of primary and secondary controllers.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Switch NMSP and Location Status	4 hours	Schedules Switch Network Mobility Services Protocol (NMSP) and Civic Location status polling.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Switch Operational Status	5 minutes	Schedules switch operational status polling.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Third Party Access Point Operational Status	3 hours	Schedules operational status polling of third party APs.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Third Party Controller Operational Status	3 hours	Schedules operational status polling of third party Controllers.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Unmanaged APs	15 minutes	Collects poll information for unmanaged access points.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Wired Client Status	2 hours	Schedules Wireless Client status polling	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Wireless AP Discovery	5 minutes	Schedules Wireless AP discovery.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Wireless Configuration Audit	1 day	Schedules Wireless Configuration Agent audit collection.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Wireless Monitoring Jobs			

Task Name	Default Schedule	Description	Editable options
AP Ethernet Statistics	15 minutes	Schedules AP Ethernet statistics collection.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
AP Image Pre-Download Status	15 minutes	Allows you to see the Image Pre-download status of the associated APs in the controllers. To see the status of the access points, the “Pre-download software to APs” checkbox should be selected while downloading software to the controller.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Autonomous AP CPU and Memory Utilization	15 minutes	Schedules collection of information on memory and CPU utilization of Autonomous APs.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Autonomous AP Radio Performance	15 minutes	Schedules collection of information about radio performance information as well as radio up or down status for autonomous APs.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Autonomous AP Tx Power and Channel Utilization	15 minutes	Schedules collection of information about radio performance of Autonomous APs.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
CCX Client Statistics	1 hour	Schedules collection of the Dot11 and security statistics for CCX Version 5 and Version 6 clients.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
CleanAir Air Quality	15 minutes	Schedules collection of information about CleanAir air quality.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Client Statistics	15 minutes	Schedules retrieval of statistical information for autonomous and lightweight clients.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Map Info Polling Job	1 minute		Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.

Task Name	Default Schedule	Description	Editable options
Media Stream Clients	15 minutes	Schedules collection of information about media stream clients.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Mesh Link Status	5 minutes	Schedules collection of status of mesh links.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Mesh link Performance	10 minutes	Schedules collection of information about the performance of mesh links.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Radio Performance	15 minutes	Schedules collection of statistics from wireless radios.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Radio Voice Performance	15 minutes	Schedules collection of voice statistics from wireless radios.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Rogue AP	2 hours	Schedules collection of information about rogue access points.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Switch CPU and Memory Poll	30 minutes	Schedules polling of switch CPU and memory information.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Traffic Stream Metrics	8 minutes	Retrieves traffic stream metrics for the clients.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Wireless Controller Performance	30 minutes	Schedules collection of performance statistics for wireless controllers.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.
Wireless QoS Statistics	15 minutes	Schedules collection of information QoS Statistics for Wireless Controllers.	Select Edit Schedule > Recurrence and select the appropriate settings to schedule the job.

Migrate Data from Cisco Prime LMS to Cisco Prime Infrastructure

Prime Infrastructure supports data migration from Cisco Prime LAN Management Solution (LMS) version 4.2.5 on all platforms. The following LMS data can be imported into Prime Infrastructure using the CAR CLI:

- Device Credential and Repository (DCR) Devices
- Static Groups
- Dynamic Groups
- Software Image Management Repository Images
- User Defined Templates (Netconfig)
- LMS Local Users
- MIBs

Only the Dynamic Groups containing the rule with the following attributes can be imported from LMS.

- PI attribute Name—LMS attribute name
- Contact—System.Contact
- Description—System.Description
- Location— System.Location
- Management_Address—Device.ManagementIpAddress
- Name—System.Name
- Product_Family—Device.Category
- Product_Series—Device.Series
- Product_Type—Device.Model
- Software_Type—System.OSType
- Software_Version—Image.Version

To migrate LMS data to Prime Infrastructure, follow these steps:

-
- Step 1** Identify the server where LMS backup data is stored.
- Step 2** Open a CLI session with the Prime Infrastructure server (see [How to Connect Via CLI, on page 111](#)).
- Step 3** Enter the following commands to configure the backup location:

```
admin# configure terminal
admin(config)# repository carsapps
admin(config-Repository)# url location
admin(config-Repository)# user root password plain password
admin(config-Repository)# end
```

where:

- a. *location* is a fully qualified URL, including access protocol, for the location of the LMS backup data. For example: `ftp://10.77.213.137/opt/lms` , `sftp://10.77.213.137/opt/lms` , or `fdisk:foldername` .
- b. *password* is the root user password

Step 4 Import the LMS backup into Prime Infrastructure using the following command:

```
admin# lms migrate repository carsapps
```

Step 5 Exit your CLI session, log back in to the Prime Infrastructure user interface, and verify that your LMS data was imported properly. The following table shows where to look in Prime Infrastructure for the imported LMS data.

LMS Data	Prime Infrastructure Location
DCR Devices	Inventory > Network Devices
Static Group	Inventory > Network Devices > User Defined Group
Dynamic Group	Inventory > Network Devices > User Defined Group
Software Image Management Repository Images	Inventory> Software Images
User Defined Templates (Netconfig)	Configuration > Templates > Features & Technologies
LMS Local Users	Administration > Users, Roles & AAA > Users
MIBs	Monitor > Monitoring Policies. In the menu, click Add, then select Policy Types > Custom MIB Polling.



CHAPTER 7

User Permissions and Device Access

- [User Interfaces, User Types, and How To Transition Between Them](#), on page 153
- [Enable and Disable root Access for the Linux CLI and the Web GUI](#), on page 156
- [Control the Tasks Users Can Perform \(User Groups\)](#), on page 157
- [Add Users and Manage User Accounts](#), on page 182
- [Configure Guest Account Settings](#), on page 184
- [Use Lobby Ambassadors to Manage Guest User Accounts](#), on page 185
- [Find Out Which Users Are Currently Logged In](#), on page 189
- [View the Tasks Performed By Users \(Audit Trail\)](#), on page 190
- [Configure Job Approvers and Approve Jobs](#), on page 190
- [Configure Job Notification Mail for User Jobs](#), on page 191
- [Configure Global Password Policies for Local Authentication](#), on page 191
- [Configure the Global Timeout for Idle Users](#), on page 191
- [Set Up the Maximum Sessions per User](#), on page 192
- [Create Virtual Domains to Control User Access to Devices](#), on page 193
- [Configure Local Authentication](#), on page 201
- [Configure External Authentication](#), on page 201

User Interfaces, User Types, and How To Transition Between Them

These topics describe the GUI and CLI interfaces used by , and how to transition between the and Linux CLI interfaces.

- [User Interfaces and User Types](#), on page 153
- [How to Transition Between the CLI User Interfaces in](#) , on page 155

User Interfaces and User Types

The following table describes the user interfaces employed by , and the types of users that can access each interface.

User Interface	Interface Description	User Types
web GUI	<p>Web interface that facilitates day-to-day and administration operations using the web GUI. These users can have varying degrees of privileges and are classified into role-based access control (RBAC) classes and subclasses.</p> <p>This interface provides a subset of operations that are provided by the CLI admin and CLI config users.</p>	<p>web GUI everyday users—Created by web GUI root user . These users have varying degrees of privileges and are classified into role-based access control (RBAC) classes and subclasses called <i>user groups</i> (Admin, Super Users, Config Managers, and so forth). For information on the user groups, see Types of User Groups, on page 157.</p> <p>web GUI root user—Created at installation and intended for first-time login to the web GUI, and for creating other user accounts. This account should be disabled after creating at least one web GUI user that has Admin privileges—that is, a web GUI user that belongs to the Admin or Super Users user group. See Disable and Enable the Web GUI root User, on page 157.</p> <p>Note The web GUI root user is not the same as the Linux CLI root user, nor is it the same as the CLI admin user.</p>
Admin CLI	Cisco proprietary shell which provides secure and restricted access to the system (as compared with the Linux shell). This Admin shell and CLI provide commands for advanced administration tasks. These commands are explained throughout this guide. To use this CLI, you must have CLI admin user access. You can access this shell from a remote computer using SSH.	<p>CLI Admin user—Created at installation time and used for administration operations such as stopping and restarting the application and creating remote backup repositories. (A subset of these administration operations are available from the web GUI).</p> <p>To display a list of operations this user can perform, enter ? at the prompt.</p> <p>Some tasks must be performed in config mode. To transition to config mode, use the procedure in Transition Between the admin CLI and config CLI, on page 155.</p>
Config CLI	Cisco proprietary shell which is restricted and more secure than the Linux shell. This Config shell and CLI provide commands for system configuration tasks. These commands are explained throughout this guide. To use this CLI, you must have admin-level user access (see the information in the User Types column of this table). You can access this shell from the Admin CLI shell.	<p>The admin CLI user can create other CLI users for a variety of reasons, using the following command:</p> <pre>(config) username <i>username</i> password role {<i>admin user</i>} <i>password</i></pre> <p>These users may have admin-like privilege/roles or lower level privileges as defined during creation time. To create a CLI user with admin privileges, run the username command with the admin keyword; otherwise, use the user keyword.</p>
Linux CLI	Linux shell which provides all Linux commands. The Linux shell should only be used by Cisco technical support representatives. Regular system administrators should not use the Linux shell. You cannot reach this shell from a remote computer using SSH; you can only reach it through the admin shell and CLI.	<p>Linux CLI admin user—Created at installation time and used for Linux-level administration purposes.</p> <p>This admin user can get root-level privileges by following the procedure in Log In and Out as the Linux CLI root User, on page 155. Tasks that require root-level permissions should only be performed by Cisco Support teams to debug product-related operational issues. For security purposes, the Linux CLI admin and root users should be disabled; see Disable and Enable the Linux CLI Users in , on page 156.</p>

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 .

Transition Between the admin CLI and config CLI

To move from the admin CLI to the config CLI, enter **config** at the admin prompt.

```
(admin)# config
(config)#
```

To move from the config CLI back to the admin CLI, enter **exit** or **end** at the config prompt:

```
(config)# exit
(admin)#
```

Log In and Out as the Linux CLI root User

The Linux CLI has two shell users: One with administrative access (Linux CLI admin user), and another with root access (Linux CLI root user). The diagram in [How to Transition Between the CLI User Interfaces in , on page 155](#) illustrates the flow for logging in and out as the various CLI users.

To log in as the Linux CLI root user, you will have to transition from being the CLI admin user to the Linux CLI admin user to the Linux CLI root user. The following procedure gives you the exact steps you must follow.

Before you begin

If the Linux CLI user is disabled, re-enable it. See [Disable and Enable the Linux CLI Users in , on page 156](#).

Step 1

To log in as the Linux CLI root user:

- Start an SSH session with the server and log in as the CLI admin user.
- As the CLI admin user, log in as the Linux CLI admin user:

```
shell
Enter shell access password: password
```

- Log in as the Linux CLI root user.

```
sudo -i
```

By default, the Linux CLI shell prompt is the same for the Linux CLI admin and root user. You can use the **whoami** command to check the current user.

Step 2

To exit:

- Log out as the Linux CLI root user.

```
exit
```

- Log out as the Linux CLI admin user.

```
exit
```

You are now logged in as the CLI admin user.

What to do next

For security purposes, disable the Linux CLI root user. See [Disable and Enable the Linux CLI Users in](#) , on page 156.

Enable and Disable root Access for the Linux CLI and the Web GUI

As described in [How to Transition Between the CLI User Interfaces in](#) , on page 155, after installation, you should disable the web GUI **root** user after creating at least one other web GUI user that has Admin or Super Users privileges. See [Disable and Enable the Web GUI root User, on page 157](#).

The Linux CLI root user is disabled after installation time. If you need to re-enable it, follow the procedure in [Disable and Enable the Linux CLI Users in](#) , on page 156.

Disable and Enable the Linux CLI Users in

This procedure shows you how to disable and enable the Linux CLI admin shell in deployments running 2.x. When you disable the shell, you will no longer be able to log in as the Linux CLI admin or root users. When the shell is enabled, users can log in by following the procedure in [How to Transition Between the CLI User Interfaces in](#) , on page 155.

Before you begin

Make sure you have the password for the Linux CLI admin user.

Step 1 Log in to as the CLI admin user. See [Establish an SSH Session With the Server, on page 78](#).

Step 2 Disable the Linux CLI admin shell (which disables the Linux CLI admin and root users):

```
shell disable
Enter shell access password: passwd
shell access is disabled
```

Step 3 To re-enable the Linux CLI admin shell (you must run this command as the CLI admin user):

```
shell
Shell access password is not set
Configure password for shell access

Password: passwd
Password again: passwd

Shell access password is set
Run the command again to enter shell
```

Disable and Enable the Web GUI root User

Step 1 Log into the web GUI as root, and create another web GUI user that has root privileges—that is, a web GUI user that belongs to the Admin or Super Users user group. See [Add Users and Manage User Accounts, on page 182](#). Once this is done, you can disable the web GUI **root** account.

Step 2 Disable the web GUI root user account. (The web GUI admin account, which remains active, can perform all required CLI functions.)

```
ncs webroot disable
```

Step 3 To re-enable the account:

```
ncs webroot enable
```

Control the Tasks Users Can Perform (User Groups)

user authorization is implemented through user groups. A user group contains a list of tasks that control which parts of a user can access and the tasks the user can perform in those parts.

While user groups control what the user can do, *virtual domains* control the devices on which a user can perform those tasks. Virtual domains are described in [Create Virtual Domains to Control User Access to Devices, on page 193](#).

provides several predefined user groups. If a user belongs to a user group, the user inherits all of the authorization settings for that group. A user is normally added to user groups when their account is created.

These topics explain how to manage user authorization:

- [Types of User Groups, on page 157](#)
- [View and Change the Tasks a User Can Perform, on page 159](#)
- [View and Change the Groups a User Belongs To, on page 160](#)
- [View User Groups and Their Members, on page 160](#)
- [Create a Customized User Group, on page 178](#)
- [View and Change the Tasks a Group Can Perform, on page 180](#)
- [Use User Groups with RADIUS and TACACS+, on page 181](#)

Types of User Groups

provides the following predefined user groups:

- [User Groups—Web UI, on page 158](#)
- [User Groups—NBI, on page 158](#)

For information about CLI users, see [User Interfaces and User Types, on page 153](#).

User Groups—Web UI

provides the default web GUI user groups listed in the following table. You can assign users to multiple groups, except for users that belong to the Monitor Lite user group (because Monitor Lite is meant for users who should have very limited permissions).

See [View and Change the Tasks a Group Can Perform, on page 180](#) for information on the tasks that pertain to each user group and the default settings.

User Group	Group Task Focus
Root	All operations. The group permissions are not editable. The root web UI user is available after installation and is described in User Interfaces and User Types, on page 153 . A best practice is to create other users with Admin or Super Users privileges, and then disable the root web UI user as described in Disable and Enable the Web GUI root User, on page 157 .
Super Users	All operations (similar to root). The group permissions are editable.
Admin	Administer the system and server. Can also perform monitoring and configuration operations. The group permissions are editable.
Config Managers	Configure and monitor the network (no administration tasks). The permissions assigned to this group are editable.
System Monitoring	Monitor the network (no configuration tasks). The group permissions are editable.
Help Desk Admin	Only has access to the help desk and user preferences related pages. Members of this user group cannot be members of any other user group. This is a special group which lacks access to the user interface.
Lobby Ambassador	User administration for Guest users only. Members of this user group cannot be members of any other user group.
User-Defined 1-4	these are blank groups and can be edited and customized as needed.
Monitor Lite	View network topology and use tags. The group permissions are not editable. Members of this user group cannot be members of any other user group.
North Bound API	Access to the SOAP APIs.
User Assistant	Local Net user administration only. Members of this user group cannot be members of any other user group.
mDNS Policy Admin	mDNS policy administration functions.

User Groups—NBI

provides the default NBI user groups listed in the following table. The permissions in these groups are not editable.

See [View and Change the Tasks a Group Can Perform, on page 180](#) for information on the tasks that pertain to each user group and the default settings.

User Group	Provides access to:
NBI Credential	
NBI Read	
NBI Write	

View and Change the Tasks a User Can Perform

The tasks a user can perform is controlled by the user groups the user belongs to. Follow these steps to find out which groups a user belongs to and which tasks a user is authorized to perform.



Note If you want to check the *devices* a user can access, see [Assign Virtual Domains to Users](#), on page 198.

- Step 1** Choose **Administration > Users > Users, Roles & AAA** and locate the user name.
- Step 2** Locate the user name and check the **Member of** column to find out which user groups the user belongs to.
- Step 3** Click a user group hyperlink. The **Group Detail** window lists the tasks that group members can and cannot perform.
- A checked check box means group members have permission to perform that task. If a checked box is greyed-out, it means you cannot disable the task. For example, does not allow you to remove the "View tags" task for the Monitor Lite user group because it is an integral task for that user group.
 - A blank check box means group members cannot perform that task. If a blank check box is greyed out, it means you cannot enable the task for the user group.

The web GUI root and Monitor Lite groups, and the NBI groups, are not editable.

- Step 4** If you want to change permissions, you have these choices:

- Note** Be careful. Selecting and deselecting tasks in the Group Detail window will apply your changes to *all group members*.
- Change permissions for all user group members. See [View and Change the Tasks a Group Can Perform](#), on page 180.
 - Add the user to a different user group. The predefined user groups are described in [User Groups—Web UI](#), on page 158 and [User Groups—NBI](#), on page 158. Those topics also describe any group restrictions; for example, if a user belongs to the predefined Monitor Lite user group, the user cannot belong to any other groups.
 - Remove the user from this group. See [View and Change the Groups a User Belongs To](#), on page 160.
 - Use a customized user group and add the user to that group. To find out which customized groups already exist, see [View and Change the Tasks a Group Can Perform](#), on page 180. To create a new customized group, see [Create a Customized User Group](#), on page 178.

View and Change the Groups a User Belongs To

The tasks users can perform is determined by the user groups they belong to. This is normally configured when a user account is created (see [Add and Delete Users, on page 183](#)). User groups are described in [Types of User Groups, on page 157](#).

This procedure explains how to view the groups a user belongs to and, if necessary, change the user's group membership.

-
- Step 1** Choose **> Administration > Users, Roles & AAA Users**, then choose **Users**.
- Step 2** In the **User Name**, column, locate and click the user name hyperlink to open the **User Details** window. All user groups are listed under the General tab.
- A checked check box means the user belongs to that group. If a checked box is greyed-out, it means you cannot remove the user from that group. For example, will not allow you to remove the user named **root** from the root user group.
 - A blank check box means the user does not belong to that group. If a blank check box is greyed-out, it means you cannot add the user to that group.
- (To check the tasks that a group can perform, choose **User Groups** from the left sidebar menu and click a group name.)
- Step 3** To change the groups the user belongs to, select and unselect the appropriate groups in the **User Details** window, then click **Save**.
-

View User Groups and Their Members

Users can belong to multiple groups, unless they belong to a very restricted group such as Monitoring Lite. This procedure explains how to view existing user groups and their members.

-
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **User Groups**.
- The User Groups page lists all existing user groups and a short list of their members. For a description of these groups, see [Types of User Groups, on page 157](#).
- Step 2** To view all members of a group, click a group hyperlink to open the **Group Details** window, then click the **Members** tab.
- Step 3** If you want to make changes to these groups, see:
- [View and Change the Tasks a Group Can Perform, on page 180](#)
 - [View and Change the Groups a User Belongs To, on page 160](#)
-

User Group Permissions and Task Description

The following table describes user group permissions and task descriptions.

Table 12: User Group Permissions and Task Description

Task Group Name	Task Name	Description
APIC-EM Controller	Apic Controller Read Access	Allows user to read APIC-EM controller details.
	Apic Controller Write Access	Allows user to create or update APIC-EM controller details.
	Apic Global PnP Read Access	Allows user to read the Apic Global PnP/Ztd settings.
	Apic Global PnP Write Access	Allows user to create or update the Apic Global PnP/Ztd settings.
Active Sessions	Force Logout Access	Allows user to force logout other user active sessions.

Task Group Name	Task Name	Description
Administrative Operations	Appliance	Gives the user access to the Administration > Settings > Appliance menu.
	Application Server Management Access	Allows user to manage NAM server lists.
	Application and Services Access	Allows user to create, modify, and delete custom applications and services.
	Data Migration	
	Design Endpoint Site Association Access	Allows user to create Assurance site classification rules.
	Device Detail UDF	Allows user to access Device details UDF.
	Export Audit Logs Access	Allows user to access Import Policy Update through Admin Mega menu.
	Health Monitor Details	Allows user to modify Site Health Score definitions.
	High Availability Configuration	Allows user to configure High Availability for pairing primary and secondary servers.
	Import Policy Update	Allow user to manually download and import the policy updates into the compliance and Audit manager engine.
	License Center/Smart License	Allows user to access license center/smart license..
	Logging	Gives access to the menu item which allows user to configure the logging levels for the product.
	Scheduled Tasks and Data Collection	Controls access to the screen to view the background tasks.
	System Settings	Controls access to the Administration > System Settings menu.
Tools	Allows user to access the Administration > System Settings menu.	

Task Group Name	Task Name	Description
	User Preferences	Controls access to the Administration > User Preference menu.
	View Audit Logs Access	Allows user to view Network and System audits.
Alerts and Events	Ack and Unack Alerts	Allows user to acknowledge or unacknowledge existing alarms.
	Alarm Policies	Allows user to access alarm policies.
	Alarm Policies Edit Access	Allows user to edit alarm policies.
	Delete and Clear Alerts	Allows user to clear and delete active alarms.
	Notification Policies Read Access	Allows user to view alarm notification policy.
	Notification Policies Read-Write Access	Allows user to configure alarm notification policy.
	Pick and Unpick Alerts	Allows user to pick and unpick alerts.
	Syslog Policies	Grants access to the Syslog Policies page.
	Syslog Policies Edit Access	Allows creating, modifying and deleting syslog policies.
	Troubleshoot	Allows user to do basic troubleshooting, such as traceroute and ping, on alarms.
	View Alert Condition	Allows user to view alert condition.
View Alerts and Events	Allows user to view a list of events and alarms.	
Configuration Archive	Configuration Archive Read-Only Task	Allows user to view the archived configurations and schedule configuration archive collection jobs.
	Configuration Archive Read-Write Task	Allows user to perform all configuration archive jobs.
Diagnostic Tasks	Diagnostic Information	Controls access to diagnostic page.

Task Group Name	Task Name	Description
Feedback and Support Tasks	Automated Feedback	Allows access to automatic feedback.
	TAC Case Management Tool	Allows user to open a TAC case.
Global Variable Configuration	Global Variable Access	Allows user to access global variables.
Groups Management	Add Group Members	Allows user to add an entity, such as a device or port, to groups.
	Add Groups	Allows user to create groups.
	Delete Group Members	Allows user to remove members from groups.
	Delete Groups	Allows user to delete groups.
	Export Groups	Allows user to export groups.
	Import Groups	Allows user to export groups.
	Modify Groups	Allows user to edit group attributes such as name, parent, and rules.

Task Group Name	Task Name	Description
Job Management	Approve Job	Allows user to submit a job for approval by another user.
	Cancel Job	Allows user to cancel the running jobs.
	Delete Job	Allows user to delete jobs from job dashboard.
	Edit Job	Allows user to edit jobs from job dashboard.
	Pause Job	Allows user to pause running and system jobs.
	Schedule Job	Allows user to schedule jobs.
	View Job	Allows user to schedule jobs.
	Config Deploy Edit Job	Allows user to edit config deployed jobs.
	Device Config Backup Job Edit Access	Allows user to change the external backup settings such as repository and file encryption password.
	Job Notification Mail	Allows user to configure notification mails for various job types.
	Run Job	Allows user to run paused and scheduled jobs.
	System Jobs Tab Access	Allows user to view the system jobs.
Maps	Client Location	Allows user to view client locations on Map.
	Maps Read Only	Allows user to view the map in a read-only mode.
	Maps Read Write	Allows user to view and also manipulate elements within the maps such as AP placement.
	Planning Mode	Allows user to launch the planning mode tool.
	Rogue Location	Allows user to view rogue AP locations on Map

Task Group Name	Task Name	Description
Mobility Services	Mobility Service Management	Allows user to edit properties and parameters, view session and Trap destinations,manage user and group accoounts,and monitor status information for mobility services engine.
	View CAS Notifications Only	Allows user to view the CAS notifications

Task Group Name	Task Name	Description
Network Configuration	Add Device Access	Allows user to add devices to Prime Infrastructure.
	Admin Templates Write Access	Check this check-box for enabling admin templates write access for user defined role.
	Auto Provisioning	Allows access to auto provisioning.
	Compliance Audit Fix Access	Allows user to view, schedule and export compliance fix job/ report.
	Compliance Audit PAS Access	Allows user to view, schedule and export "PSIRT" and "EOX" job/ report
	Compliance Audit Policy Access	Allows user to create, modify, delete, import and export compliance policy.
	Compliance Audit Profile Access	Allows user to view, schedule and export compliance audit job or report view and download violations summary.
	Compliance Audit Profile Edit Access	Allows user to create, modify and delete compliance profiles view and schedule export compliance audit job or report view and download violations summary.
	Configuration Templates Read Access	Allows to access configuration templates in read only mode.
	Configure ACS View Servers	Allows access to manage ACS View Servers.
	Configure Access Points	Allows users to configure access points.
	Configure Autonomous Access Point Templates	Allows access to configure Autonomous AP Templates on Prime Infrastructure.
	Configure Choke Points	Allows users to Configure Choke Points.
	Configure Config Groups	Allows access to Config Groups.
	Configure Controllers	Allows users to configure the Wireless Controller features.

Task Group Name	Task Name	Description
	Configure Ethernet Switch Ports	Controls access to the config ability when viewing ethernet details in DWC for any device.
	Configure Ethernet Switches	Controls access to the config ability when viewing ethernet details in DWC for any device.
	Configure ISE Servers	Allows users to manage ISE servers on Prime Infrastructure
	Configure Lightweight Access Point Templates	Allows users to configure Lightweight Access Point Templates on Prime Infrastructure
	Configure Mobility Devices	Allows user to configure the CAS,WIPS,Mobile concierge service, location analytics service, and provide the mobility procedures
	Configure Spectrum Experts	Allows users to Configure Spectrum Experts.
	Configure Switch Location Configuration Templates	Allow the user to modify Configuration templates
	Configure Templates	Allow the user to do the CRUD operation of Feature Templates on DWC and configuration Template
	Configure Third Party Controllers and Access Point	Allows users to configure Third Party Controllers and Access Points on Prime Infrastructure.
	Configure WIPS Profiles	Allows users to access WIPS Profiles.
	Configure WiFi TDOA Receivers	Allows users to configure WiFi TDOA Receivers.
	Credential Profile Add_Edit Access	Allows user to Add and edit credential profile.
	Credential Profile Delete Access	Allows user to delete credential profile.
	Credential Profile View Access	Allows user to view credential profile.
	Delete Device Access	Allows user to delete devices from Prime Infrastructure.

Task Group Name	Task Name	Description
	Deploy Configuring Access	Allows user to deploy Configuration and IWAN templates.
	Design Configuration Template Access	Allows user to create Configuration > Shared Policy Object templates and Configuration Group templates.
	Device Bulk Import Access	Allows user to perform bulk import of devices from CSV files.
	Device View configuration Access	Allows user to configure devices in the Device Work Center.
	Edit Device Access	Allows user to edit device credentials and other device details.
	Export Device Access	Allows user to export the list of devices, including credentials, as a CSV file.
	Global SSID Groups	Allows users to configure Global SSID Groups.
	Migration Templates	Allows user to create autonomous AP migration templates
	Network Devices	Allows user to access to the Network devices.
	Network Topology Edit	Allows user to create devices, links and network in the topology map, edit the manually created link to assign the interfaces.
	Scheduled Configuration Tasks	Allows user to create and schedule a configuration template, configuration group, software download task and template.
	TrustSec Readiness Assessment	Access to the TrustSec menu which allows users to configure TrustSec in their network.
	View Compute Devices	Access to Data Center compute servers and virtual elements such as Hosts and Virtual Machines managed in Prime Infrastructure.
	WIPS Service	

Task Group Name	Task Name	Description
		Allows users to configure WIPS Service.
	Wireless Security	Allows user to configure Rogue Policy, Rogur Rule and wIPS profile using Wireless Security Configuration wizard.

Task Group Name	Task Name	Description
Network Monitoring	Ack and Unack Security Index Issues	Allows users to Acknowledge or Unacknowledge Security Index Violations.
	Admin Dashboard Access	Allows user to access the Admin Dashboard.
	Config Audit Dashboard	Allows users to access Config Audit Dashboard.
	Data Collection Management Access	Allow user to access the Assurance Data Sources page.
	Details Dashboard Access	Allow user to access the Detail dashboards.
	Disable Clients	Allows users to access Disabled Clients page.
	Identify Unknown Users	Allows users to access Identify Unknown Users page.
	Incidents Alarms Events Access	Allows user to access incidents alarms events.
	Latest Config Audit Report	Allows user to view the latest config audit reports.
	Lync Monitoring Access	Allows the user to access and view the Lync monitoring page
	Monitor Access Points	Allows users to view Monitor Access Points page.
	Monitor Chokepoints	Allows users to access Monitor Chokepoints page.
	Monitor Clients	Allows users to access Monitor Clients page.
	Monitor Ethernet Switches	Allows user to monitor ethernet interfaces,VLAN switch port,and VLAN trunk of ethernet switches.
	Monitor Interferers	Allows users to access Monitor Interferers pages.
Monitor Media Streams		

Task Group Name	Task Name	Description
		Allows user to monitor the media stream configuration information such as name, start and end address ,maximum bandwidth,operational status,average packet size,RRC updates, priority and violation.
	Monitor Mobility Devices	Allows user to monitor mobility group events such as mobility statistics,mobility responder statistics,mobility initiator statistics.
	Monitor Security	Allows user to monitor controller security information such as RADIUS authentication,RADIUS accounting,management frame protection,Rogue AP rules and guest users.
	Monitor Spectrum Experts	Allows users to monitor spectrum experts.
	Monitor Tags	Allows user to monitor tags.
	Monitor Third Party Controllers and Access Point	Allows users to access Monitor Third Party Controllers and Access Point pages.
	Monitor WiFi TDOA Receivers	Allows users to access Monitor WiFi TDOA Receivers pages.
	Monitoring Policies	Allows user to identify the most used rules, troubleshoot a specific rule, and verify hits for the selected rule.
	Network Topology	Allows users to launch the Network Topology map and view the devices and links in the map.
	Packet Capture Access	Allow user to initiate packet captures on NAM and supported routers.
	Performance Dashboard Access	Allow user to access the Performance dashboard.
	PfR Monitoring Access	Allows the user to access and view the PfR Monitoring page
	RRM Dashboard	Allows users to access RRM Dashboard page.

Task Group Name	Task Name	Description
	Remove Clients	Allows users to access Remove Clients page.
	Service Health Access	Allows the user to access and view the Service Health page.
	Site Visibility Access	Allows user to access site visibility.
	Track Clients	Allows users to access Track Clients page.
	View Security Index Issues	Allows users to access Security Index Issues page.
	Voice Diagnostics	Allows users to access Voice Diagnostics information.
	Wireless Dashboard Access	Allows user to view the wireless dashboard.
Operations Center Tasks	Administrative privileges under Manage and Monitor Servers page	Allows for administrative tasks such as Add/Delete/Edit/Activate and deactivate of servers under M&M page.
	Allow report/dashlet use for users with only NBI Read access	Enable this option for users with NBI Read access so they can generate reports and populate all dashlets.
	Manage and Monitor Servers Page Access	Allows access to the Manage & Monitor Servers Page.

Task Group Name	Task Name	Description
Plug n Play Configuration	PnP Deploy History Read Access	Allows user to read provisioned devices status.
	PnP Deploy History Read-Write Access	Allows user to read and delete operations on provisioned devices.
	PnP Preferences Read Access	Allows user to view Plug and Play preferences.
	PnP Preferences Read-Write Access	Allows user to edit Plug and Play preferences.
	PnP Profile Deploy Read Access	Allows user to view Plug and Play provisioning profiles.
	PnP Profile Deploy Read-Write Access	Allow user to create, modify, and delete Plug and Play provisioning profiles.
	PnP Profile Read Access	Allow user to view Plug and Play profiles.
	PnP Profile Read-Write Access	Allow user to create, delete, and modify Plug and Play profiles.
	WorkflowsReadWriteAccess	Allows user to set up configure the cisco IOS switches and access devices
Product Usage	Product Feedback	Allows the user to access the Help Us Improve page.

Task Group Name	Task Name	Description
Reports	Autonomous AP Reports	Allows user to create new Autonomous AP Reports.
	Autonomous AP Reports Read Only	Allows user to view Autonomous AP Reports
	CleanAir Reports	Allows user to create new CleanAir Reports.
	CleanAir Reports Read Only	Allows user to view CleanAir Reports
	Client Reports	Allow user to create Client Reports
	Client Reports Read Only	Allow user to view Client Reports.
	Compliance Reports	Allows user to customize the configuration audit ,network discrepancy,PCI DSS detailed and PCI DSS summary reports,PSIRT detailed and PSIRT summary reports.
	Compliance Reports Read Only	Allows user to configuration audit,network discrepancy,PCI DSS detailed and PCI DSS summary reports,PSIRT detailed and PSIRT summary reports.
	Context Aware Reports	Allows user to run context aware/location-specific reports.
	Context Aware Reports Read Only	Allows user to run context aware/location-specific reports.
	Custom Composite Report	Allow user to create 'custom' report with two or more (upto 5 reports) existing report templates into a single report.
	Custom NetFlow Reports	Allow user to access custom NetFlow reports
	Custom NetFlow Reports Read Only	Allow user to view custom NetFlow reports.
	Device Reports	Allow user to run reports specific to monitoring specific report related to Devices.
Device Reports Read Only	Allows user to read generated device reports	

Task Group Name	Task Name	Description
	Guest Reports	Allow user to create Guest Reports
	Guest Reports Read Only	Allow user to view Guest Reports.
	MSAP Reports	Allows user to run Mobile Concierge reports.
	MSAP Reports Read Only	Allows user to run Mobile Concierge reports.
	Mesh Reports	Allow user to create Mesh Reports.
	Mesh Reports Read Only	Allow user to view Mesh Reports.
	Network Summary Reports	Allows user to create and run network summary reports
	Network Summary Reports Read Only	Allows user to view all Summary reports.
	Performance Reports	Allows user to create performance reports.
	Performance Reports Read Only	Allows user to view performance reports.
	Raw NetFlow Reports	Allows user to view NetFlow reports.
	Raw NetFlow Reports Read Only	Allows user to view Raw NetFlow reports.
	Report Launch Pad	Allows user to access the Report page.
	Report Run History	Allows user to view report history.
	Run Reports List	Allows user to run reports.
	Saved Reports List	Allows user to save reports.
	Saved Reports List Read Only	Allows user to view saved reports.
	Security Reports	Allows user to create Security Reports.
	Security Reports Read Only	Allows users to view wireless security reports related to rogue APs, wIPS etc.
	Virtual Domains List	Allows user to create the Virtual Domain related report.
	Voice Audit Report	

Task Group Name	Task Name	Description
		Allows user to create the Virtual Domain related report
Software Image Management	Add Software Image Management Servers	Allows user to add software imagemanagement servers.
	Software Image Access Privilege	Allows user to access Inventory > Software Images.
	Software Image Activation	Allows user to upgrade and downgrade software versions to manage devices in their network.
	Software Image Collection	Allows user to collect images from different locations such as from devices, Cisco.com or from URLs.
	Software Image Delete	Allows user to delete an image from the Software Images page, except for images that are included in Plug and Play profiles.
	Software Image Details View	Allows user to view the image details.
	Software Image Distribution	Allows user to distribute software verisons to managed devices in the network.
	Software Image Info Update	Allows the user to edit and save image properties such as minimum RAM, minimum FLASH and minimum boot ROM version.
	Software Image Management Server-Managed Protocols	Allows user to manage protocol
	Software Image Preference Save	Allows user to save preference options on Software Images page.
	Software Image Recommendation	Allows user to recommend images from Cisco.com and from the local repository.
Software Image Upgrade Analysis	Allows user to analyze software images to determine if the hardware upgrades (boot ROM, flash memory, RAM, and boot flash, if applicable) are required before performing a software upgrade.	

Task Group Name	Task Name	Description
User Administration	Audit Trails	Allows user to access the Audit trails on user login and logout.
	RADIUS Servers	Allows user to access the RADIUS Servers menu.
	SSO Server AAA Mode	Allows user to access the AAA menu
	SSO Servers	Allows user to access the SSO menu
	TACACS+ Servers	Allows user to access the TACACS+ Servers menu
	Users and Groups	Allows user to access the Users and Groups menu.
	Virtual Domain Management	Allows user to access the Virtual Domain Management menu.
	Virtual Elements Tab Access	When creating virtual domain or adding members to a virtual domain, allows uses to access the virtual elements tab, so as to allow user to add virtual elements (Datacenters, Clusters and Hosts) to virtual domain.
View Online Help	OnlineHelp	Allows user to access the Prime Infrastructure online help.

Create a Customized User Group

provides a set of predefined user groups that help you control user authorization. These groups are described in [Types of User Groups, on page 157](#) and include four User Defined groups which you can customize to create a user group that is specific to your deployment. The following procedure explains how to create a customized group using one of the four predefined User Defined group templates.

-
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **User Groups**.
 - Step 2** Locate a User Defined group that has no members, then click its group name hyperlink.
 - Step 3** Customize the group permissions by checking and unchecking tasks in the **Group Detail** window. If a task is greyed-out, it means you cannot adjust its setting. You cannot change the group name.
 - Step 4** Click **Save** to save your group settings.
 - Step 5** Add members to your group by editing the relevant user accounts and adding the user to your new group. See [Add and Delete Users, on page 183](#) for information on adjusting user accounts.
-

Add User with Wireless Persona

You can add a local user with wireless persona so that the user can view only wireless related navigation menu items.



Note You cannot add AAA user or remote user with wireless persona.

-
- Step 1** Log in to Cisco Prime Infrastructure as an administrator.
- Step 2** Choose **Administration** > **Users** > **Users, Roles & AAA**, then choose **Users**.
- Step 3** From the **Select a command** drop-down list, choose **Add User**, then click **Go**.
- Step 4** Configure the user account.
- Enter a username and password.
 - Control the actions the user can perform by selecting one or more user groups. For descriptions of user groups, see [View User Groups and Their Members, on page 160](#).
 - Control the devices a user can access by clicking the **Virtual Domains** tab and assigning domains to the user. For more information, see [Create Virtual Domains to Control User Access to Devices, on page 193](#).
- Step 5** In the **Persona** pane, check the **Wireless** check box. Hover your mouse cursor over the help text question mark to view the menu items that are removed from the navigation.
- Step 6** Click **Save**.
-



Note The following user groups do not support the wireless persona-based menu:

1. Root
 2. Lobby Ambassador
 3. Lobby Ambassador + NBI Credential
 4. Lobby Ambassador + NBI Read
 5. Lobby Ambassador + NBI Write
 6. Lobby Ambassador + (NBI Credential + NBI Read)
 7. Lobby Ambassador + (NBI Read + NBI Write)
 8. Lobby Ambassador + (NBI Credential + NBI Write)
 9. Lobby Ambassador + (NBI Credential + NBI Read + NBI Write)
 10. Help Desk Admin
 11. Help Desk Admin + NBI Credential
 12. Help Desk Admin + NBI Read
 13. Help Desk Admin + NBI Writer
 14. Help Desk Admin + (NBI Credential + NBI Read)
 15. Help Desk Admin + (NBI Read + NBI Write)
 16. Help Desk Admin + (NBI Credential + NBI Write)
 17. Help Desk Admin + (NBI Credential + NBI Read + NBI Write)
 18. mDNS Policy Admin
-

View and Change the Tasks a Group Can Perform

Follow these steps to get information about existing user groups and the tasks group members can perform. The predefined user groups are described in [View User Groups and Their Members, on page 160](#).



Note If you want to change *device* access, see [Assign Virtual Domains to Users, on page 198](#).

Step 1 Choose **Administration > Users > Users, Roles & AAA**, then choose **User Groups**.

The User Groups page lists all existing user groups.

Step 2 Click a user group hyperlink. The **Group Detail** window lists the group permissions.

- A checked task means group members have permission to perform that task. If a checked box is greyed-out, it means you cannot disable the task.
- A blank check box means group members cannot perform that task. If a blank check box is greyed out, it means you cannot enable the task for the user group.

The web GUI root and Monitor Lite groups, and the NBI groups, are not editable.

Step 3 If you want to change the group permissions—which will affect *all group members*—check and uncheck tasks, then click **Save**.

Use User Groups with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the user groups that exist in . You can do this using the procedure in [Export the User Group and Role Attributes for RADIUS and TACACS+](#), on page 181.

Export the User Group and Role Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all user group and role information into your Cisco Access Control Server (ACS) or Cisco Identity Services Engine (ISE) server. You can do this using the Task List dialog box provided in the web GUI. If you do not export the data into your Cisco ACS or Cisco ISE server, will not allow users to perform their assigned tasks.

The following information must be exported:

- TACACS+—Requires virtual domain and role information (tasks are automatically added).
- RADIUS—Requires virtual domain and role information (tasks are automatically added).

Information in the Task List dialog is preformatted for use with the Cisco ACS server.



Note When you add tasks to the external server, be sure to add the **Home Menu Access** task. It is mandatory for all users.

Before you begin

Make sure you have added the AAA server and configured the AAA mode as explained in [Configure External Authentication, on page 201](#).

Step 1

In :

- a) Choose **Administration > Users > User Groups**.
- b) From the User Groups table, copy the role for each user group by clicking the **Task List** hyperlink (at the end of a user group row).
 - If you are using RADIUS, right-click the *role0 line* in the RADIUS Custom Attributes field and choose **Copy**.
 - If you are using TACACS+, right-click the *role0 line* in the TACACS+ Custom Attributes field and choose **Copy**.

- Step 2** Paste the information into your Cisco ACS or Cisco ISE server. These steps show how to add the information to an existing user group in Cisco ACS. If you have not yet added this information to Cisco ACS or Cisco ISE, see:
- [Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 208](#)
 - [Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 203](#)
- a) Navigate to **User or Group Setup**.
 - b) For the applicable user or group, click **Edit Settings**.
 - c) Paste the attributes list into the appropriate text box.
 - d) Select the check boxes to enable these attributes, then click **Submit + Restart**.
-

Add Users and Manage User Accounts

- [Create Web GUI Users with Administrator Privileges, on page 183](#)
- [Add and Delete Users, on page 183](#)
- [Disable \(Lock\) a User Account, on page 184](#)
- [Change a User's Password, on page 184](#)

Change User Group Memberships

You can quickly change a user's privileges in Prime Infrastructure by changing the user groups to which the user belongs.

You can also assign sites or devices to which a virtual domain has access. For details, see “Create Virtual Domains to Control User Access to Devices ” in Related Topics.

Prime Infrastructure will not permit certain combinations of user group membership. For example, a user cannot be a member of the “Root” and “Lobby Ambassador” user groups at the same time (for details, see the table in “Control the Tasks Users Can Perform (User Groups) ”, in Related Topics). If you are using RADIUS to authenticate Prime Infrastructure users, make sure that you do not insert invalid user-group membership combinations into the RADIUS user attribute/value pairs.

-
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 3** Click on the user name for the user whose memberships you want to change. The User Details page appears.
- Step 4** On the General tab, under **Groups Assigned to This User**:
- Select the checkbox next to each user group to which you want the user to belong.
 - Unselect the checkbox next to each user group from which you want the user to be removed.
- Step 5** When you are finished, click **Save**.

Related Topics

- [Control the Tasks Users Can Perform \(User Groups\), on page 157](#)
- [View and Change the Tasks a Group Can Perform, on page 180](#)

[Create Virtual Domains to Control User Access to Devices](#), on page 193

Create Web GUI Users with Administrator Privileges

After installation, has a web GUI root account named **root**. This account is used for first-time login to the server to create:

- Web GUI users with Administrator privileges who will manage the product and features
- All other user accounts

You should *not* use the web GUI root account for normal operations. For security purposes, create a new web GUI user with Administrator privileges (and access to all devices), and then disable the web GUI root account.

-
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **Users**.
- Step 2**
- Step 3** Complete the required fields.
- Step 4** In the **General** tab under **Groups Assigned to This User**, click **Admin**.
- Step 5** Click the **Virtual Domains** tab to specify which devices the user can access. You should have at least one Admin web GUI user that has access to all devices (ROOT-DOMAIN). For more information on virtual domains, see [Create Virtual Domains to Control User Access to Devices](#), on page 193.
- Step 6** Click **Save**.
-

What to do next

If you have not done so already, for security purposes, disable the web GUI root account as described in [Disable and Enable the Web GUI root User](#), on page 157.

Add and Delete Users

Before you create user accounts, create virtual domains to control device access so you can apply them during account creation. Otherwise you will have to edit the user account to add the domain access. See [Create Virtual Domains to Control User Access to Devices](#), on page 193.

If you want to temporarily disable an account (rather than delete it), see [Disable \(Lock\) a User Account](#), on page 184.

-
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **Users**.
- Step 2** .
- Step 3** Configure the user account.
- a) Enter a username and password.
 - b) Enter the first name, last name, and a description for the user.
 - c) Control the actions the user can perform by selecting one or more user groups. For descriptions of user groups, see [View User Groups and Their Members](#), on page 160.
 - d) Control the devices a user can access by clicking the **Virtual Domains** tab and assigning domains to the user. (see [Create Virtual Domains to Control User Access to Devices](#), on page 193).

- Step 4** Click **Save**.
- Step 5** To delete a user account, select a user, .

Disable (Lock) a User Account

Disable a user account when you temporarily want to disallow a user from logging in to the GUI. You might want to do this if a user is temporarily changing job functions. If the user tries to log in, displays a message saying the login failed because the account is locked. You can unlock the account later without having to re-create the user. If you want to delete a user account, see [Add and Delete Users, on page 183](#).

User accounts may be disabled automatically if the password is not changed before expiration. Only an administrator can reset the password in this case. See [Change a User's Password, on page 184](#) and [Configure Global Password Policies for Local Authentication, on page 191](#).

- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then click **Users**.
- Step 2** Select the user whose access you want to disable or enable.
- Step 3** From the **Select a command** drop-down list, select **Lock User(s)** (or **Unlock User(s)**), then click **Go**.

Change a User's Password

You can force users to change their passwords on a regular basis using password rules (see [Configure Global Password Policies for Local Authentication, on page 191](#)). Users can change their own passwords . If you need to make an immediate change to a user's password, use this procedure.

- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then click **Users**.
- Step 2** Click the username hyperlink.
- Step 3** Enter the new password in the password fields, then click **Save**.

Configure Guest Account Settings

Prime Infrastructure administrators can choose to:

- Force all expired guest accounts to be deleted automatically.
- Limit Lobby Ambassadors' control over guest accounts to just those accounts they have created.

Both of these options impose restrictions on the latitude lobby ambassadors have to manage these temporary guest accounts. For details on using lobby ambassador accounts, see "Using Lobby Ambassadors to Manage Guest User Accounts" in Related Topics.

- Step 1** Log in to Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Settings > System Settings > General > Guest Account**.

Step 3 Change radio button selections as follows:

- Select **Automatically remove expired guest accounts** to have guest accounts whose lifetimes have ended moved to the Expired state. Guest accounts in the Expired state are deleted from Prime Infrastructure automatically.
- Select **Search and List only guest accounts created by this lobby ambassador** to restrict Lobby Ambassadors to modifying only the guest accounts that they have created. By default, any Lobby Ambassador can modify or delete any guest account, irrespective of who created that account.

Step 4 Click **Save**.

Related Topics

[Use Lobby Ambassadors to Manage Guest User Accounts](#), on page 185

[Control the Tasks Users Can Perform \(User Groups\)](#), on page 157

[Create Virtual Domains to Control User Access to Devices](#), on page 193

Use Lobby Ambassadors to Manage Guest User Accounts

Lobby ambassador accounts are a special kind of Prime Infrastructure administrative account used to add, manage and retire temporary guest user accounts. Lobby ambassador accounts have very limited network configuration privileges specified in the lobby ambassador profile, and have access only to those Prime Infrastructure functions used to manage guest accounts.

Typically, an enterprise-supplied guest network allows access to the Internet for a guest without compromising the enterprise's hosts. Web authentication is usually provided without a specialized client, so most guests will need to initiate a VPN tunnel to their desired destination.

Prime Infrastructure permits both wired and wireless guest user access. 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 may be available via a guest office or through 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.

The lobby ambassador can create the following types of guest user accounts:

- A guest user account with a limited lifetime. After the specified time period, the guest user account automatically expires.
- A guest user account with an unlimited lifetime. This account never expires.
- A guest user account that is activated at a predefined time in the future. The lobby ambassador defines the beginning and end of the valid time period.

Related Topics

[Manage Guest User Accounts: Workflows](#), on page 186

[Save Guest Accounts on a Device](#), on page 189

[Edit Guest User Credentials](#), on page 189

Manage Guest User Accounts: Workflows

Lobby ambassadors can manage guest user accounts following this workflow

1. Create guest user accounts—While logged in as a lobby ambassador, create guest user accounts as needed.
2. Schedule guest user accounts—While logged in as a lobby ambassador, schedule automatic creation of guest user accounts.
3. Print or email guest user details—While logged in as a Lobby Ambassador, print or email the guest user account details to the host or person who will be welcoming the guests.

Prime Infrastructure administrators with full access can manage lobby ambassadors and their work using this workflow:

1. Create lobby ambassador accounts—While logged in as a Prime Infrastructure administrator, create lobby ambassador accounts as needed.
2. View lobby ambassador activities—While logged in as a Prime Infrastructure administrator, supervise the lobby ambassador's activities using the log.

[Create Lobby Ambassador Accounts](#), on page 186

[Create Guest User Accounts as a Lobby Ambassador](#), on page 187

[Schedule Guest User Accounts](#), on page 187

[Print or Email Guest User Details](#), on page 188

[View Lobby Ambassador Activities](#), on page 188

Create Lobby Ambassador Accounts

Before you begin creating Lobby Ambassador accounts, you must ensure that you have proper time settings on the devices (if you do not, you will incorrect account lifetimes on Guest User accounts after they are discovered).

-
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users, Roles & AAA > Users**.
- Step 3** Choose **Select a command > Add User > Go**.
- Step 4** Complete the required fields as follows:
- a) In the *Groups Assigned to this User* section, select the **Lobby Ambassador** check box to access the Lobby Ambassador Defaults tab.
 - b) Complete the required fields on the Lobby Ambassador Defaults tab.
 - c) Click the Virtual Domains tab to assign a virtual domain for this lobby ambassador account.
 - d) In the **Available Virtual Domains** list, click to highlight the virtual domain you want this user to access. Then click Add to add it to the Selected Virtual Domains list.
- Step 5** Click **Save**.

Related Topics

[Manage Guest User Accounts: Workflows](#), on page 186

[Save Guest Accounts on a Device](#), on page 189

[Edit Guest User Credentials](#), on page 189

Login as a Lobby Ambassador

You must use the lobby ambassador username and password to log into the Prime Infrastructure user interface. When you log in as a lobby ambassador, the Guest User page appears and provides a summary of all created Guest Users.

Related Topics

[Manage Guest User Accounts: Workflows](#), on page 186

[Save Guest Accounts on a Device](#), on page 189

[Edit Guest User Credentials](#), on page 189

Create Guest User Accounts as a Lobby Ambassador

- Step 1** Log in to Prime Infrastructure as a lobby ambassador.
- Step 2** Choose **Select a command > Add User Group > Go**.
- Step 3** Complete the required fields on the **General** and **Advanced** tabs.
See reference guide for field descriptions.
- Step 4** Click **Save**.
-

Related Topics

[Manage Guest User Accounts: Workflows](#), on page 186

[Save Guest Accounts on a Device](#), on page 189

[Edit Guest User Credentials](#), on page 189

Schedule Guest User Accounts

- Step 1** Log in to Prime Infrastructure as a lobby ambassador.
- Step 2** Choose **Select a command > Schedule Guest User > Go**.
- Step 3** **Configure the required** parameters:

If the **Generate new password on every schedule** and **No. days of the week** check boxes are selected, then the user will have one password for the entire time the account is active.

If the **Generate new password on every schedule** and **Any days of the week** check boxes are selected, then the user will have a new password for each day.
- Step 4** Click **Save**.
-

Related Topics

[Manage Guest User Accounts: Workflows](#), on page 186

[Save Guest Accounts on a Device](#), on page 189

[Edit Guest User Credentials](#), on page 189

Print or Email Guest User Details

The lobby ambassador can print or e-mail the guest user account details to the host or person who welcomes guests. The email or printed sheet will show the following account details:

- Guest user account name.
- Password for the guest user account.
- Start date and time when the guest user account becomes active.
- End date and time when the guest user account expires.
- Profile ID assigned to the guest user. Your administrator can advise which Profile ID to use.
- Disclaimer information for the guest user.

Step 1 Log in to Prime Infrastructure as a lobby ambassador.

Step 2 On the Guest User page, select the check box next to the user name whose account details you want to send.

Step 3 Choose **Select a command > Print/E-mail User Details > Go**. Then proceed as follows:

- If you are printing, click **Print**. From the **Print** page, select a printer, and click **Print**.
- If emailing, click **Email**. From the Email page, enter the subject-line text and the email address of the recipient, then click **Send**.

Related Topics

[Manage Guest User Accounts: Workflows](#), on page 186

[Save Guest Accounts on a Device](#), on page 189

[Edit Guest User Credentials](#), on page 189

View Lobby Ambassador Activities

Prime Infrastructure administrators can supervise lobby ambassadors using the Audit Trail feature.

Step 1 Log into Prime Infrastructure as an administrator.

Step 2 Choose **Administration > Users > Users, Roles & AAA > User Groups**.

Step 3 Click the **Audit Trail** icon for the lobby ambassador account you want to view. The Audit Trail page for the lobby ambassador appears. This page enables you to view a list of lobby ambassador activities over time.

- User login name
- Type of operation audited
- Time when the operation was audited
- Login success or failure
- Indicates the reason for any login failure (for example, “invalid password”).

Related Topics

[Manage Guest User Accounts: Workflows](#), on page 186

[Save Guest Accounts on a Device](#), on page 189

[Edit Guest User Credentials](#), on page 189

Save Guest Accounts on a Device

-
- Step 1** Log into Prime Infrastructure as a lobby ambassador.
- Step 2** On the Guest User page, choose **Save Guest Accounts on Device** check box to save guest accounts to a Cisco Wireless LAN Controller (WLC) flash so that they are maintained across WLC reboots.

Related Topics

[Manage Guest User Accounts: Workflows](#), on page 186

[Edit Guest User Credentials](#), on page 189

Edit Guest User Credentials

-
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 3** Click the user name whose credentials you want to edit.
- Step 4** Modify the required credentials.
- While editing, if the *Profile* selection is removed (changed to *Select a profile*), the defaults are removed for this lobby ambassador. The user must reconfigure the defaults to reinforce them.
- Step 5** Click Save.

Related Topics

[Manage Guest User Accounts: Workflows](#), on page 186

[Save Guest Accounts on a Device](#), on page 189

Find Out Which Users Are Currently Logged In

Use this procedure to find out who is currently logged into the server. You can also view a historical list of the actions performed by the user in the current web GUI session and past sessions.

-
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **Active Sessions**. lists all users that are currently logged in to the server, including their client machine IP address. If the user performed any actions on managed devices (for example, the user added new devices to), the device IP addresses are listed in the Device IP Address column.
- Step 2** To view a historical list of all actions performed by this user, click the Audit Trail icon that corresponds to the user name.
-

View the Tasks Performed By Users (Audit Trail)

maintains a history of all actions performed by users in active and past web GUI sessions. Follow these steps to view a historical list of tasks performed by a specific *user* or by all members of a specific *user group*. The audit information includes a description of the task, the IP address of the client from which the user performed the task, and the time at which the task was performed. If a task affects a managed device (for example, a user adds a new device), the affected device's IP address is listed in the Device IP Address column. If a change is made to multiple devices (for example, a user deploys a configuration template to 10 switches), displays an audit entry for each switch.

To find out which users are currently logged into the web GUI, see [Find Out Which Users Are Currently Logged In, on page 189](#).

To view audits that are not user-specific, see these topics:

- [Audit Actions Executed from the GUI \(System Audit\), on page 233](#)
- [Audit Configuration Archive and Software Management Changes \(\) , on page 231](#)
- [Audit Changes Made By Users \(Change Audit\), on page 231](#)

-
- Step 1** Choose **Administration > Users > Users, Roles & AAA**.
- Step 2** To view the tasks performed by a specific user:
- a. Choose **Users**.
 - b. Locate the user name, then click the Audit Trail icon corresponding to that user.
- Step 3** To view a historical list of the tasks performed by all members of a user group:
- a. Choose **User Groups**.
 - b. Locate the user group name, then click the Audit Trail icon corresponding to that group.
-

Configure Job Approvers and Approve Jobs

Use job approval when you want to control jobs that could significantly impact the network. If a job requires approval, sends an e-mail to and does not run the job until one of them approves it. If a job is rejected by an approver, the job is removed from the database. By default, all jobs do not require approval.

If job approval is already enabled and you want to view jobs that need approval, approve a job, or reject a job, choose **Administration > Settings > System Settings**, then choose **General > Job Approval**.

To enable job approval and configure the jobs that require approval before running:

-
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Job Approval**.
- Step 2** Check the **Enable Job Approval** check box.

- Step 3** Find the jobs you want to configure for approval, and move them from the left field to the right field.
- Step 4** Click **Save**.

Configure Job Notification Mail for User Jobs

You can configure to send job notification mail for every user job if the **Last_Run_Status** shows: **Failure** and **Success**. Use this procedure to configure the job notification mail settings for user jobs.

-
- Step 1** Select **Administration > Settings > System Settings**, then choose **Mail and Notification > Job Notification Mail**.
- Step 2** Check the **Enable Job Notification Mail** check box to enable notifications.
- Step 3** Enter the email addresses in the **To** text box. By default, the email address configured in the **Mail Server Configuration** settings or the pre-configured email addresses appear in the **To** text box. You can configure an email server by performing the steps explained in [Configure Email Server Settings](#), on page 357
- Step 4** Enter the subject of the job notification mail in the **Subject** text box. The subject is automatically appended by the job name.
- Step 5** Select the **Job Status**. You can select any one of the two options or both the options.
- Step 6** Select the **Compliance Audit Job** and **Compliance Fix Job** check boxes. The job notification mails are triggered for the selected jobs.
- Step 7** Click **Save**. A job notification mail is sent after scheduling the job and another mail is sent after the job completion. The job notification mail is triggered only for the job status that you select. You will not receive a job notification mail if the file size exceeds the size specified in the configured mail server.

Configure Global Password Policies for Local Authentication

If you are using local authentication (s authentication mechanism), you control the global password policies from the web GUI. If you are authenticating users using external authentication, the policies are controlled by an external application (see).

By default, users are not forced to change passwords after any period of time. To enforce password changes and configure other password rules, choose **Administration > Users > Users, Roles & AAA**, then choose **Local Password Policy**.

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 192](#)


-
- 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.
-

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 [Configure the Global Timeout for Idle Users, on page 191](#).

-
- 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.
-

Set Up the Maximum Sessions per User

Use this procedure to configure the maximum sessions per user using the web GUI.

-
- Step 1** Choose **Administration > Settings > System Settings > General > Server**.
 - Step 2** To set the maximum sessions per user, enter the value in the **Max Sessions** text box. You can enter any value from 1 to 50 and the default value is 5.
 - Step 3** When you are finished, click **Save**.

Step 4 Restart the server to apply the changes.



Note The session limit is applicable only for Local, RADIUS, and TACACS+ servers. The session limit is not applicable for HA and SSO modes.

Create Virtual Domains to Control User Access to Devices

- [What Are Virtual Domains?](#), on page 193
- [How Virtual Domains Affect Features](#), on page 194
- [Create New Virtual Domains](#), on page 195
- [Import a List of Virtual Domains](#), on page 197
- [Add Network Devices to Virtual Domains](#), on page 197
- [Assign Virtual Domains to Users](#), on page 198
- [Export the Virtual Domain Attributes for RADIUS and TACACS+](#), on page 200
- [Edit a Virtual Domain](#), on page 199
- [Delete a Virtual Domain](#), on page 199

What Are Virtual Domains?

Virtual domains are logical groupings of devices, sites, and other NEs, and are used to control who has access to those NEs. You choose which elements are included in a virtual domain and which users have access to that virtual domain. Virtual domains can be based on physical sites, device types, user communities, or any other designation you choose. All devices belong to ROOT-DOMAIN, which is the parent domain for all new virtual domains.

Virtual domains work in conjunction with user groups. Virtual domains control the devices a user can access, while user groups determine the actions a user can perform on those devices. Users with access to a virtual domain (depending on their privileges) can configure devices, view alarms, and generate reports for the NEs in their virtual domain.

You can create virtual domains after you have added devices to . Each virtual domain must have a name and can have an optional description, email address, and time zone. uses the email address and time zone that you specify to schedule and email domain-specific reports.

Users work in one virtual domain at a time. Users can change the current virtual domain by choosing a different one from the Virtual Domain drop-down list .

Before you set up virtual domains, determine which users are responsible for managing particular areas of the network. Then organize your virtual domains according to those needs—for example, by geography, by device type, or by the user community served by the network.

How Virtual Domains Affect Features

Virtual domains are organized hierarchically. The ROOT-DOMAIN domain includes all virtual domains.

Because network elements are managed hierarchically, user views of devices—as well as some associated features and components—are affected by the user's virtual domain. The following topics describe the effects of virtual domains on these features.

- [Reports and Virtual Domains, on page 194](#)
- [Search and Virtual Domains, on page 194](#)
- [Alarms and Virtual Domains, on page 194](#)
- [Maps and Virtual Domains, on page 194](#)
- [Configuration Templates and Virtual Domains, on page 195](#)
- [Config Groups and Virtual Domains, on page 195](#)
- [Email Notifications and Virtual Domains, on page 195](#)

Reports and Virtual Domains

Reports only include components that belong to the active virtual domain. A parent virtual domain cannot view reports from its child domains. New components are only reflected in reports that are generated after the components were added.

Search and Virtual Domains

Search results only include components that belong to the active domain. You can only view saved search results if you are in the same domain from which the search was performed and saved. When working in a parent domain, you cannot view the results of searches performed in child domains.

Alarms and Virtual Domains

When a component is added to a virtual domain, no previous alarms for that component are visible to that virtual domain. Only new alarms are visible. For example, if a network element is added to , and that network element generated alarms before and after it was added, its alarm history would only include alarms generated after it was added.

**Note**

For alarm email notifications, only the ROOT-DOMAIN virtual domain can enable Location Notifications, Location Servers, and email notifications.

Maps and Virtual Domains

Maps only display network elements that are members of the active virtual domain.

Configuration Templates and Virtual Domains

When you create or discover a configuration template in a virtual domain, it can only be applied to network elements in that virtual domain. If you apply a template to a device and then add that device to a child domain, the template is also available to the same device in the child domain.



Note If you create a child domain and then apply a configuration template to both network elements in the virtual domain, might incorrectly reflect the number of partitions to which the template was applied.

Config Groups and Virtual Domains

A parent domain can view the network elements in a child domain's configuration groups. The parent domain can also edit the child domain's configuration groups.

Email Notifications and Virtual Domains

Email notifications can be configured per virtual domain.

For *alarm* email notifications, only the ROOT-DOMAIN can enable Location Notifications, Location Servers, and email notifications.

Create New Virtual Domains

To create a new virtual domain, use one of the following procedures depending on the desired hierarchy of the virtual domain.

To create a new virtual domain (<i>new-domain</i>) here:	See this procedure:
ROOT-DOMAIN > <i>new-domain</i>	Create Virtual Domains Directly Under ROOT-DOMAIN, on page 195
ROOT-DOMAIN > <i>existing-domain</i> > <i>new-domain</i>	Create Child Virtual Domains (Subdomains), on page 196
ROOT-DOMAIN > <i>existing-domain</i> > <i>existing-domain</i> > <i>new-domain</i>	
(etc.)	

Create Virtual Domains Directly Under ROOT-DOMAIN

The following procedure creates an empty virtual domain under ROOT-DOMAIN. You can also create multiple virtual domains at one time by using the procedure in [Import a List of Virtual Domains, on page 197](#).

If a virtual domain already exists under ROOT-DOMAIN, and you want to create a new domain under it (a child domain), see [Create Child Virtual Domains \(Subdomains\), on page 196](#).

-
- Step 1** Choose **Administration > Users > Virtual Domains**.
- Step 2** In the Virtual Domains sidebar menu, click the + icon (Add New Domain).
- Step 3** Enter a name in the Name text box. This is required.

Step 4 (Optional) Enter the new domain's time zone, email address and description.

Step 5 Click **Submit** to view a summary of the newly-created virtual domain.

What to do next

Add devices to the virtual domain as described in [Add Network Devices to Virtual Domains, on page 197](#).

Create Child Virtual Domains (Subdomains)

The following procedure creates a child virtual domain (also called a subdomain). A child virtual domain is a domain that is *not* directly under ROOT-DOMAIN; it is under a domain that is under ROOT-DOMAIN.

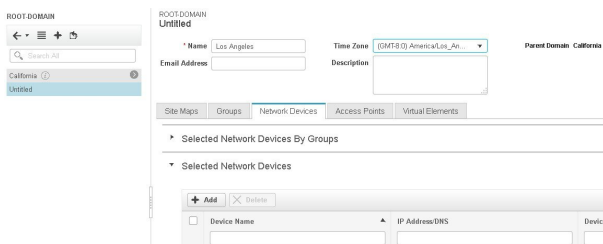
Do not use this procedure if you want the new virtual domain to appear directly under ROOT-DOMAIN. In that case, see [Create Virtual Domains Directly Under ROOT-DOMAIN, on page 195](#).

Step 1 Choose **Administration > Users > Virtual Domains**.

Step 2 In the Virtual Domains sidebar menu:

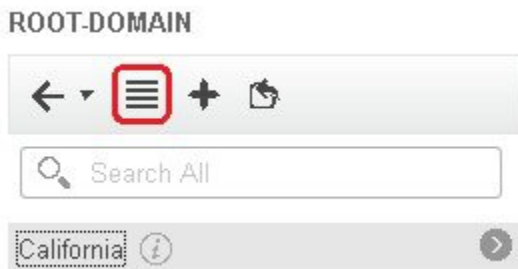
- Locate the domain under which you want to create a new child domain. (This is called the parent domain.) In this example, the parent domain is **California**.
- Click the information (**i**) icon next to the domain name. This opens a data popup window.
- In the popup window, click **Create Sub Domain**. The navigation pane switches to the list view, with the parent domain **California** displayed above **Untitled**.

Step 3 Enter a name in the Name text box. This is required. In this example, the new child domain is named **Los Angeles**. (The name in the navigation pane will not change from **Untitled** to **Los Angeles** until you save the new child domain.)

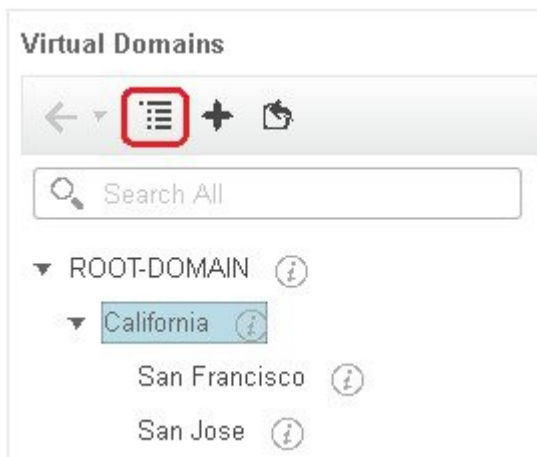


Step 4 (Optional) Enter the new domain's time zone, email address and description.

Step 5 Click **Submit** and confirm the creation of the new child domain. To revert back to the hierarchical view, click the view toggle button at the top of the navigation pane.



The view reverts to the hierarchical view.



What to do next

Add devices to the virtual domain as described in [Add Network Devices to Virtual Domains, on page 197](#).

Import a List of Virtual Domains

If you plan to create many virtual domains, or give them a complex hierarchy, you will find it easier to specify them in a properly formatted CSV file, and then import it. The CSV format allows you to specify a name, description, time zone, and email address for each virtual domain you create, as well as each domain's parent domain. Adding network elements to the virtual domains must be performed separately.

- Step 1** Choose **Administration > Users > Virtual Domains**.
- Step 2** Click the **Import Domain(s)** icon, download a sample CSV file from the link provided in the popup, and prepare the CSV file.
- Step 3** Click **Choose File** and navigate to your CSV file.
- Step 4** Click **Import** to import the CSV and create the virtual domains you specified.

What to do next

Add devices to the virtual domains as explained in [Add Network Devices to Virtual Domains, on page 197](#).

Add Network Devices to Virtual Domains

Use this procedure to add network devices to a virtual domain. When you add a new network device to an existing virtual domain, the device becomes immediately accessible to users with access to that domain (users do not have to restart the web GUI).

- Step 1** Choose **Administration > Users > Virtual Domains**.

- Step 2** From the Virtual Domains sidebar menu, click the virtual domain to which you want to add network devices.
- Step 3** Click **Submit** to view the summary of the virtual domain contents.
- Step 4** Click **Save** to confirm your changes.

What to do next

Give users access to the virtual domain as described in [Assign Virtual Domains to Users, on page 198](#).

Add Groups to Virtual Domains

Use this procedure to add device groups to a virtual domain.

-
- Step 1** Log in to Prime Infrastructure as an administrator.
- Step 2** Choose **Administration > Users > Virtual Domains**.
- Step 3** From the Virtual Domains sidebar menu, click a virtual domain to which you want to add a location group.
- Step 4** On the **Groups** tab, click **Add** to view the list of available location and user-defined groups.
The **Add Group** window appears.
- Step 5** The **Add Group** window lists only those groups that are applicable to you, which can be added to the virtual domains. Select the required group check box under All Locations, and click **Select** to add the devices to the Selected Groups table.
- Note** If the selected group is a parent group, all of its child groups gets automatically added to the virtual domain.
- Step 6** Click **Submit** to view the summary of the virtual domain.
- Step 7** Click **Save** to confirm the changes.
These groups added from the **Groups** tab will have create, read, update and delete privileges.
- Step 8** Proceed to create Users accounts.

Assign Virtual Domains to Users

Once a virtual domain is assigned to a user account, the user is restricted to viewing and performing operations on the devices in their assigned domain(s).



-
- Note** When using external AAA, be sure to add the custom attributes for virtual domains to the appropriate user or group configuration on the external AAA server. See [Use Virtual Domains with RADIUS and TACACS+, on page 200](#).
-

-
- Step 1** Choose **Administration > Users > Users, Roles & AAA > Users**.
- Step 2** Select the user to whom you want to grant device access.
- Step 3** Click the **Virtual Domains** tab.

Step 4 Use the **Add** and **Remove** buttons to make your assignment changes, then click **Save**.

Edit a Virtual Domain

To adjust a virtual domain, choose it from the Virtual Domain Hierarchy on the left sidebar menu to view or edit its assigned network devices. You cannot edit any of the settings for ROOT-DOMAIN.

Step 1 Choose **Administration > Users > Virtual Domains**.

Step 2 Click the virtual domain you want to edit in the Virtual Domains sidebar menu.

Step 3 To adjust the name, email address, time zone, or description, enter your changes in the text boxes.

Step 4 To adjust device members:

- To add devices, click **Add** and follow the instructions in [Add Network Devices to Virtual Domains, on page 197](#).
- To delete devices, select the devices using their check boxes, then click **Delete**.

Step 5 Click **Submit**, then check the summary of your changes.

Step 6 Click **Save** to apply and save your edits.

Delete a Virtual Domain

Use this procedure to delete a virtual domain from . This procedure only deletes the virtual domain; it does not delete the network elements from (the network elements will continue to be managed by).

Before you begin

You can only delete a virtual domain if:

- The virtual domain does not contain any network elements and does not have any child domains.
 - It is not the only domain a user can access. In other words, if a user has access to *only* that domain, you cannot delete it.
 - No users are logged into the domain.
-

Step 1 Choose **Administration > Users > Virtual Domains**.

Step 2 In the Virtual Domains sidebar menu, click the information (i) icon next to the virtual domain name. This opens a data popup window.

Step 3 In the popup window, click **Delete**.

Step 4 Click **OK** to confirm deleting the virtual domain.

Use Virtual Domains with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the virtual domains that exist in . You can do this using the procedure in [Export the Virtual Domain Attributes for RADIUS and TACACS+, on page 200](#).

If your RADIUS or TACACS+ server does not have any virtual domain information for a user, the following occurs, depending on the number of virtual domains that are configured in :

- If has only one virtual domain (ROOT-DOMAIN), the user is assigned the ROOT-DOMAIN by default.
- If has multiple virtual domains, the user is prevented from logging in.

Export the Virtual Domain Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all virtual domain information into your Cisco ACS or Cisco ISE server. You can do this using the Virtual Domains Custom Attributes dialog box provided in the web GUI. If you do not export the data into your Cisco ACS or Cisco ISE server, will not allow users to log in.

The following information must be exported, depending on the protocol you are using:

- TACACS+—Requires virtual domain, role, and task information.
- RADIUS—Requires virtual domain and role information (tasks are automatically added).

When you create a child domain for an existing virtual domain, the sequence numbers for the RADIUS/TACACS+ custom attributes are also updated in the parent virtual domain. These sequence numbers are for representation only and do not impact AAA integration.

Information in the Virtual Domains Custom Attributes dialog is preformatted for use with Cisco ACS server.



Note When you add tasks to the external server, be sure to add the **Home Menu Access** task. It is mandatory for all users.

Before you begin

Make sure you have added the AAA server and configured the AAA mode as explained in [Configure External Authentication, on page 201](#).

Step 1

In :

- Choose **Administration > Users > Virtual Domains**.
- Click **Export Custom Attributes** at the top right of the window. This opens the Virtual Domain Custom Attributes dialog.
- Copy the attributes list.
 - If you are using RADIUS, right-click *all of the text* in the RADIUS Custom Attributes field and choose **Copy**.
 - If you are using TACACS+, right-click *all of text* in the TACACS+ Custom Attributes field and choose **Copy**.

Step 2

Paste the information into your Cisco ACS or Cisco ISE server. If you have not yet added this information to Cisco ACS or Cisco ISE, see:

- [Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 208](#)
- [Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 203](#)

Configure Local Authentication

uses local authentication by default, which means that user passwords are stored and verified from the database. To check the authentication mode that is being used, choose **Administration > Users > Users, Roles & AAA**, then choose **AAA Mode Settings**. The selection is displayed on the AAA Mode Settings page. If you are using local authentication, be sure to configure strong password policies. See [Configure Global Password Policies for Local Authentication, on page 191](#).

If you want to use SSO with local authentication, see [Use SSO With Local Authentication, on page 201](#).

For information on external authentication, see [Configure External Authentication, on page 201](#).

Use SSO With Local Authentication

To use SSO with local authentication, you must add the SSO server and then configure to use SSO in local mode.

does not support localization on the SSO sign-in page.

The following topics describe how to configure SSO for external authentication, but you can use the same procedures to configure SSO for local authentication. The only difference is that when you configure the SSO mode on the server, choose **Local** mode (not RADIUS or TACACS+).

- [Add the SSO Server, on page 214](#)

Configure External Authentication

Users with web GUI root user or SuperUser privileges can configure to communicate with external RADIUS, TACACS+, and SSO servers for external authentication, authorization, and accounting (AAA). If you choose to configure external authentication, the user groups, users, authorization profiles, authentication policies, and policy rules must be created in the external server through which all access requests to will be routed.

You can use a maximum of three AAA servers. Users are authenticated on the second server only if the first server is not reachable or has network problems.

If you want to configure external authentication from the CLI, see .

See the following topics for more information.

- [Use RADIUS or TACACS+ for External Authentication, on page 202](#)
- [Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 203](#)
- [Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 208](#)
- [Use SSO with External Authentication, on page 214](#)

Integrate with an LDAP Server

supports external authentication using an LDAP server. If you are interested in this configuration, contact your Cisco representative.

Use RADIUS or TACACS+ for External Authentication

These topics explain how to configure to use RADIUS or TACACS+ servers.

- [Add a RADIUS or TACACS+ Server to , on page 202](#)
- [Configure RADIUS or TACACS+ Mode on the Server, on page 202](#)

Add a RADIUS or TACACS+ Server to

To add a RADIUS or TACACS+ server to :

-
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **RADIUS Servers**.
- Step 2** Select the type of server you want to add.
- For RADIUS, choose **RADIUS Servers**. From the **Select a command** drop-down list, choose **Add RADIUS Server**, then click **Go**.
 - For TACACS+, choose **TACACS+ Servers**. From the **Select a command** drop-down list, choose **Add TACACS+ Server**, then click **Go**.
- Note** You can use Move Up and Move Down arrow to reorder the available IP address.
- Step 3** Enter the required information—IP address, DNS Name, and so forth. For to communicate with the external authentication server, the shared secret you enter on this page must match the shared secret configured on the RADIUS or TACACS+ server. You can use alphabets, numbers, and special characters except ‘ (single quote) and “ (double quote) while entering the shared secret key for a third-party TACACS+ or RADIUS server.
- Step 4** Select the authentication type.
- PAP—Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication.
 - CHAP—Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).
- Step 5** If you have enabled the High Availability feature and configured a virtual IP address for the **Local Interface IP**, choose either the virtual IP address or the physical IP address of the primary server. .
- Note** The IP address configured in the external authentication server must match the **Local Interface IP**.
- Step 6** Click **Save**.
-

Configure RADIUS or TACACS+ Mode on the Server

-
- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **AAA Mode**.

- Step 2** Select **TACACS+** or **RADIUS**.
- Step 3** Check the Enable Fallback to Local check box to enable the use of the local database when the external AAA server is down.
- Step 4** If you want to revert to local authentication if the external RADIUS or TACACS+ server goes down, perform the following steps:
- a) Select **Enable Fallback to Local**. I
- Step 5** Click **Save**.

Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes

If you change the IP address of the Prime Infrastructure server after you add a TACACS+ or RADIUS server, you must manually configure the TACACS+ or RADIUS server with the new IP address of the Prime Infrastructure server. Prime Infrastructure stores in cache the local interface on which the RADIUS or TACACS+ requests are sent, and you need to manually edit the RADIUS or TACACS+ server configurations to make sure the Prime Infrastructure IP address is updated.

Related Topics

[Add a RADIUS or TACACS+ Server to](#) , on page 202

[Renew AAA Settings After Installing a New Prime Infrastructure Version](#), on page 203

Renew AAA Settings After Installing a New Prime Infrastructure Version

If you were using external RADIUS or TACACS+ user authentication before migrating your existing data to a new version of Prime Infrastructure, you must transfer the expanded Prime Infrastructure user task list to your AAA server. After you upgrade Prime Infrastructure, you must re-add any permissions on the TACACS+ or RADIUS server and update the roles in your TACACS server with the tasks from the Prime Infrastructure server.

Related Topics

[Add a RADIUS or TACACS+ Server to](#) , on page 202

[Required TACACS+/RADIUS Configurations After Prime Infrastructure IP Address Changes](#), on page 203

Use Cisco ISE With RADIUS or TACACS+ for External Authentication

Cisco Identity Services Engine (ISE) uses the RADIUS or TACACS+ protocols for authentication, authorization, and accounting (AAA). You can integrate with Cisco ISE to authenticate the users using the RADIUS or TACACS+ protocols. When you use external authentication, the details such as users, user groups, passwords, authorization profiles, authorization policies, and policy rules that are required for AAA must be stored and verified from the Cisco ISE database.

Complete the following tasks to use Cisco ISE with the RADIUS or TACACS+ protocol for external authentication:

Tasks to be completed to use Cisco ISE for external authentication	For information, see:
Make sure you are using a supported version of Cisco ISE	Supported Versions of Cisco ISE in , on page 204

Add as an AAA client in Cisco ISE	Add as a Client in Cisco ISE, on page 204
Create a user group in Cisco ISE	Create a User Group in Cisco ISE, on page 205
Create a user in Cisco ISE and add the user to the user group that is created in Cisco ISE	Create a User and Add the User to a User Group in Cisco ISE, on page 205
(If using RADIUS) Create an authorization profile for network access in Cisco ISE, and add the RADIUS custom attributes with user roles and virtual domains created in Note For RADIUS, you do not need to add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for RADIUS in Cisco ISE, on page 205
(If using TACACS+) Create an authorization profile for network access in Cisco ISE, and add the TACACS+ custom attributes with user roles and virtual domains created in Note For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.	
Create an authorization policy in Cisco ISE and associate the policy with the user groups and authorization profile created in Cisco ISE	Configure an Authorization Policy in Cisco ISE, on page 207
Create an authentication policy to define the protocols that Cisco ISE must use to communicate with , and the identity sources that it uses for authenticating users to	Create an Authentication Policy in Cisco ISE, on page 208
Add Cisco ISE as a RADIUS or TACACS+ server in	Add a RADIUS or TACACS+ Server to , on page 202
Configure the RADIUS or TACACS+ mode on the server	Configure RADIUS or TACACS+ Mode on the Server, on page 202

Supported Versions of Cisco ISE in

Add as a Client in Cisco ISE

-
- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Administration > Network Resources > Network Devices**.
- Step 3** In the **Network Devices** page, click **Add**.
- Step 4** Enter the device name and IP address of the server.
- Step 5** Check the **Authentication Settings** check box, and then enter the shared secret.

Note Ensure that this shared secret matches the shared secret you enter when adding the Cisco ISE server as the RADIUS server in .

Step 6 Click **Submit**.

Create a User Group in Cisco ISE

- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Administration > Identity Management > Groups**.
- Step 3** In the **User Identity Groups** page, click **Add**.
- Step 4** In the **Identity Group** page, enter the name and description of the user group.
- Step 5** Click **Submit**.
-

Create a User and Add the User to a User Group in Cisco ISE

- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Administration > Identity Management > Identities**.
- Step 3** In the **Network Access Users** page, click **Add**.
- Step 4** From the **Select an item** drop-down list, choose a user group to assign the user to.
- Step 5** Click **Submit**.
-

Create an Authorization Profile for RADIUS in Cisco ISE

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the RADIUS custom attributes that are associated with user roles, tasks, and virtual domains created in .



Note For RADIUS, you can add the user role attributes without adding the task attributes. The tasks are automatically added with the user roles.

For more information about Cisco ISE authorization profiles, see the information on managing authorization policies and profiles in the [Cisco Identity Services Engine Administrator Guide](#).

To create an authorization profile for RADIUS in Cisco ISE:

Before you begin

Make sure you have the complete list of the following custom attributes for RADIUS. You will need to add this information to Cisco ISE in this procedure.

- user roles and tasks—see [Export the User Group and Role Attributes for RADIUS and TACACS+, on page 181](#)

- virtual domains—see [Export the Virtual Domain Attributes for RADIUS and TACACS+, on page 200](#)

-
- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Policy > Policy Elements > Results**.
- Step 3** From the left sidebar, choose **Authorization > Authorization Profiles**.
- Step 4** In the **Standard Authorization Profiles** page, click **Add**.
- Step 5** In the **Authorization Profile** page, enter the name and description of the authorization profile.
- Step 6** From the **Access Type** drop-down list, choose **ACCESS_ACCEPT**.
- Step 7** In the **Advanced Attributes Settings** area, paste in the complete list of RADIUS custom attributes for:
- User roles
 - Virtual domains
- Note** If you do add user tasks, be sure to add the Home Menu Access task. It is mandatory.
- Step 8** Click **Submit**.
-

Create an Authorization Profile for TACACS+ in Cisco ISE

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the TACACS+ custom attributes that are associated with user roles and virtual domains created in .



-
- Note**
- For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.
 - In Release 8.5.135.0, the creation of Authorization server is deprecated. To create an Authorization server, you must create an Authentication server and duplicate it as an Authorization server. Due to this change in functionality, an alarm is generated in Cisco Prime Infrastructure 3.2 as follows:
 - 1.Successfully created Authentication server.
 - 2.Failed to create authorization server:SNMP operation to Device failed: Set Operation not allowed for TACACS authorization server.
 - 1.Successfully created Accounting server.

The workaround on Cisco Prime Infrastructure is to uncheck the Authorization server on the template. For more information, see [CSCvm01415](#).
-

For more information about Cisco ISE authorization profiles, see the information on managing authorization policies and profiles in the [Cisco Identity Services Engine Administrator Guide](#).

To create an authorization profile for TACACS+ in Cisco ISE:

-
- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Work Centers > Device Administration > Policy Elements > Results**.
- Step 3** From the left sidebar, choose **TACACS Profiles**.
- Step 4** In the **TACACS Profiles** page, click **Add**.
- Step 5** In the **TACACS Profile** page, enter the name and description of the authorization profile.
- Step 6** In the **Raw View** area, paste in the complete list of TACACS+ custom attributes for:
- User roles, including the tasks
 - Virtual domains
- Step 7** Click **Submit**.
-

Configure an Authorization Policy in Cisco ISE

An authorization policy consists of a rule or a set of rules that are user-defined and produce a specific set of permissions, which are defined in an authorization profile. Based on the authorization profile, access requests to are processed.

There are two types of authorization policies that you can configure:

- **Standard**—Standard policies are intended to be stable and are created to remain in effect for long periods of time, to apply to a larger group of users, devices, or groups that share a common set of privileges.
- **Exception**—Exception policies are created to meet an immediate or short-term need, such as authorizing a limited number of users, devices, or groups to access network resources. An exception policy lets you create a specific set of customized values for an identity group, condition, or permission that are tailored for one user or a subset of users.

For more information about authorization policies, see the “Manage Authorization Policies and Profiles” chapter in the [Cisco Identity Services Engine Administrator Guide](#).

To create an authorization policy in Cisco ISE:

-
- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Policy > Authorization**.
- Step 3** In the **Standard** area, click the down arrow on the far right and select either **Insert New Rule Above** or **Insert New Rule Below**.
- Step 4** Enter the rule name and choose identity group, condition, attribute, and permission for the authorization policy.
- For example, you can define a user group as -SystemMonitoring-Group and choose this group from the Identity Groups drop-down list. Similarly, define an authorization profile as -SystemMonitoring-authorization profile and choose this profile from the Permissions drop-down list. Now, you have defined a rule where all users belonging to the System Monitoring identity group receive an appropriate authorization policy with system monitoring custom attributes defined.
- Step 5** Click **Done**, and then click **Save**.
-

Configure an Authorization Policy for TACACS in Cisco ISE

To create an authorization policy for TACACS in Cisco ISE:

-
- Step 1** Log in to Cisco ISE as the admin user.
- Step 2** Choose **Device Work Centers > Device Administration > Device admin Policy Sets**.
- Step 3** Choose **Default** in the left side pane.
- Step 4** In the **Authorization Policy** area, click the down arrow on the far right and select either **Insert New Rule Above** or **Insert New Rule Below**.
- Step 5** Enter the rule name and choose identity group, condition, Shell Profile for the authorization policy.
- For example, you can define a user group as -SystemMonitoring-Group and choose this group from the Identity Groups drop-down list. Similarly, define an authorization profile as -SystemMonitoring-authorization profile and choose this profile from the Permissions drop-down list. Now, you have defined a rule where all users belonging to the System Monitoring identity group receive an appropriate authorization policy with system monitoring custom attributes defined.
- Step 6** Click **Save**.
-

Create an Authentication Policy in Cisco ISE

Authentication policies define the protocols that Cisco ISE uses to communicate with , and the identity sources that it uses for authenticating users to . An identity source is an internal or external database where the user information is stored.

You can create two types of authentication policies in Cisco ISE:

- Simple authentication policy - In this policy, you can choose the allowed protocols and identity sources to authenticate users.
- Rule-based authentication policy - In this policy, you can define conditions that allow Cisco ISE to dynamically choose the allowed protocols and identity sources.

For more information about authentication policies, see the "Manage Authentication Policies" chapter in the [Cisco Identity Services Engine Administrator Guide](#).

To create an authentication policy in Cisco ISE:

-
- Step 1** Log in to Cisco ISE as the Super Admin or System Admin user.
- Step 2** Choose **Policy > Authentication**.
- Step 3** Choose the Policy Type as **Simple** or **Rule-Based** to create the required authentication policy.
- Step 4** Enter the required details based on the policy type selected.
- Step 5** Click **Save**.
-

Use Cisco ACS With RADIUS or TACACS+ for External Authentication

Cisco Secure Access Control System (ACS) uses RADIUS and TACACS+ protocol for authentication, authorization, and accounting (AAA). You can integrate with Cisco ACS to authenticate the users using the

RADIUS or TACACS+ protocol. When you use an external authentication, the details such as users, user roles, passwords, authorization profiles, authorization policies, and policy rules that are required for AAA must be stored and verified from the Cisco ACS database.

Complete the following tasks to use Cisco ACS with the RADIUS or TACACS+ protocol for external authentication:

Tasks to be completed to use Cisco ACS for external authentication	For information, see:
Make sure you are using a supported version of Cisco ACS	Supported Versions of Cisco ACS in , on page 209
Add as an AAA client in Cisco ACS	Add as a Client in Cisco ACS , on page 210
Create a user group in Cisco ACS	Create a User Group in Cisco ACS , on page 210
Create a user in Cisco ACS and add the user to the Cisco ACS user group	Create a User and Add the User to a User Group in Cisco ACS , on page 210
(If using RADIUS) Create an authorization profile for network access in Cisco ACS, and add the RADIUS custom attributes for user roles and virtual domains created in . Note For RADIUS, you do not need to add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for RADIUS in Cisco ACS , on page 210
(If using TACACS+) Create an authorization profile for device administration in Cisco ACS, and add the TACACS+ custom attributes with user roles and virtual domains created in . Note For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for TACACS+ in Cisco ACS , on page 211
Create an access service in Cisco ACS and define a policy structure for the access service.	Create an Access Service for in Cisco ACS , on page 212
Create an authorization policy rule in Cisco ACS, and map the authorization or shell profile based on the access type (network access or device administration).	Create an Authorization Policy Rule in Cisco ACS , on page 213
Configure a service selection policy in Cisco ACS and assign an access service to an incoming request.	Configure a Service Selection Policy in Cisco ACS , on page 213
Add Cisco ACS as a RADIUS or TACACS+ server in .	Add a RADIUS or TACACS+ Server to , on page 202
Configure the RADIUS or TACACS+ mode on the server.	Configure RADIUS or TACACS+ Mode on the Server , on page 202

Supported Versions of Cisco ACS in

supports Cisco ACS 5.x releases.

Add as a Client in Cisco ACS

- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Network Resources > Network Devices > Network Devices and AAA Clients**.
- Step 3** In the **Network Devices** page, click **Create**.
- Step 4** Enter the device name and IP address of the server.
- Step 5** Choose the authentication option as **RADIUS** or **TACACS+**, and enter the shared secret.
- Note** Ensure that this shared secret matches the shared secret you enter when adding the Cisco ACS server as the RADIUS or TACACS+ server in .
- Step 6** Click **Submit**.
-

Create a User Group in Cisco ACS

- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, Choose **Users and Identity Stores > Identity Groups**.
- Step 3** In the **Identity Groups** page, click **Create**.
- Step 4** Enter the name and description of the user group.
- Step 5** Select a network device group parent for the user group.
- Step 6** Click **Submit**.
-

Create a User and Add the User to a User Group in Cisco ACS

- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, Choose **Users and Identity Stores > Internal Identity Stores > Users**.
- Step 3** In the **Internal Users** page, click **Create**.
- Step 4** Enter the required details.
- Step 5** In the **Identity Group** field, click **Select** to choose a user group to assign the user to.
- Step 6** Click **Submit**.
-

Create an Authorization Profile for RADIUS in Cisco ACS

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the RADIUS custom attributes that are associated with user roles, tasks, and virtual domains created in .



Note For RADIUS, you can add the user role attributes without adding the task attributes. The tasks are automatically added with the user roles.

For more information about Cisco ACS authorization profiles and policies, see chapters on managing policy elements and access policies in the [User Guide for Cisco Secure Access Control System](#).

To create an authorization profile for RADIUS in Cisco ACS:

Before you begin

Make sure you have the complete list of the following custom attributes for RADIUS. You will need to add this information to Cisco ACS in this procedure.

- user roles and tasks—see [Export the User Group and Role Attributes for RADIUS and TACACS+, on page 181](#)
- virtual domains—see [Export the Virtual Domain Attributes for RADIUS and TACACS+, on page 200](#)

-
- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Policy Elements > Authorizations and Permissions > Network Access > Authorization Profiles**.
- Step 3** Click **Create**.
- Step 4** On the **General** tab, enter the name and description of the authorization profile.
- Step 5** Click the **RADIUS Attributes** tab, and paste in the complete list of RADIUS custom attributes for:
- User roles
 - Virtual domains
- Note** If you do add user tasks, be sure to add the Home Menu Access task. It is mandatory.
- Step 6** Click **Submit**.
-

Create an Authorization Profile for TACACS+ in Cisco ACS

When you create an authorization profile for device administration, you must add the TACACS+ custom attributes that are associated with user roles and virtual domains created in .



Note For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.

For more information about Cisco ACS authorization profiles and policies, see chapters on managing policy elements and access policies in the [User Guide for Cisco Secure Access Control System](#).

To create an authorization profile for TACACS+ in Cisco ACS:

Before you begin

Make sure you have the complete list of the following custom attributes. You will need to add this information to Cisco ACS in this procedure.

- user roles and tasks—see [Export the User Group and Role Attributes for RADIUS and TACACS+, on page 181](#)
- virtual domains—see [Export the Virtual Domain Attributes for RADIUS and TACACS+, on page 200](#).

-
- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Policy Elements > Authorizations and Permissions > Device Administration > Shell Profiles**.
- Step 3** Click **Create**.
- Step 4** On the **General** tab, enter the name and description of the authorization profile.
- Step 5** Click the **Custom Attributes** tab, and paste in the complete list of TACACS+ custom attributes for:
- User roles, including the tasks
 - Virtual domains
- Step 6** Click **Submit**.
-

Create an Access Service for in Cisco ACS

Access services contain the authentication and authorization policies for access requests. You can create separate access services for different use cases; for example, device administration (TACACS+), network access (RADIUS), and so on.

When you create an access service in Cisco ACS, you define the type of policies and policy structures that it contains; for example, policies for device administration, network access, and so on.



Note You must create access services before you define service selection rules, although you do not need to define the policies in the services.

To create an access service for requests:

- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Access Policies > Access Services**.
- Step 3** Click **Create**.
- Step 4** Enter the name and description of the access service.
- Step 5** Choose one of the following options to define a policy structure for the access service:
- **Based on service template**—Creates an access service containing policies based on a predefined template.
 - **Based on existing service**—Creates an access service containing policies based on an existing access service. However, the new access service does not include the existing service's policy rules.

- **User selected service type**—Provides you the option to select the access service type. The available options are Network Access (RADIUS), Device Administration (TACACS+), and External Proxy (External RADIUS or TACACS+ servers).

- Step 6** Click **Next**.
- Step 7** Choose the authentication protocols that are allowed for the access service.
- Step 8** Click **Finish**.
-

Create an Authorization Policy Rule in Cisco ACS

- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Access Policies > Access Services > service > Authorization**.
- Step 3** Click **Create**.
- Step 4** Enter the name of the rule and then choose the rule status.
- Step 5** Configure the required conditions for the rule.
- For example, you can create a rule based on the location, device type, or user group that you have created.
- Step 6** If you are creating an authorization policy rule for network access (RADIUS), choose the required authorization profile(s) to map to the authorization policy rule.
- Alternatively, if you are creating an authorization policy rule for device administration (TACACS+), choose the required shell profile(s) to map to the authorization policy rule.
- Note** If you are using multiple authorization profiles or shell profiles, make sure you order them in priority.
- Step 7** Click **OK**.
-

Configure a Service Selection Policy in Cisco ACS

A service selection policy determines which access service applies to an incoming request. For example, you can configure a service selection policy to apply the device administration access service to any access request that uses the TACACS+ protocol.

You can configure two types of service selection policy:

- Simple service selection policy—Applies the same access service to all requests.
- Rule-based service selection policy—Contains one or more conditions and a result, which is the access service that will be applied to an incoming request.

To configure a service selection policy:

- Step 1** Log in to Cisco ACS as the admin user.
- Step 2** From the left sidebar, choose **Access Policies > Access Services > Service Selection Rules**.
- Step 3** If you want to configure a simple service selection policy, click the **Single result selection** radio button, and then choose an access service to apply to all requests.

Alternatively, if you want to configure a rule-based service selection policy, click the **Rule based result selection** radio button, and then click **Create**.

- Step 4** Enter the name of the rule and then choose the rule status.
- Step 5** Choose either **RADIUS** or **TACACS+** as the protocol for the service selection policy.
- Step 6** Configure the required compound condition, and then choose an access service to apply to an incoming request.
- Step 7** Click **OK**, and then click **Save Changes**.

Use SSO with External Authentication

To set up and use SSO (with or without a RADIUS or TACACS+ server), see these topics:

- [Add the SSO Server, on page 214](#)

does not support localization on the SSO sign-in page.

Add the SSO Server

can be configured with a maximum of three AAA servers.

- Step 1** Choose **Administration > Users > Users, Roles & AAA**, then choose **SSO Servers**.
- Step 2** From the **Select a command** drop-down list, choose **Add SSO Servers**, then click **Go**.
- Step 3** Enter the SSO information. The maximum number of server retries for an SSO server authentication request is 3.
- Step 4** Click **Save**.

Configure SSO Mode on the Prime Infrastructure Server

Single Sign-On Authentication (SSO) is used to authenticate and manage users in multi-user, multi-repository environments. SSO servers store and retrieve the credentials that are used for logging in to disparate systems. You can set up as the SSO server for other instances of .



Note If you are using this procedure to configure SSO but are using local authentication, choose **Local** in Step 2.

- Step 1** Choose **Administration > Users > Users, Roles & AAA > SSO Server Settings**.
- Step 2** Select the SSO Server AAA Mode you want to use. The options are: **Local**, **RADIUS**, or **TACACS+**.
- Step 3** Click **Save**.



CHAPTER 8

Fault Management Administration Tasks

This section contains the following topics:

- [Event Receiving, Forwarding, and Notifications, on page 215](#)
- [Specify Alarm Clean Up, Display and Email Options, on page 222](#)
- [Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms, on page 224](#)
- [Change Severity Levels, on page 224](#)
- [Customize the Troubleshooting Text for an Alarm, on page 225](#)
- [Change Alarm Auto-Clear Intervals, on page 225](#)
- [Change the Information Displayed in the Failure Source for Alarms, on page 226](#)
- [Change the Behavior of Expedited Events, on page 226](#)
- [Customize Generic Events That Are Displayed in the Web GUI, on page 226](#)
- [Troubleshoot Fault Processing Errors, on page 228](#)
- [Get Help from the Cisco Support Community and Technical Assistance Center \(TAC\), on page 229](#)

Event Receiving, Forwarding, and Notifications

processes syslogs and SNMPv1, v2, and v3 traps that it receives from devices. The server automatically listens for these events on UDP port 162. You do not have to perform any event listening configuration on the server, but you do have to configure devices to forward traps and syslogs to on the appropriate port.

Notifications are forwarded in SNMPv2 or SNMPv3 format. They are also forwarded to email recipients when you setup corresponding Notification Policies. If you are adding a notification with the notification type UDP, the you add should be listening to UDP on the same port on which it is configured. Only INFO level events are processed for the selected category and alarms are processed with critical, major, minor and warning levels.

can forward alarms and events that are generated by the processing of received syslogs, traps, and TL/1 alarms to northbound notification .

You can also use the SNMP trap notification mechanism to forward SNMP traps that indicate server problems. Alerts and events are sent as SNMPv2.

User Roles and Access Permissions for Configuring Alarm Notification Settings

This table describes the user roles and access permissions for configuring notification destination and creating customized notification policies.



Note Ensure that you enable the following Task Permissions for any user roles to view, create, and edit notification destination and notification policy:

- Notification Policies Read-Write Access under Alerts and Events
- Virtual Domains List (under Reports)

For more information, see [View and Change the Tasks a User Can Perform, on page 159](#).

User Role	Access Permission
Root user with root domain	View, create, delete and edit notification destination and notification policy.
Root user with non-root domain	View notification destination and notification policy.
Admin user with root domain	View, create, delete and edit notification destination and notification policy.
Super user with root domain	View, create, delete and edit notification destination and alarm notification policy.
System monitoring user with root domain	View notification destination and notification policy.
Config manager with root domain	View notification destination and notification policy.
Admin user with non-root domain	View notification destination and notification policy created under their respective virtual domain.
Super user with non-root domain	View notification destination and notification policy created under their respective virtual domain.
System monitoring user with non-root domain	View notification destination and notification policy created under their respective virtual domain.
Config manager with non-root domain	View notification destination and notification policy created under their respective virtual domain.

Points to Remember While Adding a New Notification Policy

The following table explains you some points you must remember while adding a new notification policy.

Category selected under Notification Policy Page	Points to Remember
Email	<ul style="list-style-type: none">• Each virtual domain must have a unique Contact Name and email address (email recipient).• Email recipients can be added, modified, and deleted only from the ROOT-DOMAIN.• Same email address can be associated with multiple virtual domains.• Prime Infrastructure does not use the Telephone Number, Cell Number, and Postal Address details for sending alarm notifications.
Trap Receiver	<ul style="list-style-type: none">• Contact Name is unique for each trap receiver.• Trap receivers can be added, modified, and deleted only from the ROOT-DOMAIN. Trap receivers are applicable only in ROOT-DOMAIN.• Only North Bound trap receivers can receive alarms/events forwarded from the Notification Policy engine.• Guest-Access trap receivers will receive only alarms related to guest clients.

Category selected under Notification Policy Page	Points to Remember
Notification Policy	<ul style="list-style-type: none"> • Each notification policy consists of following criteria: alarm categories, alarm severities, alarm types, device groups, notification destinations, and time range. • Each notification policy is associated with a unique virtual domain. • While selecting the required conditions, you can drill down the tree view drop-down list and select the individual categories (for example, Switches and Routers) and the severity (for example, Major). You can further select the specific Alarm types (for example, link down). • Alarms that match the criteria in a policy are forwarded to the respective notification destinations. • If an alarm is matched against multiple policies in the same virtual domains and these policies have the same destinations, only one notification is sent to each destination. • If the virtual domain associated with a notification policy is deleted, no alarm will match this policy. Though, this notification policy will be listed in the main Notification Policy page, you cannot modify or view the details of this notification policy. However, you can delete this policy. • If one or more device groups specified in a policy is deleted, no alarm will match this policy. Though, this notification policy will be listed in the main Notification Policy page, you cannot modify or view the details of this notification policy. However, you can delete this policy. • Alarms that are suppressed due to an existing alarm policy will not be forwarded to the notification destinations. • If a notification policy that includes both system and non-system category alarms in the rule criteria, you must select the device group(s) for the non-system category alarms. • The alarms generated in the specified duration alone are sent to the notification destination. For example, if you specify the duration as 8:00 to 17:00, the alarms will be notified from 8.00 a.m. to 5.00 p.m.

Configure Alarms Notification Destination

You can configure the email notification and Northbound trap receiver settings to notify the alarms generated by Prime Infrastructure.

-
- Step 1** Choose **Administration > Settings > System Settings > Mail and Notification > Notification Destination**.
- Step 2** Click the **Add** icon to create a new notification destination.
- Step 3** To configure Email Destination, do the following:
- From the **Select Contact Type** drop-down list, choose **Email**.
 - Enter the **Contact Name** in the text box.
 - Enter a valid email ID in the **Email To** text box.
The email is sent to the email ID entered in the **Email To** field.
 - Enter the **Contact Full Name**.
 - Choose the virtual domain from the **Virtual Domain** drop-down list.
 - Enter the **Telephone Number**, **Mobile Number**, and **Postal Address**.
 - Click **Save**.
- Step 4** To configure a Northbound trap receiver using IP Address, do the following:
- From the **Select Contact Type**, choose **Northbound Trap Receiver**.
 - Select the **IP Address** radio button and enter the **IP Address** and **Server Name**.
 - Choose the required **Receiver Type** and **Notification Type**.
 - Enter the **Port Number**, and choose the **SNMP Version**.
 - If you choose the **SNMP Version** as **v2c**, enter the **Community** settings as required.
 - If you choose the **SNMP Version** as **v3**, enter the **Username**, **Mode**, **Auth.Type**, **Auth.Password**, **Confirm Auth.Password**, **Privacy Type**, **Privacy Password** and **Confirm Privacy Password**.
 - Click **Save**.
- Step 5** To configure a Northbound trap receiver using DNS, do the following:
- From the **Select Contact Type**, choose **Northbound Trap Receiver**.
 - Select the **DNS** radio button and enter the **DNS Name**.
 - Choose the required **Receiver Type** and **Notification Type**.
 - Enter the **Port Number**, and choose the **SNMP Version**.
 - If you choose the **SNMP Version** as **v2c**, enter the **Community** settings as required.
 - If you choose the **SNMP Version** as **v3**, enter the **Username**, **Mode**, **Auth.Type**, **Auth.Password**, **Confirm Auth.Password**, **Privacy Type**, **Privacy Password** and **Confirm Privacy Password**.
 - Click **Save**.
-

**Note**

- If you choose the **Receiver Type** as **Guest Access**, will not forward the alarms to the Northbound trap receiver using the notification policy. The Guest Access receiver receives only guest-client related events. The notification policy uses only Northbound trap receivers. Make sure that you use the same Engine ID and same auth and priv passwords when configuring the external SNMPv3 trap receiver.
- While updating the Notification Destination Trap Receiver, the operational status shows the previous Trap Receiver status until the status is updated by the next polling.
- You can also navigate to Notification Policies page by choosing **Monitor > Monitoring Tools > Notification Policies** .
- If recipient email id is configured in multiple Notification policies, alarm will be forwarded only once to the email id, when condition matches.
- You will not be allowed to delete Notification Destinations which are associated with Notification Policies.

Customize Alarm Notification Policies

You can add a new alarm notification policy or edit an existing alarm notification policy to send notifications on specific alarms of interest that are generated on particular device groups, to specific recipients: either email recipients or northbound trap receivers or both.

Step 1

Choose **Administration > Settings > System Settings > Alarms and Events > Notification Policies** . To add a new alarm notification policy, do the following:

- Click the **Add** icon and choose the required virtual domain in the **Select a Virtual Domain** pop-up window.

Cisco Prime Infrastructure matches the alarms that are received from devices from a virtual domain against the notification policies for the same virtual domain. The system category alarms generated by Prime Infrastructure can be matched against all the alarm notification policies.

Note For a non-root domain, the alarms from a device will be forwarded only if the device or device group(s) containing the device was added or selected under **Network Devices** tab in virtual domain page.

- Click **OK**.
The **Notification Policies** wizard appears.
- Choose the severity, category, and event condition for which the notifications must be triggered. By default all the severity types, categories, and conditions are selected.
- Click **Next** and choose the device groups for which you want the alarm notifications to be triggered.

The alarm notifications are triggered only for the device groups that you select.

For instance, if you select the **User Defined** device group type, then the alarm notification is triggered for all the configured user defined device groups. Similarly, if you select both the **User Defined** and **Locations** device group types, then the alarm notifications are triggered for all the configured user defined and location device groups.

Select the desired device group type to abstain from receiving insignificant alarm notifications from other device groups.

If you choose only system category alarms in the previous step, a message "Device Groups are not applicable when only 'System' based alarms are selected" is displayed under the **Device Group** tab. However, if you choose a non-system category alarm, you must select at least one device group.

- Click **Next** and choose the required destination in the **Notification Destination** page.

If you choose root-domain in Step 1-a, all the Email and Northbound trap receiver destinations created in Prime Infrastructure will be listed in the **Notification Destination** page. If you choose, non-root domain, the Email destinations created under that particular domain will be listed in the **Notification Destination** page. See [Configure Alarms Notification Destination, on page 219](#)

- f) Alternately, choose the **Email** or **Northbound Trap Receiver** option from the Add icon drop-down list and complete the required fields.
- g) Choose the notification destination and click **Change Duration**.
- h) Choose the **From** and **To** timings in the **Set Duration** pop-up window and click **OK**.
The alarms generated in the specified duration alone are sent to the notification destination.
- i) Click **Next** and enter the **Name** and **Description** for the alarm notification policy in the **Summary** page.
- j) Click **Save**.

Note "Interface" is a reserved word and hence don't use it as the name for Alarm Notification Policy.

Step 2 To edit an alarm notification policy, do the following:

- a) Choose the policy and click the **Edit** icon.
The **Notification Policies** wizard appears.
- b) Choose the **Conditions**, **Device Groups**, and **Destination** as explained in Step 1.
- c) Click **Save**.



Note Notifications will not be sent to email recipient for North Bound trap receiver, if you change the severity of an alarm type from **Monitor > Monitoring Tools > Alarm Policies**.

Related Topics

[Configure Alarms Notification Destination, on page 219](#)

Convert Old Email and Trap Notification Data to New Alarm Notification Policy

The email and trap notification data created in previous releases is converted in to new alarm notification policies while upgrading or migrating from previous release to the latest version.

The migrated alarm notification policies can be viewed in the Alarms and Events Notification Policies pages.

The following Alarm categories are supported in Release 3.5:

- Change Audit
- Generic
- System
- Application Performance
- Compute Servers
- Nexus VPC switch
- Switches and Routers
- AP
- Adhoc Rogue
- Clients
- Context Aware Notifications

- Controller
- Coverage Hole
- Mesh Links
- Mobility Service
- Performance
- RRM
- Rogue AP
- SE Detected Interferers
- Security
- Third Party AP
- Third Party Controller

The following Alarm categories are not supported in Release 3.5:

- Autonomous AP
- Cisco UCS Series
- Routers
- Switches and Hubs
- Wireless Controller

To edit the migrated alarm notification policies, see [Customize Alarm Notification Policies](#).

Specify Alarm Clean Up, Display and Email Options

The **Administration > Settings > System Settings > Alarms and Events** page enables you to specify when and how to clean up, display and email alarms.

Step 1 Choose **Administration > Settings > System Settings > Alarms and Events > Alarms and Events**.

Step 2 Modify the **Alarm and Event Cleanup Options**:

- Delete active and cleared alarms after—Enter the number of days after which active and cleared alarms are deleted.
- Delete cleared security alarms after—Enter the number of days after which Security, Rogue AP, and Adhoc Rogue alarms are deleted.
- Delete cleared non-security alarms after—Enter the number of days after which non-security alarms are deleted. Non-security alarms include all alarms that do not fall under the Security, Rogue AP, or Adhoc Rogue categories.
- Delete all events after—Enter the number of days after which all the events are deleted.
- Max Number of Events to Keep—Enter the number of events that needs to be maintained in the database.

Cisco Prime Infrastructure deletes old alarms and events, as part of normal data cleanup tasks, and checks the storage size of the database alarm table once in every 2 hours, by default. When the alarm table exceeds the 300,000 limit, Prime Infrastructure deletes the oldest cleared alarms until the alarm table size is within the limit. If you want to keep cleared alarms for more than seven days, then you can specify a value more than seven days in the **Delete cleared non-security alarms after** text box, until the alarm table size reaches the limit.

Step 3 Modify the **Syslog Cleanup Options**:

- Delete all Syslogs after—Enter the number of days after which all aged syslogs are to be deleted.
- Max Number of Syslog to Keep—Enter the number of Syslogs that needs to be maintained in the database.

Step 4 Modify the **Alarm Display Options** as needed:

- Hide acknowledged alarms—When the check box is selected, Acknowledged alarms do not appear in the Alarm page. This option is enabled by default. Emails are not generated for acknowledged alarms, regardless of severity change.
- Hide assigned alarms—When the check box is selected, assigned alarms do not appear in the Alarm page.
- Hide cleared alarms—When the check box is selected, cleared alarms do not appear in the Alarm Summary page. This option is enabled by default.
- Add device name to alarm messages—Select the check box to add the name of the device to alarm messages.

Changes in these options affect the Alarm page only. Quick searches for alarms for any entity will display all alarms for that entity, regardless of alarm state.

Step 5 Modify the alarm Failure Source Pattern:

- Select the category you need to customize and click **Edit**.
- Select the failure source pattern from the options available and click **OK**.
- Select the category for which you want to customize the separator and click **Edit Separator**. Select one of the options available, then click **OK**.

The alarms generated for the selected category will have the customized pattern that you set. For example, if you select the Clients category, and then edit the separator to be #, when any supported client alarm is generated, when you select **Monitor > Monitoring Tools > Alarms and Events**, the Failure Source column for that alarm will be *MACaddress #Name*.

Note Failure Source is not supported for Custom traps, Syslog generated events and Custom syslog translation.

Step 6 Modify the Alarm Email Options:

- Add Prime Infrastructure address to email notifications—Select the check box to add the Prime Infrastructure address to email notifications.
- Include alarm severity in the email subject line—Select the check box to include alarm severity in the email subject line. This option is enabled by default.
- Include alarm Category in the email subject line—Select the check box to include alarm category in the email subject line. This option is enabled by default.
- Include prior alarm severity in the email subject line—Select the check box to include prior alarm severity in the email subject line.
- Include custom text in the email subject line—Select the check box to add custom text in the email subject line. You can also replace the email subject line with custom text by selecting the Replace the email subject line with custom text check box.
- Include custom text in body of email—Select the check box to add custom text in the body of email.
- Include alarm condition in body of email—Select the check box to include alarm condition in the body of email.
- Add link to Alarm detail page in body of email—Select the check box to add a link to the Alarm detail page in the body of email.
- Enable Secure Message Mode—Select the check box to enable a secure message mode. If you select the Mask IP Address and Mask Controller Name check boxes, the alarm emails are sent in secure mode where all the IP addresses and controller names are masked.
- Email Send Interval—Specify the time interval in which the email has to be sent.
- Include alarm application category data in body of email—Select the check box to include alarm category in the body of email.

Note Prime Infrastructure sends alarm notification email for the first instance of an alarm and the subsequent notification is sent only if the alarm severity is changed.

Step 7 Modify the **Alarm Other Settings**:

- Controller license count threshold—Enter the minimum number of available controller licenses you want to maintain. An alarm is triggered if the number of available controller licenses falls below this threshold.
- Enable AP count threshold alarm option will be enabled by default, to set the Controller access point count threshold.
- Controller access point count threshold—Enter the maximum number of available controller access points you want to maintain. An alarm is triggered if the number of available access points exceeds this threshold limit.

Step 8 Click **Save**.

Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms

The following table lists some display options for acknowledged, cleared, and assigned alarms. These settings *cannot* be adjusted by individual users (in their display preferences) because, for very large systems, a user could make a change that will impact system performance.

- [Alarm, Event, and Syslog Purging, on page 139](#)

Step 1 Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarms and Events**.

Step 2 Under the Alarm Display Options area, enable or disable these settings, as desired:

Alarm Display Options	Description	Does setting also affect search results?
Hide acknowledged alarms	Do not display Acknowledged alarms in the Alarms list or include them in search results	Yes
Hide assigned alarms	Do not display assigned alarms in the Alarms list or in search results	Yes
Hide cleared alarms in alarm browser	Do not display cleared alarms in the Alarms list or in search results	No
Add device name to alarm messages	Include device name in e-mail notifications	No

Step 3 To apply your changes, click **Save** at the bottom of the Alarms and Events window.

Change Severity Levels

Each alarm in has a severity. The alarm severity is determined by the most severe event associated to the alarm. You can adjust the severity for alarms by changing the severity for newly-generated events.



Note For alarms that are related to system administration, such as high availability, refer to [Customize Server Internal SNMP Traps and Forward the Traps, on page 91](#).

- Step 1** Choose **Administration > System Settings**, then choose **Alarms and Events > Alarm Severity and Auto Clear**.
- Step 2** Expand the categories available under the column, or search for the you want by entering all or part of the event text in the search field just below the column heading.
-

Customize the Troubleshooting Text for an Alarm

You can associate troubleshooting and explanatory information with an alarm so that users with access to the Alarms and Events tables will be able to see it. Use this procedure to add or change the information that is displayed in the popup window.

- Step 1** Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarm Severity and Auto Clear**.
- Step 2** Select an alarm, then click **Recommended Action**.
- Step 3** Add or change the content in the **Explanation** and **Recommended Actions** fields, then click **Save**. To revert to the default text, click **Reset** and **Save**.
-

Change Alarm Auto-Clear Intervals

You can configure an alarm to auto-clear after a specific period of time. This is helpful in cases, for example, where there is no clearing event. Auto-clearing an alarm will not change the severity of the alarm's correlated events.

- Step 1** Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarm Severity and Auto Clear**.
- Step 2** Expand the categories available under the **Event Types** column, or search for the event type you want by entering all or part of the event text in the **Event Types** search field just below the column heading.
- Step 3** To change the auto-clear duration for an event or group of events:
- For a single event, check the event's check box, click in the **Auto Clear Duration** field, enter the new duration, then click **Save**.
 - For multiple events, select the events, then click **Alarm Auto Clear**, enter the new duration in the dialog box, then click **OK**.
- Step 4** Change the Auto Clear Interval by performing one of the following tasks:
- Click on the **Auto Clear Duration** field, enter the new interval, and click **Save**.
-

- Select the check box of the event type, click **Alarm Auto Clear**, enter the new interval, and click **OK**.

Change the Information Displayed in the Failure Source for Alarms

When an alarm is generated, it includes information about the source of the failure. Information is presented using a specific format. For example, performance failures use the format *MACAddress:SlotID*. Failure sources for other alarms may include the host name, IP address, or other properties. Adjust the properties and separators (a colon, dash, or number sign) that are displayed in the alarm's failure source using the following procedure.

Step 1 Choose **Administration > Settings > System Settings**, then choose **Alarms and Events > Alarms and Events**.

Step 2 In the Failure Source Pattern area, select the alarm category you want to customize.

Step 3 Adjust the failure source format as follows:

- To customize the *properties* that are displayed, click **Edit**, select the properties, then click **OK**. If a property is greyed-out, you cannot remove it.
- To customize the *separators* that are displayed between the properties, click **Edit Separator**.

Step 4 To apply your changes, click **Save** at the bottom of the Alarms and Events settings window.

Change the Behavior of Expedited Events

By default, when receives a configuration change event from a device, it waits 10 minutes before starting inventory collection in case other related events are sent. This prevents multiple collection processes from running at the same time. This is called the *inventory collection hold off time* and is set to 10 minutes by default. This setting is controlled from the Inventory system settings page (**Administration > Settings > System Settings > Inventory**).

Expedited events are handled differently. Although they use the same hold off time mechanism, expedited events use the value set in a rules file rather than the value set in the web GUI. The rules file also instructs whether to perform an inventory collection only on specific parts of the network element, or on the whole NE.

has multiple rules file that are stored in `/opt/CSColumos/conf/fault/correlationEngine`. Expedited event settings are controlled by the files that end in the string **EventBasedInventoryRules.xml**.

Customize Generic Events That Are Displayed in the Web GUI

You can customize the description and severity for generic events generated by SNMP traps and syslogs. Your customization will be displayed in the Events tab for SNMP trap events. If a MIB module is not loaded, you can load it manually and then customize the notifications provided in that MIB.

See [Customize Generic Events Based on SNMP Traps, on page 227](#), for information on how to customize these generic events.

Disable and Enable Generic Trap and Syslog Handling

By default does not drop any received syslogs or traps. maintains an event catalog that determines whether should create a new event for incoming syslogs or traps (and if it creates a new event, whether it should also create an alarm). If does not create an event, the trap or syslog is considered a *generic event* .

By default, does the following:

- Displays the generic events in the Events list.
- Forwards generic events in e-mail or SNMP trap notifications, after normalizing them using the

All of these events are assigned the MINOR severity, regardless of the trap contents, and fall under the alarm category Generic.

Disable and Enable Generic Trap Processing

Use the genericTrap.sh command to manage generic syslogs.

To do the following:	Use this command:
Turn off generic trap processing	<code>/opt/CSCOLumos/bin/genericTrap.sh -l</code>
Turn on generic trap processing	<code>/opt/CSCOLumos/bin/genericTrap.sh -u</code>

Disable and Enable Generic Syslog Processing

Use the genericSyslog.sh command to manage generic syslogs.

To do the following:	Use this command:
Turn off generic syslog processing	<code>/opt/CSCOLumos/bin/genericSyslog.sh -l</code>
Turn on generic syslog processing	<code>/opt/CSCOLumos/bin/genericSyslog.sh -u</code>

Customize Generic Events Based on SNMP Traps

supports the customized representation of generic events in the GUI. Managed objects normally generate SNMP traps and notifications that contain an SNMP trap object identifier (SnmpTrapOID) and a variable bind object identifier (VarBindOIDs) in numerical format. translates the numeric SnmpTrapOIDs and VarBindOIDs into meaningful names using customized MIB modules, then displays the generic events in the web GUI (in the event tables, Device 360 view, and so forth).

Using the SNMP MIB files that are packaged with , you can customize the defined MIBs for your deployment's technology requirement.

The following table illustrates how ObjectIDs are decoded and displayed in the GUI.

Table 13: Example: ObjectID Representation

OIDs before Decoding	OIDs after Decoding
snmpTrapOID = 1.3.6.1.4.1.9.10.120.0.1', Values: 1.3.6.1.4.1.9.10.119.1.1.2.1.11.7.1=1	mplsL3VpnVrfDown, values: mplsL3VpnVrfOperStatus.("vrf1").(1) = 1

Follow the steps below to create customized generic events.

-
- Step 1** Select **Monitor > Monitoring Tools > Alarms and Events**.
 - Step 2** Click the **Events** tab.
 - Step 3** Click **Custom Trap Events** and then click **Upload New Mibs**.
 - Step 4** In the **Upload Mib** window, click **Upload New MIB** to upload a MIB file.
 - Step 5** If you upload a new MIB file, wait until the file upload is complete, and then click **Refresh MIBs** to have the newly added MIB included in the **MIB** drop-down list.
 - Step 6** Click **OK**.
creates a new event type and alarm condition for the specified trap.
-

Troubleshoot Fault Processing Errors

If your deployment is having fault processing problems, follow this procedure to check the fault logs.

-
- Step 1** Log in to with a user ID that has Administrator privileges.
 - Step 2** Select **Administration > Settings > Logging**, then choose **General Logging Options**.
 - Step 3** In the **Download Log File** area, click **Download**.
 - Step 4** Compare the activity recorded in these log files with the activity you are seeing in your management application:
 - console.log
 - ncs-x-x.log
 - decap.core.java.log
 - xmp_correlation.log
 - decap.processor.log
-

What to do next

You can also get help from the Cisco support community. If you do need to open a support case, attach the suspect log files with your case. See [Get Help from the Cisco Support Community and Technical Assistance Center \(TAC\)](#), on page 229.

Get Help from the Cisco Support Community and Technical Assistance Center (TAC)

- [Open a Cisco Support Case](#), on page 229
- [Join the Cisco Support Community](#), on page 230

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.



CHAPTER 9

Audits and Logs

This section contains the following topics:

- [Audit Configuration Archive and Software Management Changes \(\)](#), on page 231
- [Audit Changes Made By Users \(Change Audit\)](#), on page 231
- [Audit Actions Executed from the GUI \(System Audit\)](#), on page 233
- [System Logs](#), on page 234

Audit Configuration Archive and Software Management Changes ()

The window displays changes made to devices using the Configuration Archive and Software Management features. To view these changes, choose . lists the most recent devices changes including the type of change (Configuration Archive, Software Image Management).

You can also view the most recent changes for a device in the **Recent Changes** tab of its Device 360 view.

Audit Changes Made By Users (Change Audit)

supports managing change audit data in the following ways:

- [Generate a Change Audit Report](#), on page 231
- [Enable Change Audit Notifications and Configure Syslog Receivers](#), on page 232

Generate a Change Audit Report

The Change Audit report lists the actions that users have performed using the features. The following table provides examples of what may appear in a Change Audit report.

Feature	Examples
Device management	Device '209.165.202.159' Added
User management	User 'mmjones' added

Feature	Examples
Administration	Logout successful for user jlsmith from 209.165.202.129 Authentication Failed. Login failed for user fjclark from 209.165.202.125
Configuration changes	CLI Commands : ip access-list standard testremark test
Monitoring policies	Monitoring Template 'IF Outbound Errors (Threshold)' Created
Configuration templates	Configuration Template 'Add-Host-Name-IOS-Test' Created
Jobs	'Show-Users-On-Device-IOS_1' job of type Config Deploy - Deploy View scheduled.
Inventory	Logical File '/bootflash/tracelogs/inst_cleanup_R0-0.log.19999.20150126210302' deleted.

You can schedule a Change Audit report to run on a regular basis and, if desired, can e-mail the results to you. You can also forward this information in a Change Audit notification (see [Enable Change Audit Notifications and Configure Syslog Receivers, on page 232](#)).

-
- Step 1** Choose **Reports > Report Launch Pad**, then choose **Compliance > Change Audit**.
- Step 2** Click **New** to configure a new report.
- Step 3** In the **Settings** area, enter the report criteria (time frame, when to start the report, and so forth).
- Step 4** If you want to schedule the report to run at a later time, enter your settings in the **Schedule** area. You can also specify an e-mail address that the report should be sent to.
- Step 5** If you want to run the report immediately, click **Run** at the bottom of the window.
- The **Report Run Result** lists all users and the changes they made during the specified time period.
-

Enable Change Audit Notifications and Configure Syslog Receivers

If desired, you can configure to send a change audit notification when changes are made to the system. These changes include device inventory and configuration changes, configuration template and monitoring template operations, and user operations such as logins and logouts and user account changes.

You can configure to:

- Forward changes as change audit notifications to a Java Message Server (JMS).
- Send these messages to specific syslog receivers.

If you configure syslog receivers but do not receive syslogs, you may need to change the anti-virus or firewall settings on the destination syslog receiver to permit reception of syslog messages.

-
- Step 1** Select **Administration > Settings > System Settings**, then choose **Mail and Notification > Change Audit Notification**.
- Step 2** Select the **Enable Change Audit Notification** check box to enable notifications.

- Step 3** If you want to send the messages to specific syslog receivers:
- Click the **Add** button (+) to specify a syslog receiver.
 - In the **Syslog Receivers** area, enter the IP address, protocol, and port number of the syslog receiver.

You can repeat these steps as needed to specify additional syslog receivers.

- Step 4** Click **Save**.

Note It is recommended to restart the server for the records to be reflected in secure tls log.

View Change Audit Details

- Step 1** Log in to as an administrator

- Step 2** Choose **Monitor > Tools > Change Audit Dashboard**.

The **Change Audit Dashboard** displays the network audit logs and change audit data of device management, user management, configuration template management, device community and credential changes, and inventory changes of devices. The **Change Audit report** and **Change Audit** dashboard display the details irrespective of the virtual domain you are logged in.

Audit Actions Executed from the GUI (System Audit)



Note sends all change audit notifications in XML format to the topic **ChangeAudit.All**. You must be subscribed to **ChangeAudit.All** to receive the notifications.

The System Audit window lists all GUI pages that users have accessed. To view a System Audit, choose **Administration > Settings > System Audit**.

The following table shows some of the information you can find from the System Audit page using the quick filter. To enable the quick filter, choose **Quick Filter** from the **Show** drop-down list.

Find actions performed:	Do the following:
By a specific user	Enter the username in the Username quick filter field
By all users in a user group	Enter the group name in the User Group quick filter field
On devices in a specific virtual domain	Enter the virtual domain name in the Active Virtual Domain quick filter field
By the web GUI root user	Select Root User Logs from the Show drop-down list
On a specific device	Enter the IP address in the IP Address quick filter field

Find actions performed:	Do the following:
On a specific day	Enter the day in the Audit Time quick filter field (in the format <i>yyyy-mm-dd</i>)

System Logs

provides three classes of logs which are controlled by choosing **Administration > Settings > Logging**.

Logging Type	Description	See:
General	Captures information about actions in the system.	View and Manage General System Logs, on page 234
SNMP	Captures interactions with managed devices.	Enable SNMP Traces and Adjust SNMP Log Settings (Levels, Size), on page 241
Syslog	Forwards audit logs (as syslogs) to another recipient.	Forward System Audit Logs As Syslogs, on page 241

View and Manage General System Logs

You can view system logs after downloading them to your local server.

- [View the Logs for a Specific Job, on page 234](#)
- [Adjust General Log File Settings and Default Sizes, on page 234](#)
- [Download and E-Mail Log Files for Troubleshooting Purposes, on page 235](#)
- [Forward System Audit Logs As Syslogs, on page 241](#)

View the Logs for a Specific Job

-
- Step 1** Choose **Administration > Dashboards > Job Dashboard** .
- Step 2** Choose a job type from the Jobs pane, then select a job instance from the Jobs window.
- Step 3** At the top left of the Job instance window, locate the **Logs** field, then click **Download**.
- Step 4** Open or save the file as needed.
-

Adjust General Log File Settings and Default Sizes

By default, logs all error, informational, and trace messages generated by all managed devices. It also logs all SNMP messages and Syslogs that it receives. You can adjust these settings, changing logging levels for debugging purposes.

To do the following:	From Administration > Settings > Logging:
Change the size of logs and the number of logs saved	Adjust the Log File Settings. Note Change these settings with caution to avoid impacting the system.
Change the logging level for specific modules	In the General Log Settings, select the files and the desired level, and click Save . For example, from the Message Level drop-down list, choose one of the following as current logging level: <ul style="list-style-type: none"> • Error—Captures error logs on the system. • Information—Captures informational logs on the system. • Trace—Reproduces problems of managed devices on the system so the details can be captured in the logs. You will have to restart for the changes to take effect.
Download log files for troubleshooting purposes	In the Download Log File area, click Download .
E-mail log files (for example, to the Cisco Technical Center)	Enter a comma-separated list of e-mail IDs and click Send .

Download and E-Mail Log Files for Troubleshooting Purposes



Note This procedure sets and log message levels to Trace. Be sure to return the log message levels to their original setting so system performance is not impacted.

- Step 1** Choose **Administration > Settings > Logging**, then choose **General Logging Options**.
- Step 2** Note the setting in the **Message Level** drop-down list because you will need to reset it later.
- Step 3** In the **Enable Log Modules** area, select the desired **Log Modules**.

Log Modules	Description
AAA	This log module enables the ncs-0-0.log, nms_sys_error.log, usermgmt.log, and XmpUserMgmtRbac.log files. The logs are printed when the user logs in. The AAA mode changes like local, tacacs, radius, and sso mode changes are performed.
Apic	This log module enables the ifm_apic.log file which captures the log that occurs when a PNP profile gets synced against APIC.
APICPIIntegration	This log module enables the apic_pi_integration.log file that captures the logs when Prime Infrastructure profiles are synced in APICEM as sites.

Log Modules	Description
AppNav	This log module enables the appNav.log file to capture the logs when saving the ACL configuration in a template, deleting ACL from a template, creating and updating WAAS interface, and when creating, updating, and deleting the service node group and controller group.
Assurance AppClassifier	This log module enables the assurance_appclassifier.log file that captures information related to NBAR classification on incoming AVC/Wireless Netflow data. This is for application classification/identification for flow record, as a part of the netflow processing in Prime Infrastructure.
Assurance Netflow	This log module enables the assurance_netflow.log file that captures information pertaining to the processing of incoming Netflow data being sent from various Netflow devices to Prime Infrastructure. It logs information related to netflow processing performed on flow exports received on UDP port 9991.
Assurance PfR	This log module enables the assurance_pfr.log file that captures information related to the PfRMonitoring process.
Assurance WirelessUser	This log module enables the assurance_wirelessuser.log file that captures the information when the WirelessUser job runs to read the user data and populate it in the memory caches that are added by the WIRELESS_ASSURANCE trigger.
Assurance WSA	This log module enables the wsa_collector.log, access_log, assurance_wsa.log, and error_log files that captures information while WLC processes data from device to Prime Infrastructure. Logs are generated as a part of the Wireless Controller data collection.
AVC Utilities	This log module enables the aems_avc_utils.log file. The AVC configuration feature-specific utility flow logs are generated as a part of this component.
CIDS Device Logs	This log module captures information related to device pack operation of few devices that are not migrated to XDE.
Operations Center Logs	This log module enables the cluster.core.log file that captures information related to management Prime Infrastructure servers.
Collection	This log module captures the information of the dashlet that is launched to check the readiness of a device.
Common Helper	This log module captures the XMP common related information.

Log Modules	Description
Configuration	This log module enables the ifm_config.log file when the templates such as CLI, Composite, and MBC are deployed to the devices. The service business logic execution debug logs are captured.
Configuration Archive	This log module enables the ifm_config_archive.log and ifm_config_archive_core.log files. The logs are captured based on the selected log level in GUI and logs are logged for all the Configuration Archive module supported operations like Configuration Archive Collection, Configuration Archive Overwrite, Configuration Archive Rollback, and Configuration Archive Deploy.
Configuration Archive Core	This log module enables the ifm_config_archive_core.log file which captures the information on the interaction between service layer and device pack while performing the operations like Configuration Archive Collection, Configuration Archive Overwrite, Configuration Archive Rollback, and Configuration Archive Deploy.
Configuration Templates	This log module enables the ifm_config.log and ifm_template.log files. These files are logged when a System template, Custom CLI template, Composite Template, or Feature Template is deployed to a device and the deploy job is created. The logs are captured in based on the selected log level [INFO, DEBUG, TRACE] in GUI and are logged for all the Configuration templates that is deployed to the devices.
Container Management	This log module enables the logs for ifm_container.log file. This file is logged when the container management performs the life cycle operations (Install, Activate, Uninstall, and Deactivate) of the virtual appliances.
Credential Management	This log module enables the logs from NMS_SysOut.log file.
Credential Profile	This log module enables the ifm_credential_profile.log file that captures the profile creation, deletion, and profile update information.
DA	This log module enables the ifm_da.log and da_daemon.log files. This module captures the information such as SNMP polling, NAM polling and Packet Capture work flows.
Database	This log module enables the rman.log and db_migration.log files.
Datacenter	This log module enables the datacenterevent.log and ifm_datacenter.log files. These files contain debug information while adding, editing, and deleting devices

Log Modules	Description
	(Discovery Sources, UCS, Nexus). Inventory module logs also contain the debug information about Datacenter devices.
Device Credential Verification	This log module enables the XDE.log file.
Discovery	This log module enables the ifm_discovery.log and existenceDiscovery.log files that captures logs while creating, editing, and deleting discovery settings or discovery job, and running discovery job.
DSM	This log module captures the information related to Virtual Inventory Discovery Source Manager.
Fault Management	This log module enables the ifm_fault.log, xmp_correlation.log, and xmp_syslog.log files.
Faults	This log module enables the ifm_fault.log, xmp_correlation.log, and xmp_syslog.log files.
Firewall and AVC Configuration	This log module enables the aems_config.log file that captures the AVC, ZBFW, QoS, and NAT configuration details.
Firewall and AVC Inventory	This log module enables the aems_zbfw_ice_post_processors.log file that captures the device inventory time read on AVC, ZBFW, QoS, and NAT configuration.
Firewall and AVC REST API	This module enables the aems_config_access_layer.log file that captures the REST API call details for AVC, ZBFW, QoS, NAT, and PPM features.
Firewall and AVC Utilities	This log module enables the aems_utils.log file that captures the common utility calls in AVC/ZBFW/QoS, NAT and PPM features.
Firewall Utilities	This log module enables the aems_zbfw_utils.log file that captures the ZBFW utility calls.
Grouping	This log module enables the ifm_grouping.log, grouping-spring.log files. It captures data while adding, editing, and deleting groups, and adding and deleting members. It also captures the log while importing or exporting groups in CSV format and creating port groups, editing, and deleting port groups.
Inventory	This log module enables the inventory.log, ifm_inventory.log, existenceInventory.log, and xde.log files. It captures the data while adding, editing, and deleting devices and performing inventory collection.

Log Modules	Description
Mobility	This log module captures the information related to the mobility anchor devices that are added to the server.
Monitor	This log module captures the information related to the APIs that appears while launching the monitor dashlets such as Top N Memory and Top N CPU.
MSAP	This log module enables the ncs.log file. It captures the data related to MSE High Availability actions such as Proxy configuration and BBX configuration.
MSE	This log module enables the ncs.log file. It captures the data related to Mobility Service Engine activities such as adding, editing, and deleting MSE and Controller and SiteMap synchronization with MSE.
nbifw	This log module allows you to change the logging level of the NBI API framework. You can view the information in the xmpNbiFw.log file.
ncs_nbi	This log module allows you to change the logging level of the Statistics NBI Services. You can view the information in the ncs_nbi.log file.
Network Topology	This log module enables the nms-topology.log and xmptopology.log files. This log module captures logs related to the Maps > Network Topology page. Information such as adding and deleting links between devices are captured.
nfvos	This log module is used for tracking esa dna integration process.
Nice	This log module captures the topology related information after adding a device.
Notifications	This log module captures information from the ncs-0-0.log, ncs_nb.log and alarm_notification_policy.log files.
PA	This log module enables the ifm_sam.log and sam_daemon.log files. The information such as application and service, dashboard and dashlet service API calls, NAM configuration, NAM polling, and Packet Capture feature work flow are captured.
Ping	This log module captures information related to network device polling interval job. Once the job is completed, each device in the system receives a ping.
Plug and Play	You can enable this module to capture the information related to PNP profile creation and provisioning, bootstrap initial configuration, APIC EM sync timeframe. The logs are captured in the ifm_pnp.log and ifm_apic.log files.

Log Modules	Description
Protocol Pack Management	This module enables the aems_ppm_service.log , ifm_container.log , jobManager.log and ifm_jobscheduler.log files. This logs the information related to protocol pack import, distribution of protocol packs, and the jobs details.
Reports	You can enable this module to view the report related queries, memory consumption, and time frame of report generation.
Smart Licensing	This log module enables the ifm_smartagent.log and smart_call_home.log files. The ifm_smartagent.log file contains licensing logs related to smart licensing and smart_call_home.log contains call home logs that captures information transmitted to CSSM (Cisco Smart Software Manager). These logs are captured in Periodic events and User action based events.
SWIM	You can enable this module to log the Software Image Management module logs in the ifm_swim.log file. The logs will be captured as per the selected log level in GUI. It logs the information related to the Software Image Management operations like Software Image Recommendation, Software Image Upgrade Analysis, Software Image Import, Software Image Distribution, Software Image Activation, and Software Image Commit.
System Monitoring	This log module enables the ifm_sysmon.log file. This logs information pertaining to the rule start time and end time as well as the operations performed in between.
ThreadManager	This log module enables the xmp_threadmanager.log file that captures the hybernate related information.
Threshold	You can enable this module to view the details of the events processed by the Threshold Monitor.
TrustSec	You can enable this module to capture the TrustSec readiness devices, devices capable for enforcement, device classification, and capable devices information. The list is displayed in Service-TrustSec-Readiness. You can view the logs in the ifm_trustsec.log file.
Wlan AVC Configuration	This log module enables the aems_config_wlan.log file to view the WLAN configuration work flow related information.
XMLMED	You can enable this module to capture the SOAP requests and responses. You can also view these logs in the ncs.log files.

- Step 4** Select **Trace** from the **Message Level** drop-down list.
- Step 5** Reproduce the problem on the system so the details can be captured in the logs.
- Step 6** In the **Download Log File** area, click **Download**. The download zip file will have the name:
NCS-hostname-logs-yy-mm-dd-hh-mm-ss.

The file includes an HTML file that lists all files included in the zip file.

The information captured in the ifm_da.log and ifm_sam.log files are now split-up into the accompanying classes:

- assurance_wirelessuser.log
- assurance_pfr.log
- assurance_netflow.log
- assurance_appclassifier.log

The ifm_da.log file logs the information related to the Netflow devices and their respective pcaps, post device inclusion on . The assurance_wirelessuser.log file logs the information that is captured when the WirelessUser job runs to read the user data and populate in the memory caches that are added by WIRELESS_ASSURANCE. The assurance_pfr.log file stores the PfR monitoring related information. The assurance_netflow.log file logs the processing of incoming Netflow data being sent from various Netflow devices to . The assurance_appclassifier.log file stores the logs for NBAR classification on incoming AVC/Wireless Netflow data.

- Step 7** In the E-Mail Log File area, enter a comma-separated list of e-mail IDs.
- Step 8** Revert to the original setting in the **Message Level** drop-down list.

Forward System Audit Logs As Syslogs

Before you begin

To work with Forward System Audit Logs as Syslogs, the user must configure Enable Change Audit Notifications and Configure Syslog Receivers.

-
- Step 1** Choose **Administration > Settings > Logging**, then choose **Syslog Logging Options**.
- Step 2** Select the **Enable Syslog** check box to enable collecting and processing system logs.
- Step 3** In the **Syslog Host** field, enter the IP address of the destination server from which the message is to be transmitted.
- Step 4** From the **Syslog Facility** drop-down list, choose any of the eight local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.
- Step 5** Click **Save**.

Enable SNMP Traces and Adjust SNMP Log Settings (Levels, Size)

Enable SNMP tracing to access more detailed information about the packets sent and received through SNMP. You may want to do this when troubleshooting, such as when a trap is dropped.

To make the following changes, choose **Administration > Settings > Logging**, then choose **SNMP Logging Options**.

If you want to:	Do the following:
Enable SNMP tracing on specific devices	In the SNMP Log Settings area: <ol style="list-style-type: none">1. Select the Enable SNMP Trace check box and the Display Values check boxes.2. Enter the IP addresses of the devices you want to trace and click Save.
Change the size of logs and number of logs saved	In the SNMP Log File Settings area: Note Be careful when you change these settings so that you do not impact system performance (by saving too much data). <ol style="list-style-type: none">1. Adjust the maximum number of files and file size.2. Restart for your changes to take effect. See Stop and Restart, on page 81.



CHAPTER 10

Configure Controller and AP Settings

- [Configure Protocols for CLI Sessions](#), on page 243
- [Enable Unified AP Ping Reachability Settings on the Prime Infrastructure](#), on page 243
- [Refresh Controllers After an Upgrade](#), on page 245
- [Track Switch Ports to Rogue APs](#), on page 245
- [Configure Switch Port Tracing](#), on page 246

Configure Protocols for CLI Sessions

Many Prime Infrastructure wireless features, such as autonomous access point and controller command-line interface (CLI) templates and migration templates, require executing CLI commands on the autonomous access point or controller. These CLI commands can be entered by establishing Telnet or SSH sessions. The CLI session page allows you to select the session protocol.

In CLI templates, you are not required to answer the question responses (such as *Yes* or *No* answer to a command, *Press enter to continue* , and so on.). This is automatically performed by Prime Infrastructure.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > CLI Session**.
 - Step 2** Select the **Controller Session Protocol** (you can choose SSH or Telnet; SSH is the default).
 - Step 3** Select the **Autonomous AP Session Protocol** (you can choose SSH or Telnet; SSH is the default).
 - Step 4** The **Run Autonomous AP Migration Analysis on discovery** radio button is set to **No** by default. Choose **Yes** if you want to discover the autonomous APs as well as perform migration analysis
 - Step 5** Click **Save**.
-

Enable Unified AP Ping Reachability Settings on the Prime Infrastructure

Whenever a Unified AP is discovered in Cisco Prime Infrastructure, the Prime Infrastructure determines if the AP is ping capable or not and updates the ping capability status accordingly in the Prime Infrastructure database.

Various alarms are raised based on the following conditions:

- If the Unified AP is disassociated and is in FlexConnect mode, then the Prime Infrastructure checks if the AP is reachable or not. If the AP is ping capable and ping reachable, then it raises a low severity alarm. If the AP is not ping capable or reachable, then it raises a high severity alarm.
- If the Unified AP is disassociated and is not in FlexConnect mode, then the Prime Infrastructure raises a high severity alarm.

By default, the Unified AP ping reachability feature is enabled in Prime Infrastructure versions 3.3 onwards. However, it is disabled in versions 3.2 and earlier. To enable, follow these steps:

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Unified AP Ping Reachability**.
- Step 2** Select the **Allow Prime to learn about AP Reachability** radio button to allow Cisco Prime Infrastructure to learn if the AP is reachable or not. A background task is triggered which pings each access point and stores the result in the Prime Infrastructure database.
- Step 3** You are prompted with an alert saying that the background job is triggered to learn about ping reachability. Click **OK** to continue.
- A background job is triggered and is run against all the associated APs in the Prime Infrastructure to learn about the AP capabilities. A new job is created in the **Job Dashboard** with this information.
- Step 4** If you select **All access points are ping reachable from Prime** radio button, then the Administrator marks all the Unified APs as ping capable.
- Step 5** Choose **Administration > Dashboards > Job Dashboard > System Jobs > Status** to view job status.
- Step 6** To search job details, use **Quick** filter option and enter **Learn Unified AP Ping Capability** in the **Name** search field. The result is displayed in the **Status** table. The table contains the following information:
- **Job Type**
 - **Status**
 - **Last Run Status**
 - **Last Start Time**
 - **Duration**
 - **Next Start Time**
 - Click the **Learn AP Ping Reachability** link to view more details. The **Learn AP Ping Reachability** page displays the following information. Click **Show All** to view details about all job instances.
 - **Recurrence**
 - **Interval**
 - **Run ID**
 - **Status**
 - **Duration**
 - **Start Time**

- **Completion Time**

Refresh Controllers After an Upgrade

The Controller Upgrade page allows you to auto-refresh after a controller upgrade so that it automatically restores the configuration whenever there is a change in the controller image.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Controller Upgrade**.
- Step 2** Select the **Auto refresh After Upgrade** check box to automatically restore the configuration whenever there is a change in the controller image.
- Step 3** Select the **Sync on Save Config Trap** check box to trigger a Sync on the controller when the Prime Infrastructure receives a Save Config trap. When this check box is selected, you can choose either of the following options:
- Retain the configuration in the Prime Infrastructure database
 - Use the configuration on the controller currently
- Step 4** Click **Save**.
-

Track Switch Ports to Rogue APs

can automatically identify the network switch port to which each rogue access point is connected. Note that this feature relies on Automatic Switch Port Tracing, which requires a full Prime Infrastructure license to work.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Auto SPT**. The Auto SPT page appears.
- Step 2** Select the **Enable Auto Switch Port Tracing** check box to allow Prime Infrastructure to automatically trace the switch ports to which rogue access points are connected. Then specify the parameters for auto port tracing, including:
- How long to wait between rogue AP-to-port traces (in minutes)
 - Whether to trace Found On Wire rogue APs
 - Which severities to include (Critical, Major, or Minor)
- Step 3** Select the **Enable Auto Containment** check box to allow Prime Infrastructure to automatically contain rogue APs by severity. Then specify the parameters for auto containment, including:
- Whether to exclude Found On Wire rogue APs detected by port tracing
 - Which severities to include in the containment (Critical, Major)
 - The containment level (up to 4 APs)

Step 4 Click **OK**.

Configure Switch Port Tracing

Currently, Prime Infrastructure provides rogue access point detection by retrieving information from the controller. The rogue access point table is populated with any detected BSSID addresses from any frames that are not present in the neighbor list. At the end of a specified interval, the contents of the rogue table are sent to the controller in a CAPWAP Rogue AP Report message. With this method, Prime Infrastructure gathers the information received from the controllers. This enhancement allows you to react to found wired rogue access points and prevent future attacks. The trace information is available only in Prime Infrastructure log and only for rogue access points, not rogue clients.

A rogue client connected to the rogue access point information is used to track the switch port to which the rogue access point is connected in the network. If you try to set tracing for a friendly or deleted rogue, a warning message appears.

For Switch Port Tracing to successfully trace the switch ports using v3, all of the OIDs should be included in the SNMP v3 view and VLAN content should be created for each VLAN in the SNMP v3 group. The Switch Port Trace page allows you to run a trace on detected rogue access points on the wire.

To correctly trace and contain rogue access points, you must correctly provide the following information:

- Reporting APs — A rogue access point has to be reported by one or more managed access points.
- AP CDP Neighbor— Access point CDP neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials— All switches to be traced must have a management IP address and must have SNMP management enabled. You can add network address based entries instead of only adding individual switches. The correct “write” community string must be specified to enable/disable switch ports. For tracing, “read” community strings are sufficient. Network addresses using /32 subnet masks are not supported in global SNMP credentials configuration. For more guidance, see “Frequently Asked Questions on Rogues and Switch Port Tracing” in Related Topics.
- Switch port configuration— Trunking switch ports must be correctly configured. Switch port security must be disabled.
- Switch Port Tracing is supported only on Cisco Ethernet switches and the following Catalyst switches: 2960, 3560, 3560-E, 3750-E, 3850, 4500 series.
- Switch VLAN settings must be configured accurately. Prime Infrastructure gets switch IP addresses using Cisco Discovery Protocol neighbor information. It then uses VLAN information in the switch to read the switch CAM table entries. If the VLAN information in the switch is not configured properly, Prime Infrastructure will not be able to read the CAM table entries, which results in not being able to trace rogue APs in the switch.
- CDP protocol must be enabled on all switches.
- An Ethernet connection must exist between the rogue access point and the Cisco switch.
- There must be traffic between the rogue access point and the Ethernet switch, for reliable detection of rogue Ethernet Switch Port information, when the difference in the Ethernet mac address is more or less than two.
- The rogue access point must be connected to a switch within the max hop limit.
- If SNMPv3 is chosen, use the context option and create one for each VLAN, in addition to the one for the main group (which is required for non-VLAN-based MIBs).



Note For effective use of Vendor OUI match to eliminate false positive matches, the switch ports must have their location information configured. The switch ports that are not configured will remain for OUI match after elimination by location.

Related Topics

[Frequently Asked Questions on Rogues and Switch Port Tracing](#), on page 250

Configuring SNMP credentials

To view the switch port trace details, follow these steps:

Step 1 Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > SPT Configuration**.

Step 2 Configure the following basic settings:

- MAC address +1/-1 search—Select the check box to enable.

This search involves the MAC address +1/-1 convention where the wired-side MAC address of the rogue access point is obtained by adding or subtracting the radio MAC address by one.

- Rogue client MAC address search—Select the check box to enable.

When a rogue access point client exists, the MAC address of the client is added to the searchable MAC address list.

- Vendor (OUI) search— Select the check box to enable. OUI refers to Organizational Unique Identifier search which searches the first three bytes in a MAC address.
- Exclude switch trunk ports— Select the check box to exclude switch trunk ports from the switch port trace.

Note When more than one port is traced for a given MAC address, additional checks are performed to improve accuracy. These checks include the: trunk port, non-AP CDP neighbors present on the port, and whether or not the MAC address is the only one on this port.

- Exclude device list— Select the check box to exclude additional devices from the trace. Enter into the device list text box each device that you want to exclude from the switch port trace. Separate device names with a comma.
- Max hop count— Enter the maximum number of hops for this trace. Keep in mind that the greater the hop count, the longer the switch port trace takes to perform.

Note This hop count value is not applicable for Auto SPT.

- Exclude vendor list— Enter in the vendor list text box any vendors that you want to exclude from the switch port trace. Separate vendor names with commas. The vendor list is not case sensitive.

Step 3 Configure the following advanced settings:

- TraceRogueAP task max thread— Switch port tracing uses multiple threads to trace rogue access points. This field indicates the maximum number of rogue access points that can be traced on parallel threads.
- TraceRogueAP max queue size— Switch port tracing maintains a queue to trace rogue access points. Whenever you select a rogue access point for tracing, it is queued for processing. This field indicates the maximum number of entries that you can store in the queue.
- SwitchTask max thread— Switch port tracing uses multiple threads to query switch devices. This field indicates the maximum number of switch devices that you can query on parallel threads.

The default value for these parameters should be good for normal operations. These parameters directly impact the performance of switch port tracing and Prime Infrastructure. Unless required, we do not recommend that you alter these parameters.

- Select CDP device capabilities— Select the check box to enable.

Prime Infrastructure uses CDP to discover neighbors during tracing. When the neighbors are verified, Prime Infrastructure uses the CDP capabilities field to determine whether or not the neighbor device is a valid switch. If the neighbor device is not a valid switch, it is not traced.

- Step 4** Click **Save** to confirm changes made. Click **Reset** to return the page to the original settings. Click **Factory Reset** to return settings to the factory defaults.

View the switch port trace details

To view the switch port trace details, follow these steps:

- Step 1** Add switches with full licenses using the **Configuration > Network > Network Devices** page.
- Step 2** Enable Auto switch port tracing in **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Auto SPT** page.
- Step 3** Schedule to run wired client status Major Polling background task in **Administration > Dashboards > Job Dashboard** page.
- Step 4** Click the Trace switch port icon in Rogue AP detail page. New pop up will show details of switch port traced. Click the detail status to check trace status such as started/Found, and so on.



Note Manual SPT will work, even if you do not add any switch to Prime Infrastructure. But you should configure the SNMP credentials correctly in **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT** page. “Private” is the default credential, and will be used during manual Switch Port Tracing if you do not configure it.

- If a switch is added to Prime Infrastructure by selecting **Configuration > Network > Network Devices**, the SNMP credentials entered for the switch will override any switch SNMP credentials entered here, and will be used for switch port tracing. You can change the switch SNMP credentials in the **Configuration > Network > Network Devices** page. Prime Infrastructure will not require any license for adding switch with SPT and will not display wired clients connected to the switches. The **Monitor > Managed Elements > Network Devices > Device Groups > Device Type > Switches and Hubs** page will not display the switch details added with SPT.
- Prime Infrastructure requires full license for adding switch. The **Monitor > Managed Elements > Network Devices > Device Groups > Device Type > Switches and Hubs** page will display the switch details added with full license. Prime Infrastructure will also display wired clients connected to switches. Location of switches is tracked with MSE.

Establish Switch Port Tracing

- Step 1** Choose **Dashboard > Wireless > Security**.
- Step 2** In the **Malicious Rogue APs**, **Unclassified Rogue APs**, **Friendly Rogue APs**, **Custom Rogue APs**, and **Adhoc Rogues** dashlets: Click the number links showing how many rogues have been identified in the Last Hour, last 24 Hours, or Total Active. The Alarms window opens, showing alarms for the suspected rogues.
- Step 3** Choose the rogue for which you want to set up switch port tracking by selecting the check box next to it.
- Step 4** Expand the applicable alarm and manually select the **Trace Switch Port** button under the Switch Port Tracing subsection of the alarm details.

When one or more searchable MAC addresses are available, Prime Infrastructure uses CDP to discover any switches connected up to two hops away from the detecting access point. The MIBs of each CDP discovered switch is examined to see if it contains any of the target MAC addresses. If any of the MAC addresses are found, the corresponding port number is returned and reported as the rogue switch port.

See [Switch Port Tracing Details](#), on page 249 for additional information on the Switch Port Tracing Details dialog box.

Configure SNMP Credentials for Rogue AP Tracing

The SNMP Credentials page allows you to specify credentials to use for tracing rogue access points. Use this option when you cannot find a specific entry using a number-based entry. When a switch credential is not added to Cisco Prime Infrastructure, you can use SNMP credentials on this page to connect to the switch.

- Step 1** Choose **Administration > Settings > System Settings**, then choose **Network and Device > Switch Port Trace (SPT) > Manual SPT**. The Manual SPT page appears.
- Step 2** View or edit the details for a current SNMP credential entry by clicking the Network Address link for that entry. For details on this task, see “Configure Global SNMP Settings” and “View SNMP Credential Details” in related topics. Note that the default entry is for network 0.0.0.0, which indicates the entire network. SNMP credentials are defined per network, so only network addresses are allowed. The SNMP credentials defined for network 0.0.0.0 is the SNMP credential default. It is used when no specific SNMP credential is defined. You should update the pre-populated SNMP credential with your own SNMP information.
- Step 3** To add a new SNMP entry, choose **Select a command > Add SNMP Entries > Go** (see “Add SNMP Credentials”).
-

Related Topics

- [Configure Global SNMP Settings](#), on page 82
- [View SNMP Credential Details](#), on page 83
- [Add SNMP Credentials](#), on page 84

Switch Port Tracing Details

In the Switch Port Tracing Details dialog box, you can enable or disable switch ports, trace switch ports, and view detail status of the access point switch trace.

For more information on Switch Port Tracing, see the following related topics:

In the Switch Port tracing Details dialog box, do one of the following:

- Click Enable/Disable Switch Port(s)— Enables or disables any selected ports.
- Click Trace Switch Port(s)— Runs another switch port trace.
- Click Show Detail Status— Displays details regarding the switch port traces for this access point.
- Click Close.

Related Topics

[Configure Switch Port Tracing](#), on page 246

[Configure SNMP Credentials for Rogue AP Tracing](#), on page 249

Switch Port Tracing Troubleshooting

Switch Port Tracing (SPT) works on a best-effort basis. SPT depends on the following information to correctly trace and contain rogue APs:

- Reporting access points— A rogue access point must be reported by one or more managed access points.
- Access point CDP neighbor— Access point Cisco Discovery Protocol (CDP) neighbor information is required to determine the seed switches.
- Switch IP address and SNMP credentials
 - All the switches that need to be traced should have a management IP address and SNMP management enabled.
 - With the new SNMP credential changes, instead of adding the individual switches to Prime Infrastructure, network address based entries can be added.
 - The new SNMP credential feature has a default entry 0.0.0.0 with default community string as private for both read/write.
 - The correct write community string has to be specified to enable/disable switch ports. For tracing, a read community string should be sufficient.
- Switch port configuration
 - Switch ports that are trunking should be correctly configured as trunk ports.
 - Switch port security should be disabled.
- Switch Port Tracing is supported only on Cisco Ethernet switches and the following Catalyst switches: 2960, 3560, 3560-E, 3650, 3750-E, 3750-X, 3850, 4500 and 6500 series.
- Switch VLAN settings should be properly configured.
- CDP protocol should be enabled for all the switches.
- An Ethernet connection should exist between the rogue access point and the Cisco switch.
- There should be some traffic between the rogue access point and the Ethernet switch.
- The rogue access point should be connected to a switch within the max hop limit. Default hop is 2. Max hop is 10.
- If SNMPv3 is used, then make sure you use the context option and create one for each VLAN in addition to the one for the main group (which is required for non-VLAN based MIBs).

Frequently Asked Questions on Rogues and Switch Port Tracing

The following related topics answer a variety of questions about Prime Infrastructure rogue AP detection and switch port tracing (SPT).

Related Topics

- [How Do You Configure Auto SPT?](#), on page 251
- [How Does Auto SPT Differ From Manual SPT?](#), on page 251
- [Where Can I See SPT Results \(Manual and Auto\)?](#), on page 252
- [How Can I Ensure Auto SPT Runs Smoothly](#)
- [Why Does Auto SPT Take Longer to Find Wired Rogues?](#), on page 252
- [How Can I Detect Wired Rogues on Trunk Ports?](#), on page 253
- [How Can I Use the Auto SPT “Eliminate By Location” Feature?](#), on page 254
- [What is the Difference Between “Major Polling” and “Minor Polling”?](#), on page 254

How Do You Configure Auto SPT?

Follow the steps below to configure automatic SPT:

-
- Step 1** Use **Configuration > Network > Network Devices > Add Device** to add switches with a **License Level** of **Full**.
 - Step 2** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Auto SPT** and select **Enable Auto Switch Port Tracing**. Click **OK**.
 - Step 3** Select **Administration > Settings > Background Tasks > Wired Client Status**. Make sure this task is enabled and that it is scheduled to run at least twice a day.
-

Related Topics

- [Where Can I See SPT Results \(Manual and Auto\)?](#), on page 252
- [How Can I Ensure Auto SPT Runs Smoothly?](#)
- [Frequently Asked Questions on Rogues and Switch Port Tracing](#), on page 250

How Does Auto SPT Differ From Manual SPT?

Manual SPT runs against individual rogue AP alarms. You must trigger it by clicking on the **Trace Switch Port** icon on the details page for a rogue AP alarm.

Auto SPT runs on batches of alarms, automatically, on the schedule defined for the Wired Client Status background task.

Note that manual SPT triggering depends on CDP being enabled on the access points and switches with appropriate SNMP community strings. For more information on manual SPT and how it works, see the WCS Switch Port Trace Demonstration link in related topics.

Auto and manual SPT also differ in the way they handle licensing and the switch “license level”, which can be set to either “Full” or “Switch Port Trace Only” when adding the switch. These three cases demonstrate the differences:

- **Adding switches with “Full” license level:** Prime Infrastructure consumes a license for every added switch with a full license level. All the wired clients connected to switches can be seen by selecting **Monitor > Managed Elements > Network Devices > Device Type > Switches and Hubs**. You can also use MSE to track switch locations. A “Full” license level is mandatory for Auto SPT to be functional.
- **Adding no Switches:** Manual SPT will still work even without adding any switches. But you must remember to configure SNMP credentials appropriately for all switches, using **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**.
- **Adding switches with “Switch Port Trace Only” license level:** If you add a switch to Prime Infrastructure using **Configuration > Network > Network Devices > Add Device**, but select a **Switch**

Port Trace Only license level, the SNMP credentials you enter when adding the switch will override the SNMP credentials entered using **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > Manual SPT**. The entered credentials will be used for switch port tracing. This is the main difference between not adding switches and adding switches with a license level of “Switch Port Tracing Only”. Prime Infrastructure will not consume any licenses for switches with an SPT-only license level, will not show these switches under **Monitor > Managed Elements > Network Devices > Device Type > Switches and Hubs**, and will not show wired clients connected to these switches.

For more information, See [WCS Switch Port Trace Demonstration](#).

Related Topics

[What is the Difference Between “Major Polling” and “Minor Polling”?](#), on page 254
[Frequently Asked Questions on Rogues and Switch Port Tracing](#), on page 250

Where Can I See SPT Results (Manual and Auto)?

-
- Step 1** Display details for the Rogue AP alarm in which you are interested. For example:
- Click the **Alarm Summary** icon at the top of any Prime Infrastructure page. A list of alarm categories appears.
 - Click the **Rogue AP** link in the list. Prime Infrastructure displays the list of rogue AP alarms.
 - Expand the rogue AP alarm you want. The details page for that alarm appears.
- Step 2** In the **Switch Port Tracing** pane, click the **Trace Switch Port** icon. The Switch Port Trace window shows the details of the traced switch port.
- If no SPT has been performed, click **Trace Switch Port(s)** to start tracing. Click the **Show Detail Status** button to get details on the status of the trace as it progresses.

Related Topics

[Frequently Asked Questions on Rogues and Switch Port Tracing](#), on page 250

Why Does Auto SPT Take Longer to Find Wired Rogues?

Auto SPT takes relatively longer to find wired rogues than does manual SPT for the following reasons:

- Auto SPT depends on the wired client discovery process, which happens only when the Wired Client Status major polling background task runs. By default, the major poll for this background task is scheduled to run only after every two minor polls, or once every four hours.
- Even though the wired rogue AP is connected to a switch, Prime Infrastructure will discover a wired port only when the wired rogue AP is in the “associated” state. Prime Infrastructure always checks whether a wired client’s status is associated or disassociated. If the wired client status is disassociated, Prime Infrastructure shows this as no port connected.
- Rogue tracing is done in batches. The time taken to find a particular wired rogue depends on the batch in which Prime Infrastructure processes it. If a particular rogue was processed in the previous batch, it takes more time to trace it.
- The time taken to discover any wired rogue depends upon the number of rogue alarms present in Prime Infrastructure and the interval between Wired Client Status major polls.

Related Topics

[What is the Difference Between “Major Polling” and “Minor Polling”?](#), on page 254

[Frequently Asked Questions on Rogues and Switch Port Tracing](#), on page 250

How Can I Detect Wired Rogues on Trunk Ports?

You can detect wired rogues on trunk ports by following the steps below.

Note that if you are trying to detect rogues on trunk ports for Cisco 2950 switches, you must first install the updated 2950 support in Prime Infrastructure Device Pack 5.0.

-
- Step 1** Choose **Administration > Settings > System Settings > Network and Device > Switch Port Trace (SPT) > SPT Configuration**.
- Step 2** Uncheck the **Exclude switch trunk ports** check box, then click **Save**.
- Step 3** Choose **Administration > Settings > System Settings > Client and User > Client**.
- Step 4** Check the **Discover wired clients on trunk ports** check box, then click **Save**.

Switches will start detecting wired clients on trunk ports starting with the next execution of a major poll by the Wired Client Status background task.

Related Topics

[How Do You Configure Auto SPT?](#), on page 251

[What is the Difference Between “Major Polling” and “Minor Polling”?](#), on page 254

[Frequently Asked Questions on Rogues and Switch Port Tracing](#), on page 250

How Do You Configure Switch Port Location?

Follow the steps below to configure Switch Port Location:

-
- Step 1** Use **Configuration > Network > Network Devices > Switches and Hubs**.
- Step 2** Click a Device Name. By default, Configuration tab opens.
- Step 3** Click Switch Port Location in the top right corner.
- Step 4** Select the check box(es) of one or more ports to configure location, and from choose Configure Location from the drop-down list, then click Go.
- Step 5** In the Map Location group, you can configure the following:
- From the Campus/Site drop-down list, choose the campus map for the switch or switch port.
 - From the Building drop-down list, choose the building map location for the switch or switch port.
 - From the Floor drop-down list, choose the floor map.
 - If you have already saved a file with the Campus/Site, Building, and Floor details, click Import Civic. This imports civic information for the MSE using Prime Infrastructure. Enter the name of the text file or browse for the filename, and click Import.
- Step 6** In the ELIN and Civic Location group box, you can configure the following:
- Enter the Emergency Location Identifier Number (ELIN) in the ELIN text box. ELIN is a number that can be used by the local public safety answering point (PSAP) to look up the geographic location of the caller in a master database known as the automatic location information (ALI) database. The ELIN also allows the PSAP to contact the emergency caller directly in the event the phone call is disconnected.
 - Complete the required fields on the Civic Address and Advanced tabs.

- If you have the ELIN and Civic location information saved in a file, you can import it by clicking Import Switch Location.

Step 7 Click Save.

Related Topics

[How Can I Ensure Auto SPT Runs Smoothly?](#)

[How Do You Configure Auto SPT?](#), on page 251

[Frequently Asked Questions on Rogues and Switch Port Tracing](#), on page 250

How Can I Use the Auto SPT “Eliminate By Location” Feature?

“Eliminate by location” is one of the algorithms Prime Infrastructure uses to detect wired rogues. It uses the rogue AP location information to search for the associated switch ports. It helps to reduce false positives during Auto SPT processing, using the floor ID of the detecting APs, and increases accuracy in tracking wired rogues.

When “Eliminate by location” is enabled, the Wired Client Status background task discovers all the wired clients from managed switches. The next time auto SPT runs, switch ports will be filtered based on the “eliminate by location” algorithm.

Follow these steps to enable “eliminate by location”:

-
- Step 1** Integrate Cisco Mobility Service Engine (MSE) with Prime Infrastructure.
- Step 2** Ensure that MSE is in sync with the defined floor area where the detecting APs are placed. MSE should be able to track the rogues.
- Step 3** Add all switches to Prime Infrastructure.
- Step 4** After all switches are added to PI and are in the managed state, all switch ports need to be configured for the algorithm to work. If all switches are not configured with switch ports, then the false positive results occur. You can configure from the **Configuration > Network > Network Devices > Switches and Hubs > click on a Device Name > click Switch Port Location** in the top right corner.
- Step 5** Place the detecting access points on the map and make sure that the Cisco MSE is synchronized and rogues APs are detected on the floor.
- Eliminate By Location algorithm takes the floor ID of detecting APs and eliminates all others. If some switch ports are not configured, then the value of those ports will be set to Zero and will be considered. Hence the results may contain false positives, which contains the exact floor ID and floor ID which has the value zero.
- Step 6** Configure switch port locations to ensure that all ports are assigned to the correct floor area.

Related Topics

[How Do You Configure Switch Port Location?](#), on page 253

[How Do You Configure Auto SPT?](#), on page 251

[Frequently Asked Questions on Rogues and Switch Port Tracing](#), on page 250

What is the Difference Between “Major Polling” and “Minor Polling”?

The Wired Client Status background task that triggers auto SPT Definitions are as follows:

Major Polling: During a major poll, Prime Infrastructure triggers client discovery on all wired device ports by syncing all of the essential client information with the database. In Prime Infrastructure 2.2, the frequency of this poll was reduced from twice a day. It is now fully configurable.

Minor Polling: During a minor poll, Prime Infrastructure triggers client discovery only on device interfaces and ports which became active recently. Prime Infrastructure uses interface uptime data to detect when a port or interface is recently added or removed by any client.

Related Topics

[How Does Auto SPT Differ From Manual SPT?](#), on page 251

[Why Does Auto SPT Take Longer to Find Wired Rogues?](#), on page 252

[Frequently Asked Questions on Rogues and Switch Port Tracing](#), on page 250

What is the Difference Between "Major Polling" and "Minor Polling"?



CHAPTER 11

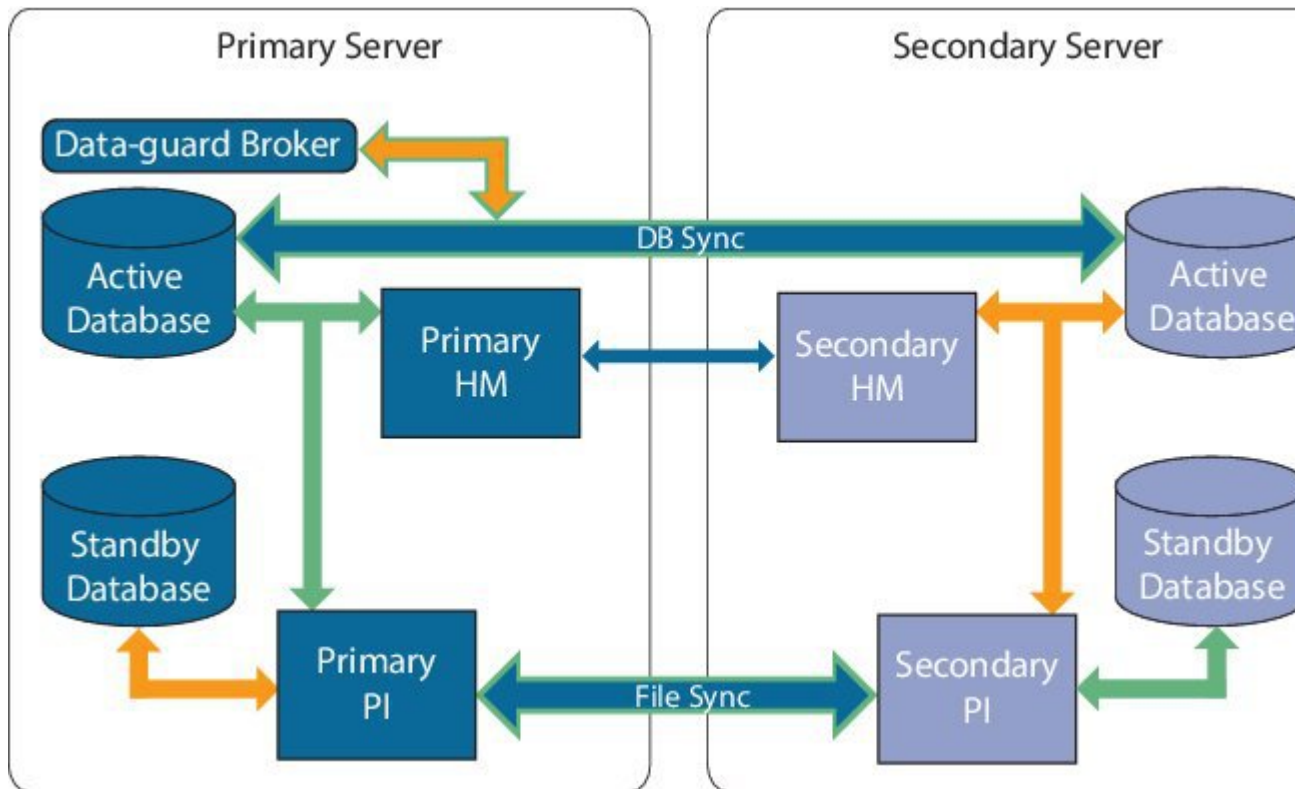
Configure High Availability

- [How High Availability Works, on page 257](#)
- [Planning HA Deployments, on page 264](#)
- [Set Up High Availability, on page 271](#)
- [How to Patch HA Servers, on page 278](#)
- [Monitor High Availability, on page 283](#)
- [High Availability Reference Information, on page 295](#)
- [Configure MSE High Availability , on page 302](#)

How High Availability Works

The following figure shows the main components and process flow for a Prime Infrastructure High Availability (HA) setup with the primary server in the active state.

Figure 1: HA Deployment



An HA deployment consists of two Prime Infrastructure servers: a primary and a secondary. Each of these servers has an active database and a standby backup copy of the active database. Under normal circumstances, the primary server is active: It is connected to its active database while it manages the network. The secondary server is passive, connected only to its standby database, but in constant communication with the primary server.

The Health Monitor processes running on both servers monitor the status of its opposite server. Oracle Recovery Manager (RMAN) running on both servers creates the active and standby databases and synchronizes the databases when there are changes, with the help of Oracle Data Guard Broker running on the primary server.

When the primary server fails, the secondary takes over, connecting to its active database, which is in sync with the active primary database. You can trigger this switch, called a “failover”, either manually, which is recommended, or have it triggered automatically. You then use the secondary server to manage the network while working to restore access to the primary server. When the primary is available again, you can initiate a switch (called a “failback”) back to the primary server and resume network management using the primary.

If you choose to deploy the primary and secondary servers on the same IP subnet, you can configure your devices to send a notifications to Prime Infrastructure at a single virtual IP address. If you choose to disperse the two servers geographically, such as to facilitate disaster recovery, you will need to configure your devices to send notifications to both servers.

Related Topics

[About the Primary and Secondary Servers](#), on page 259

[Sources of Failure](#), on page 259

[File and Database Synchronization](#), on page 259

[HA Server Communications](#), on page 260

[Health Monitor Process](#), on page 260

[Health Monitor Web Page](#), on page 261

[Using Virtual IP Addressing With HA](#), on page 262

[How to Use SSL Certificates in an HA Environment?](#), on page 263

[Import Client Certificates Into Web Browsers](#), on page 264

About the Primary and Secondary Servers

In any Prime Infrastructure HA implementation, for a given instance of a primary server, there must be one and only one dedicated secondary server.

Typically, each HA server has its own IP address or host name. If you place the servers on the same subnet, they can share the same IP using virtual IP addressing, which simplifies device configuration. The primary and secondary servers of Prime Infrastructure must be enabled on a network interface ethernet0 (eth0) during HA implementation.

Once HA is set up, you should avoid changing the IP addresses or host names of the HA servers, as this will break the HA setup (see “Reset the Server IP Address or Host Name” in Related Topics).

Related Topics

[How High Availability Works](#), on page 257

[Using Virtual IP Addressing With HA](#), on page 262

[Reset the HA Server IP Address or Host Name](#), on page 302

Sources of Failure

Prime Infrastructure servers can fail due to issues in one or more of the following areas:

- **Application Processes:** Failure of one or more of the Prime Infrastructure server processes, including NMS Server, MATLAB, TFTP, FTP, and so on. You can view the operational status of each of these application processes by running the ncs status command through the admin console.
- **Database Server:** One or more database-related processes could be down. The Database Server runs as a service in Prime Infrastructure.
- **Network:** Problems with network access or reachability issues.
- **System:** Problems related to the server's physical hardware or operating system.
- **Virtual Machine (VM):** Problems with the VM environment on which the primary and secondary servers were installed (if HA is running in a VM environment).

For more information, see [How High Availability Works](#)

File and Database Synchronization

Whenever the HA configuration determines that there is a change on the primary server, it synchronizes this change with the secondary server. These changes are of two types:

1. **Database:** These include database updates related to configuration, performance and monitoring data.
2. **File:** These include changes to configuration files.

Oracle Recovery Manager (RMAN) running on both servers creates the active and standby databases and synchronizes the databases when there are changes, with the help of Oracle Data Guard Broker running on the primary server.

File changes are synchronized using the HTTPS protocol. File synchronization is done either in:

- **Batch:** This category includes files that are not updated frequently (such as license files). These files are synchronized once every 500 seconds.
- **Near Real-Time:** Files that are updated frequently fall under this category. These files are synchronized once every 11 seconds.

By default, the HA framework is configured to copy all the required configuration data, including:

- Report configurations
- Configuration Templates
- TFTP-root
- Administration settings
- Licensing files

Related Topics

[How High Availability Works](#), on page 257

HA Server Communications

The primary and secondary HA servers exchange the following messages in order to maintain the health of the HA system:

- **Database Sync:** Includes all the information necessary to ensure that the databases on the primary and secondary servers are running and synchronized.
- **File Sync:** Includes frequently updated configuration files. These are synchronized every 11 seconds, while other infrequently updated configuration files are synchronized every 500 seconds.
- **Process Sync:** Ensures that application- and database-related processes are running. These messages fall under the Heartbeat category.
- **Health Monitor Sync:** These messages check for the following failure conditions:
 - Network failures
 - System failures (in the server hardware and operating system)
 - Health Monitor failures

Related Topics

[How High Availability Works](#), on page 257

Health Monitor Process

Health Monitor (HM) is the main component managing HA operations. Separate instances of HM run as an application process on both the primary and the secondary server. HM performs the following functions:

- Synchronizes database and configuration data related to HA (this excludes databases that sync separately using Oracle Data Guard).
- Exchanges heartbeat messages between the primary and secondary servers every five seconds, to ensure communications are maintained between the servers.
- Checks the available disk space on both servers at regular intervals, and generates events when storage space runs low.
- Manages, controls and monitors the overall health of the linked HA servers. If there is a failure on the primary server then it is the Health Monitor's job to activate the secondary server.

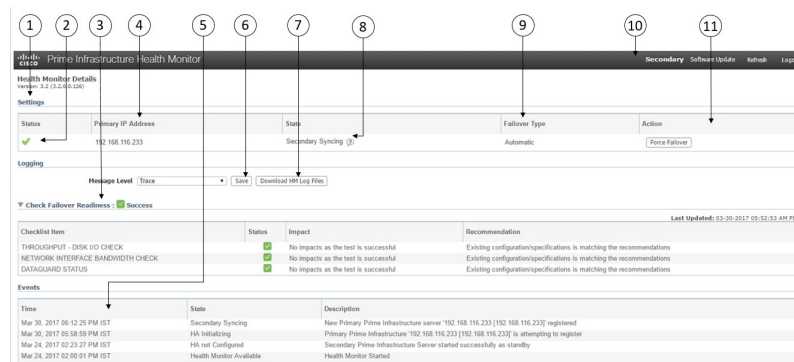
Related Topics

[How High Availability Works](#), on page 257

Health Monitor Web Page

You control HA behavior using the Health Monitor web page. Each Health Monitor instance running on the primary server or secondary server has its own web page. The following figure shows an example of the Health Monitor web page for a secondary server in the “Primary Active” and “Secondary Syncing” state.

Figure 2: Health Monitor Web Page (Secondary Server)



1	Settings area displays Health Monitor state and configuration detail in five separate sections.
2	Status indicates current functional status of the HA setup (green check mark indicates that HA is on and working).
3	Check Failover Readiness field displays the values of system failback and system failover details of the checklist items. For more details, see "Check Failover Readiness" given below the table.
4	Primary IP Address identifies the IP of the peer server for this secondary server (on the primary server, this field is labeled “Secondary IP Address”).
5	Events table displays all current HA-related events, in chronological order, with most recent event at the top.
6	Message Level field lets you change the logging level (your choice of Error, Informational, or Trace). You must press Save to change the logging level.
7	Logging Download area lets you download Health Monitor log files.
8	State shows current HA state of the server on which this instance of Health Monitor is running.
9	Failover Type shows whether you have Manual or Automatic failover configured.
10	Identifies the HA server whose Health Monitor web page you are viewing.

11	Action shows actions you can perform, such as failover or failback. Action buttons are enabled only when Health Monitor detects HA state changes needing action.
-----------	--

Check Failover Readiness section description:

Checklist Name	Description
SYSTEM - CHECK DISK IOPS	This validates the disk iops in both primary and secondary server. The minimum expected disk iops is 200 MBps.
NETWORK - CHECK NETWORK INTERFACE BANDWIDTH	This checks if the eth0 interface speed matches the recommended speed of 100 Mbps in both primary and secondary sever. This test will not measure network bandwidth by transmitting data between primary and secondary server.
NETWORK - CHECK NETWORK BANDWIDTH SPEED	This checks if the network bandwidth speed matches the recommended speed of 100 Mbps in both primary and secondary sever. This test will measure network bandwidth by transmitting data between primary and secondary server.
DATABASE - SYNC STATUS	This ensures the oracle data guard broker configuration which syncs the primary and secondary database.

Trend Graph for Check Failover Readiness :

- Click **Click here** link in the Trend Graph to check the trend graphs for all the check failover readiness test. The trend graphs shows the historical summary of the test and status on the stability of the System/Network.
- Click **Select Date Range** to modify date and time, Click **Apply**. By default, trend graphs displays the latest 6 hours value.

Related Topics

[How High Availability Works](#), on page 257

[How to Resolve Database Synchronization Issues](#), on page 295

Using Virtual IP Addressing With HA

Under normal circumstances, you configure the devices that you manage using Prime Infrastructure to send their syslog, SNMP traps and other notifications to the Prime Infrastructure server's IP address. When HA is implemented, you will have two separate Prime Infrastructure servers, with two different IP addresses. If we fail to reconfigure devices to send their notifications to the secondary server as well as the primary server, then when the secondary Prime Infrastructure server goes into Active mode, none of these notifications will be received by the secondary server.

Setting all of your managed devices to send notifications to two separate servers demands extra device configuration work. To avoid this additional overhead, HA supports use of a virtual IP that both servers can share as the Management Address. The two servers will switch IPs as needed during failover and failback

processes. At any given time, the virtual IP Address will always point to the correct Prime Infrastructure server.

Note that you cannot use virtual IP addressing unless the addresses for both of the HA servers and the virtual IP are all in the same subnet. This can have an impact on how you choose to deploy your HA servers (see “Planning HA Deployments” and “Using the Local Model” in Related Topics).

Also note that a virtual IP address is in no way intended as a substitute for the two server IP addresses. The virtual IP is intended as a destination for syslogs and traps, and for other device management messages *being sent to the* Prime Infrastructure servers. Polling of devices is always conducted from one of the two Prime Infrastructure server IP addresses. Given these facts, if you are using virtual IP addressing, you must open your firewall to incoming and outgoing TCP/IP communication on all three addresses: the virtual IP address as well as the two actual server IPs.

You can also use virtual IP addressing if you plan to use HA with Operations Center. You can assign a virtual IP as SSO to the Prime Infrastructure instance on which Operations Center is enabled. No virtual IP is needed for any of the instances managed using Operations Center (see “Enable HA for Operations Center”).

You can enable virtual IP addressing during HA registration on the primary server, by specifying that you want to use this feature and then supplying the virtual IPv4 (and, optionally, IPv6) address you want the primary and secondary servers to share (see “How to Register HA on the Primary Server”).

To remove Virtual IP addressing after it is enabled, you must remove HA completely (see “Remove HA Via the GUI”).

Related Topics

[What If I Cannot Use Virtual IP Addressing?](#), on page 268

[Planning HA Deployments](#), on page 264

[Using the Local Model](#), on page 266

[Enable HA for Operations Center](#), on page 269

[How to Register HA on the Primary Server](#), on page 273

[How High Availability Works](#), on page 257

[Remove HA Via the GUI](#), on page 299

How to Use SSL Certificates in an HA Environment?

If you decide to use SSL certification to secure communications between Prime Infrastructure server and users, and also plan to implement HA, you will need to generate separate certificates for both the primary and secondary HA servers.

These certificates must be generated using the FQDN (Fully Qualified Domain Name) for each server. To clarify: You must use the primary server’s FQDN to generate the certificate you plan to use for the primary server, and the secondary server’s FQDN to generate the certificate you plan to use for the secondary server.

Once you have generated the certificates, import the signed certificates to the respective servers.

Do not generate SSL certificates using a virtual IP address. The virtual IP address feature is used to enable communications between Prime Infrastructure and your network devices.

To set up HTTPS access for Cisco Prime Infrastructure, see [Set Up HTTPS Access to Prime Infrastructure](#)

Import Client Certificates Into Web Browsers

Users accessing Prime Infrastructure servers with certificate authentication must import client certificates into their browsers in order to authenticate. Although the process is similar across browsers, the actual details vary with the browser. The following procedure assumes that your users are using a Prime Infrastructure compatible version of Firefox.

You must ensure that the user importing the client certificates has:

- Downloaded a copy of the certificate files to a local storage resource on the client machine
- If the certificate file is encrypted: The password with which the certificate files were encrypted.

-
- Step 1** Launch Firefox and enter the following URL in the location bar: **about:preferences#advanced**.
Firefox displays its **Options > Advanced** tab.
- Step 2** Select **Certificates > View Certificates > Your Certificates**, then click **Import...**
- Step 3** Navigate to the downloaded certificate files, select them, then click **OK** or **Open**.
- Step 4** If the certificate files are encrypted: You will be prompted for the password used to encrypt the certificate file. Enter it and click **OK**.
The certificate is now installed in the browser.
- Step 5** Press **Ctrl+Shift+Del** to clear the browser cache.
- Step 6** Point the browser to the Prime Infrastructure server using certificate authentication.
You will be prompted to select the certificate with which to respond to the server authentication requested. Select the appropriate certificate and click **OK**.
-

Hot Standby Behavior

When the primary server is active, the secondary server is in constant synchronization with the primary server and runs all Prime Infrastructure processes for fast switch over. When the primary server fails, the secondary server immediately takes over the active role within two to three minutes after the failover.

Once issues in the primary server are resolved and it is returned to a running state, the primary server assumes a standby role. When the primary server is in the standby role, the Health Monitor GUI shows “Primary Syncing” state during which the database and files on the primary start to sync with the active secondary.

When the primary server is available again and a failback is triggered, the primary server again takes over the active role. This role switching between the primary and secondary servers happens within two to three minutes.

Related Topics

[How High Availability Works](#), on page 257

Planning HA Deployments

Prime Infrastructure’s HA feature supports the following deployment models:

- **Local:** Both of the HA servers are located on the same subnet (giving them Layer 2 proximity), usually in the same data center.
- **Campus:** Both HA servers are located in different subnets connected via LAN. Typically, they will be deployed on a single campus, but at different locations within the campus.
- **Remote:** Each HA server is located in a separate, remote subnet connected via WAN. Each server is in a different facility. The facilities are geographically dispersed across countries or continents.

The following sections explain the advantages and disadvantage of each model, and discusses underlying restrictions that affect all deployment models.

HA will function using any of the supported deployment models. The main restriction is on HA's performance and reliability, which depends on the bandwidth and latency criteria discussed in "Network Throughput Restrictions on HA". As long as you are able to successfully manage these parameters, it is a business decision (based on business parameters, such as cost, enterprise size, geography, compliance standards, and so on) as to which of the available deployment models you choose to implement.

Related Topics

[Network Throughput Restrictions on HA](#), on page 265

[Using the Local Model](#), on page 266

[Using the Campus Model](#), on page 267

[Using the Remote Model](#), on page 267

[What If I Cannot Use Virtual IP Addressing?](#), on page 268

[Automatic Versus Manual Failover](#), on page 268

[Enable HA for Operations Center](#), on page 269

Network Throughput Restrictions on HA

Prime Infrastructure HA performance is always subject to the following limiting factors:

- The net bandwidth available to Prime Infrastructure for handling all operations. These operations include (but are not restricted to) HA registration, database and file synchronization, and triggering failback.
- The net latency of the network across the links between the primary and secondary servers. Irrespective of the physical proximity of these two servers, high latency on these links can affect how Prime Infrastructure maintains sessions between the primary and secondary servers.
- The net throughput that can be delivered by the network that connects the primary and secondary servers. Net throughput varies with the net bandwidth and latency, and can be considered a function of these two factors.

These limits apply to at least some degree in every possible deployment model, although some models are more prone to problems than others. For example: Because of the high level of geographic dispersal, the Remote deployment model is more likely to have problems with both bandwidth and latency. But both the Local and Campus models, if not properly configured, are also highly susceptible to problems with throughput, as they can be saddled by low bandwidth and high latency on networks with high usage.

You will rarely see throughput problems affecting a failback or failover, as the two HA servers are in more or less constant communication and the database changes are replicated quickly. Most failovers and failbacks take approximately two to three minutes.

The main exception to this rule is the delay for a full database copy operation. This kind of operation is triggered when the primary server has been down for more than the data retention period and you then bring it back up. The data retention period for the express, express-plus and standard configurations server is six hours and for professional and Gen 2 appliance server it is 12 hours.

Prime Infrastructure will trigger a full database copy operation from the secondary to the primary. No failback is possible during this period, although the Health Monitor page will display any events encountered while the database copy is going on. As soon as the copy is complete, the primary server will go to the “Primary Syncing” state, and you can then trigger failback. Be sure not to restart the primary server or disconnect it from the network while the full database copy is in progress.

Variations in net throughput during a full database copy operation, irrespective of database size or other factors, can mean the difference between a database copy operation that completes successfully in under an hour and one that does not complete at all. Cisco has tested the impact of net throughput on HA deployment in configurations following the Remote model, using typical Prime Infrastructure database sizes of between 105 GB and 156 GB. Based on these tests, Cisco recommends for a typical database of 125 GB (generating a 10 GB backup file):

- For best results: With sub-millisecond latency, and net throughput of 977 Mbps or more, expect a complete database copy time of one hour or less.
- For good results: With latency of 70 milliseconds, and net throughput of 255 Mbps or more, expect a complete database copy time of two hours or less.
- For acceptable results: With latency of 220 milliseconds or less, and net throughput of 86 Mbps or more, expect a complete database copy time of 4.5 hours or less.

With latencies of 330ms or higher, and throughput of 46Mbps or less, you run the risk of the database copy not completing successfully.

Related Topics

[Planning HA Deployments](#), on page 264

[Using the Remote Model](#), on page 267

Using the Local Model

The main advantage of the Local deployment model is that it permits use of a virtual IP address as the single management address for the system. Users can use this virtual IP to connect to Prime Infrastructure, and devices can use it as the destination for their SNMP trap and other notifications.

The only restriction on assigning a virtual IP address is to have that IP address in the same subnet as the IP address assignment for the primary and secondary servers. For example: If the primary and secondary servers have the following IP address assignments within the given subnet, the virtual IP address for both servers can be assigned as follows:

- Subnet mask: 255.255.255.224 (/27)
- Primary server IP address: 10.10.101.2
- Secondary server IP address: 10.10.101.3
- Virtual IP address: 10.10.101.[4-30] e.g., 10.10.101.4. Note that the virtual IP address can be any of a range of addresses that are valid and unused for the given subnet mask.

In addition to this main advantage, the Local model also has the following advantages:

- Usually provides the highest bandwidth and lowest latency.
- Simplified administration.
- Device configuration for forwarding syslogs and SNMP notifications is much easier.

The Local model has the following disadvantages:

- Being co-located in the same data center exposes them to site-wide failures, including power outages and natural disasters.

- Increased exposure to catastrophic site impacts will complicate business continuity planning and may increase disaster-recovery insurance costs.

Related Topics

[Planning HA Deployments](#), on page 264

[Using the Campus Model](#), on page 267

[Using the Remote Model](#), on page 267

Using the Campus Model

The Campus model assumes that the deploying organization is located at one or more geographical sites within a city, state or province, so that it has more than one location forming a “campus”. This model has the following advantages:

- Usually provides bandwidth and latency comparable to the Local model, and better than the Remote model.
- Is simpler to administer than the Remote model.

The Campus model has the following disadvantages:

- More complicated to administer than the Local model.
- Does not permit use of a virtual IP address as the single management address for the system, so it requires more device configuration (see “What If I Cannot Use Virtual IP Addressing?” in Related Topics).
- May provide lower bandwidth and higher latency than the Local model. This can affect HA reliability and may require administrative intervention to remedy (see “Network Throughput Restrictions on HA” in Related Topics).
- While not located at the same site, it will still be exposed to city, state, or province-wide disasters. This may complicate business continuity planning and increase disaster-recovery costs.

Related Topics

[Planning HA Deployments](#), on page 264

[Network Throughput Restrictions on HA](#), on page 265

[Using the Local Model](#), on page 266

[Using the Remote Model](#), on page 267

[What If I Cannot Use Virtual IP Addressing?](#), on page 268

Using the Remote Model

The Remote model assumes that the deploying organization has more than one site or campus, and that these locations communicate across geographical boundaries by WAN links. It has the following advantages:

- Least likely to be affected by natural disasters. This is usually the least complex and costly model with respect to business continuity and disaster recovery.
- May reduce business insurance costs.

The Remote model has the following disadvantages:

- More complicated to administer than the Local or Campus models.
- Does not permit use of a virtual IP address as the single management address for the system, so it requires more device configuration (see “What If I Cannot Use Virtual IP Addressing?” in Related Topics).

- Usually provides lower bandwidth and higher latency than the other two models. This can affect HA reliability and may require administrative intervention to remedy (see “Network Throughput Restrictions on HA” in Related Topics).

Related Topics

- [Planning HA Deployments](#), on page 264
- [Network Throughput Restrictions on HA](#), on page 265
- [Using the Local Model](#), on page 266
- [Using the Campus Model](#), on page 267
- [What If I Cannot Use Virtual IP Addressing?](#), on page 268

What If I Cannot Use Virtual IP Addressing?

Depending on the deployment model you choose, not configuring a virtual IP address may result in the administrator having to perform additional steps in order to ensure that syslogs and SNMP notifications are forwarded to the secondary server in case of a failover. The usual method is to configure the devices to forward all syslogs and traps to both servers, usually via forwarding them to a given subnet or range of IP addresses that includes both the primary and secondary server.

This configuration work should be done at the same time HA is being set up: that is, after the secondary server is installed but before HA registration on the primary server. It must be completed before a failover so that the chance of losing data is eliminated or reduced. Not using a virtual IP address entails no change to the secondary server install procedure. The primary and secondary servers still need to be provisioned with their individual IP addresses, as normal.

This workaround is not available to you if you want to use HA with Operations Center. Enabling virtual IP addressing is a firm requirement in this case (see “Enable HA for Operations Center”).

Related Topics

- [Using Virtual IP Addressing With HA](#), on page 262
- [Planning HA Deployments](#), on page 264
- [Network Throughput Restrictions on HA](#), on page 265
- [Using the Campus Model](#), on page 267
- [Using the Remote Model](#), on page 267
- [Enable HA for Operations Center](#), on page 269

Automatic Versus Manual Failover

Configuring HA for automatic failover reduces the need for network administrators to manage HA. It also reduces the time taken to respond to the conditions that provoked the failover, since it brings up the secondary server automatically.

However, we recommend that the system be configured for Manual failover under most conditions. Following this recommendation ensures that Prime Infrastructure does not go into a state where it keeps failing over to the secondary server due to intermittent network outages. This scenario is most likely when deploying HA using the Remote model. This model is often especially susceptible to extreme variations in bandwidth and latency (see “Planning HA Deployments” and “Network Throughput Restrictions on HA” in Related Topics)

If the failover type is set to Automatic and the network connection goes down or the network link between the primary and secondary servers becomes unreachable, there is also a small possibility that both the primary and secondary servers will become active at the same time. We refer to this as the “split brain scenario”.

To prevent this, the primary server always checks to see if the secondary server is Active. As soon as the network connection or link is restored and the primary is able to reach the secondary again, the primary server checks the secondary server's state. If the secondary state is Active, then the primary server goes down on its own. Users can then trigger a normal, manual failback to the primary server.

Note that this scenario *only* occurs when the primary HA server is configured for Automatic failover. Configuring the primary server for Manual failover eliminates the possibility of this scenario. This is another reason why we recommend Manual failover configuration.

Automatic failover is especially ill-advised for larger enterprises. If a particular HA deployment chooses to go with Automatic failover anyway, an administrator may be forced to choose between the data that was newly added to the primary or to the secondary. This means, essentially, that there is a possibility of data loss whenever a split-brain scenario occurs. For help dealing with this issue, see “How to Recover From Split-Brain Scenario” in Related Topics.

To ensure that HA is managed correctly, Cisco recommends that Prime Infrastructure administrators always confirm the overall health of the HA deployment before initiating failover or failback, including:

- The current state of the primary.
- The current state of the secondary.
- The current state of connectivity between the two servers.

Related Topics

[Planning HA Deployments](#), on page 264

[Network Throughput Restrictions on HA](#), on page 265

[How to Trigger Failback](#), on page 285

[How to Recover From Split-Brain Scenario](#), on page 295

[Enable HA for Operations Center](#), on page 269

Enable HA for Operations Center

Operations Center is compatible with Prime Infrastructure’s High Availability (HA) framework. You can easily enable HA for Operations Center by setting up primary and secondary Operations Center servers, much as you do when implementing HA for normal Prime Infrastructure server instances that you manage using Operations Center.

No additional Operations Center license is required on the secondary server. HA for Operations Center supports both manual and automatic failover. In the event of a failover, when the secondary Operations Center server becomes active, all managed instances from the primary Operations Center server are automatically carried over to the secondary server. You can enable HA on your primary Operations Center server whether the primary is new or already running Operations Center.

Enabling HA for Operations Center is optional. However, if you choose to enable HA for Operations Center, you may also enable virtual IP addressing while HA registration on Operations Center. Use of virtual IP addressing also requires that the primary and secondary servers be on the same subnet.



Note The HA for Operations Center without virtual IP addressing works only for IP addressing and not for DNS names.

To set up HA for Operations Center using virtual IP, follow this workflow:

1. Determine the virtual IP address you will use for both servers. For details, see “Using Virtual IP Addressing With HA” and “Before You Begin Setting Up High Availability”, in Related Topics.
2. Install Prime Infrastructure on the server you plan to use as your primary Operations Center HA server.

If you already have a Prime Infrastructure server with Operations Center enabled, and wish to use it as your primary Operations Center server with HA: Remove Single Sign On (SSO) servers from the Operations Center instance and all the Prime Infrastructure instances managed by that Operations Center server. You can easily do this by selecting **Administration > Users > Users, Roles & AAA > SSO Servers** and then using the **Delete SSO Server(s)** command.

3. Install the secondary server and configure it for use with HA. For details, see “How to Install the HA Secondary Server” in Related Topics.
4. Register the secondary server on the primary, specifying that you want to Enable virtual IP and supplying the virtual IP address you selected. Logout from the Server and login back with the virtual IP. For details, see “How to Register HA on the Primary Server” in Related Topics.
5. If this is a new primary HA server: Apply the Operations Center license file to the primary server to transform it into an Operations Center instance. For details, see “Activate Your Operations Center License”.
6. Setup the virtual IP address as the SSO server on the primary server, specifying the virtual IP address as the IP address for the SSO server. For details, see “Enable SSO for Operations Center” in Related Topics.



Note By default the VIP TOFU is enabled in the primary server and no CA certificate is deployed in primary or secondary. After failover, delete the VIP TOFU from the PI instances and secondary server. After failback repeat the same from primary server. To remove TOFU for VIP from SSO (primary) client server:

```
ncs certvalidation tofu-certs deletecert host <vip>
```



Note Post the upgrade of Prime Infrastructure to 3.6, if you have a self-signed certificate before adding the Prime Infrastructure instance to SSO, you must remove the VIP from TOFU check.

7. Repeat the virtual IP SSO server setup on all instances of Prime Infrastructure that will be managed by the primary Operations Center server. Make sure you have deleted any old SSO configuration and launch PI server with its own IP.
8. Log out of all Prime Infrastructure instances and log back into the Operations Center instance, using the virtual IP address as the Operations Center server IP.
9. If this is a new primary HA server: Add Prime Infrastructure instances to the Operations Center server, as explained in “Add Cisco Prime Infrastructure Instances to Operations Center” in the Related Topics.

For more information, see "Activate Your Operations Center License" in Related Topics.

To set up HA for Operations Center without using virtual IP, follow this workflow:

1. Install Prime Infrastructure on the server you plan to use as your primary Operations Center HA server.
If you already have a Prime Infrastructure server with Operations Center enabled, and wish to use it as your primary Operations Center server with HA: Remove Single Sign On (SSO) servers from the Operations Center instance and all the Prime Infrastructure instances managed by that Operations Center server. You can easily do this by selecting **Administration > Users > Users, Roles & AAA > SSO Servers** and then using the **Delete SSO Server(s)** command.

2. Install the secondary server and configure it for use with HA. For details, see “How to Install the HA Secondary Server ” in Related Topics.
3. Register the secondary server on the primary.
4. If this is a new primary HA server: Apply the Operations Center license file to the primary server to transform it into an Operations Center instance. For details, see “Activate Your Operations Center License”.
5. Repeat the primary Server IP address setup on all instances of Prime Infrastructure that will be managed by the primary Operations Center server.
6. Log out of all Prime Infrastructure instances and log back into the Operations Center instance, using the Primary IP address as the Operations Center server IP.
7. If this is a new primary HA server: Add Prime Infrastructure instances to the Operations Center server, as explained in “Add Cisco Prime Infrastructure Instances to Operations Center” in the Related Topics.

For more information, see "Activate Your Operations Center License" in Related Topics.

Related Topics

- [Using Virtual IP Addressing With HA](#), on page 262
- [Before You Begin Setting Up High Availability](#), on page 272
- [How to Install the HA Secondary Server](#), on page 273
- [How to Register HA on the Primary Server](#), on page 273
- [Activate Your Operations Center License](#), on page 4
- [Add Instances to Operations Center](#), on page 6

Set Up High Availability

To use the HA capabilities in Prime Infrastructure, you must:

1. Ensure you have the information and settings you need to enable HA. For details, see “ Before You Begin Setting Up High Availability ” in Related Topics.
2. Install a second Prime Infrastructure server, and configure it to act as your secondary HA server. For details, see “ How to Install the HA Secondary Server ”.
3. Configure High Availability mode on the primary server, specifying the installed secondary server as the HA fallback server. For details, see “ How to Register HA on the Primary Server ”.

Related Topics

- [How High Availability Works](#), on page 257
- [Planning HA Deployments](#), on page 264
- [Enable HA for Operations Center](#), on page 269
- [Before You Begin Setting Up High Availability](#), on page 272
- [How to Install the HA Secondary Server](#), on page 273
- [How to Register HA on the Primary Server](#), on page 273
- [What Happens During HA Registration](#), on page 277
- [How to Patch Paired HA Servers Set for Manual Failover](#), on page 279
- [Monitor High Availability](#), on page 283
- [Access the Health Monitor Web Page](#), on page 284
- [High Availability Reference Information](#), on page 295

Before You Begin Setting Up High Availability

Before you begin, you will need:

- The Prime Infrastructure installation software. You will use this software to create the secondary HA server. The version of this software must match the version of Prime Infrastructure installed on your primary server. You can use the CLI **show version** command to verify the current version of the primary server software.
- If you have applied patches to your primary server, you must also patch the secondary server to the same level. Choose **Administration > Licenses and Software Updates > Software Update** to see a list of the patches applied to the primary server. Then, after setting up High Availability, follow the procedure in “How to Patch Paired High Availability Servers” to patch the secondary server to the same level as the primary server.
- A secondary server with hardware and software specifications that match or exceed the requirements for your primary server. For example: If your primary server was installed as a Prime Infrastructure Standard size OVA, your secondary server must also be installed as a Standard server, and must meet or exceed all requirements given for Standard size servers in the [Cisco Prime Infrastructure Quick Start Guide](#).
- The IP address or host name of the secondary server. You will need these when configuring HA on the primary server.
- If you plan to use virtual IP addressing: The virtual IPv4 and IPv6 IP address you want to use as the virtual IP for both HA servers. This is required only if you plan to use the virtual IP feature (see “Using Virtual IP Addressing with HA” in Related Topics). Note that virtual IP addressing requires that both HA servers are on the same subnet. You must use virtual IP addressing if you plan to use HA with Operations Center (see “Enable HA for Operations Center” in Related Topics)
- An authentication key of any length. It must contain at least three of the following types of characters: lowercase letters, uppercase letters, digits and special characters. You will enter this authentication key when you install the secondary server. The HA implementation uses this key to authenticate communications between the primary and secondary servers. Administrators also use the key to configure HA in the primary server, and to log on to the secondary server's Health Monitor page to monitor the HA implementation and troubleshoot problems with it.
- A Prime Infrastructure user ID with Administrator privileges on the primary server.
- A valid email address to which HA state-change notifications can be set. Prime Infrastructure will send email notifications for the following changes: HA registration, failure, failover, and failback.
- For acceptable results: Latency of 220 milliseconds or less, and net throughput of 86 Mbps or more, over the link between the primary and secondary servers. Failure to provide at least this link quality will interfere with data replication and may lead to HA failures. For advice on the range of acceptable performance requirements, see “Network Throughput Restrictions on HA”.
- If there is a firewall configured between the primary and the secondary servers, ensure that the firewall permits incoming and outgoing TCP/UDP on the following ports:
 - 8082: Used by the Health Monitor process to exchange heartbeat messages.
 - 1522: Used by Oracle to synchronize data.
 - 8085: Used by the Health Monitor process to check network bandwidth speed between Primary and Secondary servers when the user executes readiness test under High Availability.
- If you plan on using Operations Center with an HA implementation of Prime Infrastructure: Ensure that all of your HA-enabled Prime Infrastructure servers (both primary and secondary) have fully resolved host names.

For more information, see [Cisco Prime Infrastructure Quick Start Guide](#)

Related Topics

- [Set Up High Availability](#), on page 271
- [How to Patch Paired HA Servers Set for Manual Failover](#), on page 279
- [Using Virtual IP Addressing With HA](#), on page 262
- [Enable HA for Operations Center](#), on page 269
- [Network Throughput Restrictions on HA](#), on page 265

How to Install the HA Secondary Server

If your primary server has been patched, be sure to apply the same patches to your secondary server after installation and before registering HA on the primary server.

Make sure you have already decided on an authentication key, as explained in “Before You Begin Setting Up High Availability” in Related Topics.

-
- Step 1** Begin installing the Prime Infrastructure server software on your secondary server just as you would for a primary server. For instructions on installing the server, see the [Cisco Prime Infrastructure Quick Start Guide](#).
- Step 2** During the installation, you will be prompted as follows:
- Will this server be used as a secondary for HA? (yes/no)
- Enter **yes** at the prompt.
- Step 3** You will then be prompted for the HA authentication key, as follows:
- Enter Authentication Key:
- Enter the authentication key at the prompt. Enter it again at the confirmation prompt.
- Step 4** When the secondary server is installed:
- a) Use the CLI **show version** command on both servers, to verify that they are at the same version and patch level (see “Check Prime Infrastructure Version and Patch Status”).
 - b) Run the `ncs status` command to verify that all processes are up and running on the secondary server (see “Check Prime Infrastructure Server Status”).
 - c) Register HA on the primary server (see “How to Register HA on the Primary Server”).

Related Topics

- [Set Up High Availability](#), on page 271
- [Before You Begin Setting Up High Availability](#), on page 272
- [Check Prime Infrastructure Version and Patch Status](#), on page 112
- [Check Prime Infrastructure Server Status](#), on page 112
- [How to Register HA on the Primary Server](#), on page 273

How to Register HA on the Primary Server

To enable HA, you must register HA on the primary server. The primary server needs no configuration during installation in order to participate in the HA configuration. The primary needs to have only the following information:

- The IP address or host name of the secondary HA server you have already installed and configured (see “How to Install the HA Secondary Server” in Related Topics)
- The authentication key you set during installation of the secondary server.
- One or more email addresses, to which notifications will be sent.
- The Failover Type (see “Automatic Versus Manual Failover”).

If you plan to use virtual IP addressing (see “Using Virtual IP Addressing With HA”), you will also need to:

- Select the **Enable Virtual IP** checkbox.
- Specify the IPv4 virtual IP address to be shared by the primary and secondary HA servers. You may also specify an IPv6 virtual IP address, although this is not required.

The following steps explain how to register HA on the primary server. You follow these same steps when re-registering HA.

-
- Step 1** Log in to Prime Infrastructure with a user ID and password that has administrator privileges.
- Step 2** From the menu, select **Administration > Settings > High Availability**. Prime Infrastructure displays the HA status page.
- Step 3** Select **HA Configuration** and then complete the fields as follows:
- Secondary Server:** Enter the IP address or the host name of the secondary server.
 - Authentication Key:** Enter the authentication key password you set during the secondary server installation.
 - Email Address:** Enter the address (or comma-separated list of addresses) to which notification about HA state changes should be mailed. If you have already configured email notifications using the Mail Server Configuration page (see “Configure Email Server Settings”), the email addresses you enter here will be appended to the list of addresses already configured for the mail server.
 - Failover Type:** Select either **Manual** or **Automatic**. We recommend that you select **Manual**.
- Step 4** If you are using the virtual IP feature: Select the **Enable Virtual IP** checkbox, then complete the additional fields as follows:
- IPv4 Virtual IP:** Enter the virtual IPv4 address you want both HA servers to use.
 - IPv6 Virtual IP:** (Optional) Enter the IPv6 address you want both HA servers to use.
- Note that virtual IP addressing will **not** work unless both servers are on the same subnet.
- Step 5** Click **Check Readiness** to ensure if the HA related environmental parameters are ready for the configuration. For more details, see "Check Readiness for HA Registration/Configuration".
- Step 6** Click **Register** to save your changes. Prime Infrastructure initiates the HA registration process. When registration completes successfully, **Configuration Mode** will display the value **Primary Active**. For more information, see [Configure Email Server Settings](#) , on page 357.

Related Topics

- [How to Install the HA Secondary Server](#), on page 273
- [Automatic Versus Manual Failover](#), on page 268
- [Using Virtual IP Addressing With HA](#), on page 262
- [Before You Begin Setting Up High Availability](#), on page 272

[What Happens During HA Registration](#), on page 277

[Set Up High Availability](#), on page 271

[Check Readiness for HA Registration/Configuration](#), on page 275

Check Readiness for HA Registration/Configuration

During the HA registration, other environmental parameters related to HA like system specification, network configuration and bandwidth between the servers determine the HA configuration.

An approximate of 15 checks are run in the system to ensure the HA configuration completion without any error or failure. The checklist name and the corresponding status with recommendations if any, will be displayed when you run the Check Readiness feature.

To check readiness for HA configuration, follow these steps:

- Step 1** Log in to Prime Infrastructure with a user ID and password that has administrator privileges.
- Step 2** From the menu, select **Administration > Settings > High Availability**. Prime Infrastructure displays the HA status page.
- Step 3** Select **HA Configuration**.
- Step 4** Provide the secondary server IP address in the **Secondary Server** field and secondary Authentication Key **Authentication Key** field .
- Step 5** Click **Check Readiness**.

A pop up window with the system specifications and other parameters will be displayed. The screen will show the Checklist Item name, Status, Impact and Recommendation details.

Below, is the list of checklist test name and the description displayed for Check Readiness:

Table 14: Checklist name and description

Checklist Test Name	Test Description
SYSTEM - Check CPU Count	This validates the CPU count in primary and secondary server. The CPU count in primary server can be less than or equal to the secondary server.
DATABASE - LISTENER STATUS	This checks if the database listeners are up and running in both primary and secondary server. If there is a failure, the test will restart and report the status. This checks if all the wcs instances exist under oracle "listener.ora" file. This is executed in both primary and secondary server.
DATABASE - CHECK MEMORY TARGET	This checks for "/dev/shm" database memory target size for HA setup.
DATABASE - CHECK LISTENER CONFIG CORRUPTION	This checks for all the database instances exist under database listener configuration. This is executed in both primary and secondary server.

SYSTEM - HEALTH MONITOR STATUS	This checks whether the health monitor process is running in both primary and secondary server.
SYSTEM - CHECK DISK IOPS	This validates the disk IOPS in both primary and secondary server. The minimum expected disk IOPS is 200 MBps.
NETWORK - CHECK FIREWALL FOR DATABASE PORT ACCESSIBILITY	This checks if the database port 1522 is open in the system firewall. If the port is disabled, the test will grant permission for 1522 in the iptables list.
NETWORK - CHECK NETWORK INTERFACE BANDWIDTH	This checks if the eth0 interface speed matches the recommended speed of 100 Mbps in both primary and secondary sever. This test will not measure network bandwidth by transmitting data between primary and secondary server.
NETWORK - CHECK NETWORK BANDWIDTH SPEED	This checks if the network bandwidth speed matches the recommended speed of 100 Mbps in both primary and secondary sever. This test will measure network bandwidth by transmitting data between primary and secondary server.
DATABASE - CHECK ONLINE STATUS	This checks if the database files status is online and accessible in both primary and secondary server.
DATABASE - CHECK TNS CONFIG CORRUPTION	This validates if the tnsping is successful in both primary and secondary server.
DATABASE - TNS REACHABILITY STATUS	This checks if all the wcs instances exist under oracle "listener.ora" file. This is executable in both primary and secondary server.
DATABASE - VALIDATE STANDBY DATABASE INSTANCE	This validates if the standby database instance (stbywcs) is available in both primary and secondary server.
SYSTEM - CHECK RAM SIZE	This checks if the disk size of primary server less than or equal to secondary server.
SYSTEM - CHECK SERVER PING REACHABILITY	This ensures that the primary server can run ping check with the remote (secondary) server.

Step 6 Once the check is completed for all the parameters, check their status and click **Clear** to close the window.

Note The validation failback and failover events during Check Readiness will be sent to the Alarms and Events page; whereas, the registration failure event will not be present in the Alarms and Evens page.

Check High Availability Status

You can check on the status of the High Availability enabled on a Prime Infrastructure server.

- Step 1** Open a CLI session with the Prime Infrastructure server (see [How to Connect Via CLI](#), on page 111).
- Step 2** Enter the following command to display the current status of Prime Infrastructure HA processes:
 PIServer/admin# **ncs ha status**

Related Topics

[Set Up High Availability](#), on page 271

What Happens During HA Registration

Once you finish entering configuration information and click the Save button on the HA Configuration page, the primary and secondary HA servers will register with each other and begin copying all database and configuration data from the primary to the secondary server.

The time required to complete the copying is a function of the amount of database and configuration data being replicated and the available bandwidth on the network link between the two servers. The bigger the data and the slower the link, the longer the replication will take. For a relatively fresh server (in operation for a few days), with 100 devices and a 1 GB-per-second link, copying will take approximately 25 minutes.

During HA registration, the primary and secondary server state will go through the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: HA Not Configured	From: HA Not Configured
To: HA Initializing	To: HA Initializing
To: Primary Active	To: Secondary Syncing

You can view these state changes on the HA Status page for the primary server, or the Health Monitor web pages for either of the two servers. If you are using the HA Status page, click **Refresh** to view progress. Once the data is fully synchronized, the HA Status page will be updated to show the current state as “Primary Active”, as shown in the following figure.

The screenshot shows the 'HA Status' page in the Cisco Prime Infrastructure web interface. The page is divided into several sections:

- Current Configuration:** Shows 'Secondary Server' as 172.20.116.163 and 'Failover Type' as 'Manual'.
- Status:** Shows 'Current State Mode' as 'Primary Active'.
- Events:** A table listing recent events:

Time	State	Description
Jun 15, 2015 06:55:18 AM	Primary Active	Failed to send email notification: Notification Email Address is not configured.
Jun 15, 2015 06:55:18 AM	Primary Active	Completed failback from Secondary Prime Infrastructure 172.20.116.163 [172.20.116.163]
Jun 15, 2015 06:54:04 AM	Primary Failback	Starting to failback from secondary Prime Infrastructure 172.20.116.163 [172.20.116.163]
Jun 15, 2015 06:53:19 AM	Primary Syncing	Primary Prime Infrastructure Server started successfully as standby
Jun 15, 2015 06:53:19 AM	Primary Syncing	Prime Infrastructure started successfully. Prime Infrastructure server state : Primary Syncing
Jun 15, 2015 06:34:47 AM	Health Monitor Available	Health Monitor Started
Jun 15, 2015 06:34:45 AM	Health Monitor Available	Health Monitor Started

After registration is initiated, Prime Infrastructure initiates synchronization between the primary and the secondary HA servers. The synchronization should not have any impact on user activity, although users may observe slow system response until the synchronization is complete. The length of the synchronization is a function of the total database size and, is handled at the Oracle database level by the Oracle RMAN and Data Guard Broker processes. There is no impact on the execution of user- or system-related activity during the sync.

During registration, Prime Infrastructure performs a full database replication to the secondary server. All processes on the secondary server will be running, but the server itself will be in passive mode. If you execute the Prime Infrastructure CLI command **ncs status** on the secondary server while the secondary server is in the “Secondary Syncing” state, the command output will show all processes as running.

Related Topics

[How High Availability Works](#), on page 257

[Planning HA Deployments](#), on page 264

[Set Up High Availability](#), on page 271

How to Patch HA Servers

You can download and install UBF patches for your HA servers in one of the following ways, depending on your circumstances:

- Install the patch on HA servers that are not currently paired. Cisco recommends this method if you have not already set up HA for Prime Infrastructure.
- Install the patch on existing paired HA servers using manual failover. This is the method Cisco recommends if you already have HA set up.
- Install the patch on existing paired HA servers using automatic failover.

For details on each method, see the Related Topics.

Related Topics

[How to Patch New HA Servers](#), on page 278

[How to Patch Paired HA Servers Set for Manual Failover](#), on page 279

[How to Patch Paired HA Servers Set for Automatic Failover](#), on page 281

How to Patch New HA Servers

If you are setting up a new Prime Infrastructure High Availability (HA) implementation and your new servers are not at the same patch level, follow the steps below to install patches on both servers and bring them to the same patch level.

Step 1

Download the patch and install it on the primary server:

- a) Point your browser to the software patches listing for Cisco Prime Infrastructure (see Related Topics).
- b) Click the **Download** button for the patch file you need to install (the file name ends with a UBF file extension), and save the file locally.
- c) Log in to the primary server using an ID with administrator privileges and choose **Administration > Licenses and Software Updates > Software Update**.
- d) Click the **Upload** link at the top of the page and browse to the location where you saved the patch file.
- e) Select the UBF file and click **OK** to upload the file.

- f) When the upload is complete: On the Software Upload page, verify that the Name, Published Date and Description of the patch file are correct.
- g) Select the patch file and click **Install**.
- h) Click **Yes** in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.
- i) After the installation is complete on the primary server, verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

Step 2 Install the same patch on the secondary server:

- a) Access the secondary server’s Health Monitor (HM) web page by pointing your browser to the following URL:
https://ServerIP:8082
where *ServerIP* is the IP address or host name of the secondary server.
- b) You will be prompted for the secondary server authentication key. Enter it and click **Login**.
- c) Click the HM web page’s **Software Update** link. You will be prompted for the authentication key a second time. Enter it and click **Login** again.
- d) Click **Upload Update File** and browse to the location where you saved the patch file.
- e) Select the UBF file and click **OK** to upload the file.
- f) When the upload is complete: On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.
- g) Select the patch file and click **Install**.
- h) Click **Yes** in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.
- i) After the installation is complete on the secondary server, verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

Step 3 Verify that the patch status is the same on both servers, as follows:

- a) Log in to the primary server and access its Software Update page as you did in step 1, above. The “Status” column should show “Installed” for the installed patch.
- b) Access the secondary server’s Health Monitor page as you did in step 2, above. The “Status” column should show “Installed” for the installed patch

Step 4 Register the servers.

For more information, see "[Software patches listing for Cisco Prime Infrastructure](#)", "[Restart Prime Infrastructure Using CLI](#)" and "[Check Prime Infrastructure Server Status](#)".

Related Topics

- [Set Up High Availability](#), on page 271
- [How to Register HA on the Primary Server](#), on page 273
- [How to Patch HA Servers](#), on page 278

How to Patch Paired HA Servers Set for Manual Failover

If your current Prime Infrastructure implementation has High Availability servers that are not at the same patch level, or you have a new patch you must install on both your HA servers, follow the steps below.

You must start the patch install with the primary server in “Primary Active” state and the secondary server in “Secondary Syncing” state.

Patching of primary and secondary HA servers set for manual failover takes approximately 30 minutes, and does not require failover or failback. Patching of the primary and secondary HA servers takes approximately 30 minutes. Downtime during the primary patch installation restart takes 15 to 20 minutes.

In some cases, you may receive a popup error message indicating that you cannot perform an update on Prime Infrastructure servers while HA is configured. If so, you *must* first disconnect the primary and secondary servers before attempting to apply the patch. In this case, you cannot use the steps in this procedure. Instead, be sure to:

1. Follow the steps in “Remove HA Via the GUI” (see Related Topics) to disconnect the primary and secondary servers.
2. Follow the steps in “How to Patch New HA Servers” to apply the patch.
3. Follow the steps in “Set Up High Availability” to restore your HA configuration.

Step 1 Ensure that your HA implementation is enabled and ready for update:

- a) Log in to the primary server using an ID with Administrator privileges.
- b) Select **Administration > Settings > High Availability**. The primary server state displayed on the HA Status page should be “Primary Active”.
- c) Select **HA Configuration**. The current Configuration Mode should show “HA Enabled”. We recommend that you set the Failover Type to “manual” during the patch installation.
- d) Access the secondary server’s Health Monitor (HM) web page by pointing your browser to the following URL:

https://ServerIP:8082

where *ServerIP* is the IP address or host name of the secondary server.

- e) Verify that the secondary server state displayed on the HM web page is in the “Secondary Syncing” state.

Step 2 You will be prompted for the authentication key entered when HA was enabled. Enter it and click **Login**.

Step 3 Download the UBF patch and install it on the primary server:

- a) Point your browser to the software patches listing for Cisco Prime Infrastructure (see Related Topics) .
- b) Click the **Download** button for the patch file you need to install (the file name ends with a UBF file extension), and save the file locally.
- c) Log in to the primary server using an ID with administrator privileges and choose **Administration > Licenses and Software Updates > Software Update**.
- d) Click the **Upload** link at the top of the page and browse to the location where you saved the patch file.
- e) Select the UBF file and click **OK** to upload the file.
- f) When the upload is complete: On the Software Upload page, verify that the Name, Published Date and Description of the patch file are correct.
- g) Select the patch file and click **Install**.
- h) Click **Yes** in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.
- i) After the server restart is complete on the primary server, select **Administration > Settings > High Availability**. The primary server state displayed on the HA Status page should be “Primary Active”.
- j) Verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

Step 4 Install the same patch on the secondary server once patching is complete on the primary server:

- a) Access the secondary server’s HM web page and login if needed.
- b) Click the HM web page’s **Software Update** link. You will be prompted for the authentication key a second time. Enter it and click **Login** again.
- c) Click **Upload Update File** and browse to the location where you saved the patch file.

- d) Select the UBF file and click **OK** to upload the file.
- e) When the upload is complete: On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.
- f) Select the patch file and click **Install**.
- g) Click **Yes** in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.
- h) After the server restart is complete on the secondary server, log in to the secondary HM page (<https://serverIP:8082>) and verify that the secondary server state displayed on the HM web page is “Secondary Syncing”.
- i) Verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

Step 5

Once the server restart is complete, verify the patch installation as follows:

- a) Log in to the primary server and access its Software Update page as you did in step 2, above. The “Status” column on the Status of Updates > Update tab should show “Installed” for the patch.
- b) Access the secondary server’s Software Update page as you did in step 3, above. The “Status” column on the Status of Updates > Updates tab should show “Installed” for the patch.

For more information, see

- [Software patches listing for Cisco Prime Infrastructure](#).
- [Start Prime Infrastructure, on page 111](#)
- [Stop Prime Infrastructure, on page 113](#)
- [Check Prime Infrastructure Server Status, on page 112](#)

Related Topics

[Set Up High Availability](#), on page 271

[Check High Availability Status](#), on page 277

[Remove HA Via the GUI](#), on page 299

[How to Patch New HA Servers](#), on page 278

[How to Patch Paired HA Servers Set for Automatic Failover](#), on page 281

How to Patch Paired HA Servers Set for Automatic Failover

If your current Prime Infrastructure implementation has High Availability servers that are not at the same patch level, or you have a new patch you must install on both your HA servers, follow the steps below.

You must start the patch install with the primary server in “Primary Active” state and the secondary server in “Secondary Syncing” state.

Patching of primary and secondary HA servers set for automatic failover takes approximately one hour, and requires both failover and failback. Downtime during the failover and failback lasts 10 to 15 minutes.

In some cases, you may receive a popup error message indicating that you cannot perform an update on Prime Infrastructure servers while HA is configured. If so, you *must* first disconnect the primary and secondary servers before attempting to apply the patch. In this case, you cannot use the steps in this procedure. Instead, be sure to:

1. Follow the steps in “Remove HA Via the GUI” (see Related Topics) to disconnect the primary and secondary servers.
2. Follow the steps in “How to Patch New HA Servers” (see Related Topics) to apply the patch.

3. Follow the steps in “Set Up High Availability” (see Related Topics) to restore your HA configuration.

-
- Step 1** Ensure that your HA implementation is enabled and ready for update:
- a) Log in to the primary server using an ID with Administrator privileges.
 - b) Select **Administration > Settings > High Availability**. The primary server state displayed on the HA Status page should be “Primary Active”.
 - c) Select **HA Configuration**. The current Configuration Mode should show “HA Enabled”.
 - d) Access the secondary server’s Health Monitor (HM) web page by pointing your browser to the following URL:
https://ServerIP:8082
 where *ServerIP* is the IP address or host name of the secondary server.
 - e) You will be prompted for the authentication key entered when HA was enabled. Enter it and click **Login**.
 - f) Verify that the secondary server state displayed on the HM web page is in the “Secondary Syncing” state.
- Step 2** Download the UBF patch and install it on the primary server:
- a) Point your browser to the software patches listing for Cisco Prime Infrastructure (see Related Topics) .
 - b) Click the **Download** button for the patch file you need to install (the file name ends with a UBF file extension), and save the file locally.
 - c) Log in to the primary server using an ID with administrator privileges and choose **Administration > Licenses and Software Updates > Software Update**.
 - d) Click the **upload** link at the top of the page and browse to the location where you saved the patch file.
 - e) Select the UBF file and then click **OK** to upload the file.
 - f) When the upload is complete: On the Software Upload page, verify that the Name, Published Date and Description of the patch file are correct.
 - g) Select the patch file and click **Install**.
 - h) Click **Yes** in the warning pop-up. Failover will be triggered and the primary server will restart automatically. Failover will take 2 to 4 minutes to complete. After the failover is complete, the secondary server will be in “Secondary Active” state.
 - i) After the primary server is restarted, run the **ncs status** command (see “Check Prime Infrastructure Server Status”) to verify that the primary’s processes have re-started. Before continuing: Access the primary server’s HM web page and verify that the primary server state displayed is “Primary Syncing”.
- Step 3** Failback to the primary using the secondary server’s HM web page:
- a) Access the secondary server’s HM web page and login if needed.
 - b) Click **Failback** to initiate a failback from the secondary to the primary server. It will take 2 to 3 minutes for the operation to complete. As soon as failback completes, the secondary server will be automatically restarted in the standby mode. It will take a maximum of 15 minutes for the restart to complete, and it will be synched with the primary server.
 You can verify the restart by logging into the secondary server’s HM web page and looking for the message “Prime Infrastructure stopped successfully” followed by “Prime Infrastructure started successfully.”
 After failback is complete, the primary server state will change to “Primary Active”
 - c) Before continuing: Run the **ncs ha status** command on both the primary and secondary servers. Verify that the primary server state changes to “Primary Active” and the secondary server state is “Secondary Syncing”.
- Step 4** Once failback completes, verify the patch installation by logging in to the primary server and accessing its Software Update page (as you did in step 2, above). The “Status” column on the Status of Updates > Update tab should show “Installed” for the patch.

- Step 5** Install the same patch on the secondary server once patching is complete on the primary server:
- Access the secondary server's HM web page and login if needed.
 - Click the HM web page's **Software Update** link. You will be prompted for the authentication key a second time. Enter it and click **Login** again.
 - Click **Upload Update File** and browse to the location where you saved the patch file.
 - Select the UBF file and then click **OK** to upload the file.
 - When the upload is complete: On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.
 - Select the patch file and click **Install**.
 - Click **Yes** in the warning pop-up. The server will restart automatically. The restart typically takes 15 to 20 minutes.
 - After the installation is complete on the secondary server, verify that the Status of Updates table on the Software Update page shows "Installed" for the patch.
 - After the server restart is complete on the secondary server, log in to the secondary HM page and verify that the secondary server state displayed on the HM web page is "Secondary Syncing".
- Step 6** Once server restart is complete, verify the patch installation as follows:
- Log in to the primary server and access its Software Update page as you did in step 2, above. The "Status" column on the Status of Updates > Update tab should show "Installed" for the patch.
 - Access the secondary server's Software Update page as you did in step 5, above. The "Status" column on the Status of Updates > Updates tab should show "Installed" for the patch.

For more information, see [Software patches listing for Cisco Prime Infrastructure](#), [Stop Prime Infrastructure](#), [Start Prime Infrastructure](#) and [Check Prime Infrastructure Server Status](#).

Related Topics

- [Set Up High Availability](#), on page 271
- [Check High Availability Status](#), on page 277
- [Remove HA Via the GUI](#), on page 299
- [How to Patch New HA Servers](#), on page 278
- [How to Patch Paired HA Servers Set for Manual Failover](#), on page 279

Monitor High Availability

Once you have configured HA and registered it on the primary server, most of your interactions with HA will involve accessing the server Health Monitor web page and responding to email notifications by triggering a failover or failback. These processes, as well as special situations requiring more complicated responses, are covered in the following related topics.

Related Topics

- [Access the Health Monitor Web Page](#), on page 284
- [How to Trigger Failover](#), on page 284
- [How to Trigger Failback](#), on page 285
- [Force Failover](#), on page 285
- [Respond to Other HA Events](#), on page 286

Access the Health Monitor Web Page

You can access the Health Monitor web page for the primary or secondary server at any time by pointing your browser to the following URL:

`https://Server:8082`

where **Server** is the IP address or host name of the primary or secondary server whose Health Monitor web page you want to see.

You can also access the Health Monitor web page for the currently active server by logging in to Prime Infrastructure, selecting **Administration > Settings > High Availability**, and then clicking the **Launch Health Monitor** link at the top right of the HA Status page.

Related Topics

[Monitor High Availability](#), on page 283

[How to Trigger Failover](#), on page 284

[How to Trigger Failback](#), on page 285

[Force Failover](#), on page 285

How to Trigger Failover

Failover is the process of activating the secondary server in response to a detected failure on the primary.

Health Monitor (HM) detects failure conditions using the heartbeat messages that the two servers exchange. If the primary server is not responsive to three consecutive heartbeat messages from the secondary, it is considered to have failed. During the health check, HM also checks the application process status and database health; if there is no proper response to these checks, these are also treated as having failed.

The HA system takes approximately 10 to 15 seconds to detect a process failure on the primary server and initiate a failover. If the secondary server is unable to reach the primary server due to a network issue, it might take more time to initiate a failover. In addition, it may take additional time for the application processes on the secondary server to be fully operational.

As soon as HM detects the failure, it sends an email notification. The email includes the failure status along with a link to the secondary server's Health Monitor web page.

If HA is currently configured for automatic failover, the secondary server will activate automatically and there is no action you need to perform.

If HA is currently configured for manual failover, you must trigger the failover as follows:

-
- Step 1** Access the secondary server's Health Monitor web page using the web link given in the email notification, or using the steps in "Accessing the Health Monitor Web Page".
- Step 2** Trigger the failover by clicking the **Failover** button.
-

Related Topics

[How High Availability Works](#), on page 257

[How to Trigger Failback](#), on page 285

[Monitor High Availability](#), on page 283

[How to Register HA on the Primary Server](#), on page 273

[Access the Health Monitor Web Page](#), on page 284

How to Trigger Failback

Failback is the process of re-activating the primary server once it is back online. It also transfers Active status from the secondary server to the primary, and stops active network monitoring processes on the secondary.

During failback, the secondary server is available except during the period when processes are re-started on the secondary. Both servers' Health Monitor web pages are accessible for monitoring the progress of the failback. Additionally, users can also connect to the secondary server to access all normal functionality, except for these caveats:

- Do not initiate configuration or provisioning activity while the failback is in progress.
- Be aware that, after a successful failback, the secondary server will go into passive ("Secondary Syncing") mode and control will switch over to the primary server. During this process, Prime Infrastructure will be inaccessible to the users for a few moments.

You must always trigger failback manually, as follows:

Step 1 Access the secondary server's Health Monitor web page using the link given in the email notification, or using the steps in "Accessing the Health Monitor Web Page".

Step 2 Trigger the failback by clicking the **Failback** button.

The secondary server is automatically restarted in the standby mode after the failback and is automatically synced with the primary server. The primary server will now be the available Prime Infrastructure server.

Related Topics

[How High Availability Works](#), on page 257

[How to Trigger Failover](#), on page 284

[Force Failover](#), on page 285

[Monitor High Availability](#), on page 283

[Access the Health Monitor Web Page](#), on page 284

Force Failover

A forced failover is the process of making the secondary server active while the primary server is still up. You will want to use this option when, for example, you want to test that your HA setup is fully functional.

Forced failover is available to you only when the primary is active, the secondary is in the "Secondary syncing" state, and all processes are running on both servers. Forced failover is disabled when the primary server is down. In this case, only the normal Failover is enabled.

Once the forced failover completes, the secondary server will be active and the primary will restart in standby automatically. You can return to an active primary server and standby secondary server by triggering a normal failback.

Step 1 Access the secondary server's Health Monitor web page using the steps in "Accessing the Health Monitor Web Page".

Step 2 Trigger the forced failover by clicking the **Force Failover** button. The forced failover will complete in 2 to 3 minutes.

Related Topics

- [How High Availability Works](#), on page 257
- [How to Trigger Failover](#), on page 284
- [How to Trigger Failback](#), on page 285
- [Monitor High Availability](#), on page 283
- [How to Register HA on the Primary Server](#), on page 273
- [Access the Health Monitor Web Page](#), on page 284

Respond to Other HA Events

All the HA related events are displayed on the HA Status page, the Health Monitor web pages, and under the Prime Infrastructure Alarms and Events page. Most events require no response from you other than triggering failover and failback. A few events are more complex, as explained in the related topics.

Related Topics

- [HA Registration Fails](#), on page 286
- [Network is Down \(Automatic Failover\)](#), on page 287
- [Network is Down \(Manual Failover\)](#), on page 288
- [Process Restart Fails \(Manual Failover\)](#), on page 290
- [Primary Server Restarts During Sync \(Manual Failover\)](#), on page 291
- [Secondary Server Restarts During Sync](#), on page 291
- [Both HA Servers Are Down](#), on page 292
- [Both HA Servers Are Down and the Secondary Will Not Restart](#), on page 293
- [Replace Primary MSEs](#), on page 319
- [How to Recover From Split-Brain Scenario](#), on page 295

HA Registration Fails

If HA registration fails, you will see the following HA state-change transitions for each server (instead of those detailed in “What Happens During HA Registration”):

Primary HA State Transitions...	Secondary HA State Transitions...
From: HA Initializing	From: HA Initializing
To: HA Not Configured	To: HA Not Configured

To recover from failed HA registration, follow the steps below.

-
- Step 1** Use ping and other tools to check the network connection between the two Prime Infrastructure servers. Confirm that the secondary server is reachable from the primary, and vice versa.
 - Step 2** Check that the gateway, subnet mask, virtual IP address (if configured), server hostname, DNS, NTP settings are all correct.
 - Step 3** Check that the configured DNS and NTP servers are reachable from the primary and secondary servers, and that both are responding without latency or other network-specific issues.
 - Step 4** Check that all Prime Infrastructure licenses are correctly configured.

- Step 5** Once you have remedied any connectivity or setting issues, try the steps in “How to Register High Availability on the Primary Server” again in related topics.

Related Topics

- [Respond to Other HA Events](#), on page 286
- [What Happens During HA Registration](#), on page 277
- [How to Register HA on the Primary Server](#), on page 273

Network is Down (Automatic Failover)

If there is a loss of network connectivity between the two Prime Infrastructure servers, you will see the following HA state-change transitions for each server, assuming that the Failover Type is set to “Automatic”:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Lost Secondary	To: Secondary Lost Primary
To: Primary Lost Secondary	To: Secondary Failover
To: Primary Lost Secondary	To: Secondary Active

You will get an email notification that the secondary is active.

-
- Step 1** Check on and restore network connectivity between the two servers. Once network connectivity is restored and the primary server can detect that the secondary is active, all services on the primary will be restarted and made passive automatically. You will see the following state changes:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Lost Secondary	From: Secondary Active
To: Primary Failover	To: Secondary Active
To: Primary Syncing	To: Secondary Active

- Step 2** Trigger a failback from the secondary to the primary. You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Syncing	From: Secondary Active
To: Primary Failback	To: Secondary Failback
To: Primary Failback	To: Secondary Post Failback
To: Primary Active	To: Secondary Syncing

Related Topics

[Respond to Other HA Events](#), on page 286

[How to Trigger Failback](#), on page 285

Network is Down (Manual Failover)

If there is a loss of network connectivity between the two Prime Infrastructure servers, you will see the following HA state-change transitions for each server, assuming that the Failover Type is set to “Manual”:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Lost Secondary	To: Secondary Lost Primary

You will get email notifications that each server has lost the other.

Step 1 Check on and, if needed, restore the network connectivity between the two servers.

You will see the following state changes once network connectivity is restored.:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Lost Secondary	From: Secondary Lost Primary
To: Primary Active	To: Secondary Syncing

No administrator response is required.

Step 2 If network connection cannot be restored for any reason, use the HM web page for the secondary server to trigger a failover from the primary to the secondary server. You will see the following state changes:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Lost Secondary	From: Secondary Lost Primary
To: Primary Lost Secondary	To: Secondary Failover
To: Primary Failover	To: Secondary Active

You will get an email notification that the secondary server is now active.

Step 3 Check and restore network connectivity between the two servers. Once network connectivity is restored and the primary server detects that the secondary server is active, all services on the primary server will be restarted and made passive. You will see the following state changes:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Lost Secondary	From: Secondary Active
To: Primary Failover	To: Secondary Active
To: Primary Syncing	To: Secondary Active

Step 4 Trigger a failback from the secondary to the primary.

You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Syncing	From: Secondary Active
To: Primary Failback	To: Secondary Failback
To: Primary Failback	To: Secondary Post Failback
To: Primary Active	To: Secondary Syncing

Related Topics

[Respond to Other HA Events](#), on page 286

[How to Trigger Failback](#), on page 285

Process Restart Fails (Automatic Failover)

The Prime Infrastructure Health Monitor process is responsible for attempting to restart any Prime Infrastructure server processes that have failed. Generally speaking, the current state of the primary and secondary servers should be “Primary Active” and “Secondary Syncing” at the time any such failures occur.

If HM cannot restart a critical process on the primary server, then the primary server is considered to have failed. If your currently configured Failover Type is “automatic”, you will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Uncertain	To: Secondary Lost Primary
To: Primary Failover	To: Secondary Failover
To: Primary Failover	To: Secondary Active

When this process is complete, you will get an email notification that the secondary server is now active.

Step 1 Restart the primary server and ensure that it is running. Once the primary is restarted, it will be in the state “Primary Syncing”. You will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Failover	From: Secondary Active
To: Primary Preparing for Failback	To: Secondary Active
To: Primary Syncing	To: Secondary Active

Step 2 Trigger a failback from the secondary to the primary. You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Syncing	From: Secondary Active
To: Primary Failback	To: Secondary Failback
To: Primary Failback	To: Secondary Post Failback
To: Primary Active	To: Secondary Syncing

Related Topics

[Respond to Other HA Events](#), on page 286

[How to Trigger Failback](#), on page 285

Process Restart Fails (Manual Failover)

The Prime Infrastructure Health Monitor process is responsible for attempting to restart any Prime Infrastructure server processes that have failed. Generally speaking, the current state of the primary and secondary servers should be “Primary Active” and “Secondary Syncing” at the time any such failures occur. If HM cannot restart a critical process on the primary server, then the primary server is considered to have failed. You will receive an email notification of this failure. If your currently configured Failover Type is “Manual”, you will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Uncertain	To: Secondary Lost Primary

Step 1 Trigger on the secondary server a failover from the primary to the secondary. You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Uncertain	From: Secondary Syncing
To: Primary Failover	To: Secondary Failover
To: Primary Failover	To: Secondary Active

Step 2 Restart the primary server and ensure that it is running. Once the primary server is restarted, the primary’s HA state will be “Primary Syncing”. You will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Failover	From: Secondary Active
To: Primary Preparing for Failback	To: Secondary Active
To: Primary Syncing	To: Secondary Active

Step 3 Trigger a failback from the secondary to the primary. You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Syncing	From: Secondary Active
To: Primary Failback	To: Secondary Failback
To: Primary Failback	To: Secondary Post Failback
To: Primary Active	To: Secondary Syncing

Related Topics

[Respond to Other HA Events](#), on page 286

[How to Trigger Failover](#), on page 284

[How to Trigger Failback](#), on page 285

Primary Server Restarts During Sync (Manual Failover)

If the primary Prime Infrastructure server is restarted while the secondary server is syncing, you will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Alone	To: Secondary Lost Primary
To: Primary Active	To: Secondary Syncing

The “Primary Alone” and “Primary Active” states occur immediately after the primary comes back online. No administrator response should be required.

Related Topics

[Respond to Other HA Events](#), on page 286

Secondary Server Restarts During Sync

If the secondary Prime Infrastructure server is restarted while syncing with the primary server, you will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Lost Secondary	From: Secondary Lost Primary
To: Primary Active	To: Secondary Syncing

No administrator response should be required.

Related Topics

[Respond to Other HA Events](#), on page 286

Both HA Servers Are Down

If both the primary and secondary servers are down at the same time, you can recover by bringing them back up in the correct order, as explained in the steps below.

-
- Step 1** Restart the secondary server and the instance of Prime Infrastructure running on it. If for some reason you cannot restart the secondary server, see “Both HA Servers Are Down and Secondary Will Not Restart” in Related Topics.
- Step 2** When Prime Infrastructure is running on the secondary, access the secondary server’s Health Monitor web page. You will see the secondary server transition to the state “Secondary Lost Primary”.
- Step 3** Restart the primary server and the instance of Prime Infrastructure running on it. When Prime Infrastructure is running on the primary, the primary will automatically sync with the secondary. To verify this, access the primary server’s Health Monitor web page. You will see the two servers transition through the following series of HA states:

Primary HA State Transitions...	Secondary HA State Transitions...
To: Primary Lost Secondary	To: Secondary Lost Primary
To: Primary Active	To: Secondary Syncing

Related Topics

[Both HA Servers Are Down and the Secondary Will Not Restart](#), on page 293

[Access the Health Monitor Web Page](#), on page 284

[Respond to Other HA Events](#), on page 286

Both HA Servers Are Powered Down

If both the primary and secondary servers are powered down at the same time, you can recover by bringing them back up in the correct order, as explained in the steps below.

-
- Step 1** Power on the secondary server and the instance of Prime Infrastructure running on it.
- The secondary HA restart will fail at this stage because the primary is not reachable. However, the secondary Health Monitor process will be running with an error.
- Step 2** When Prime Infrastructure is running on the secondary, access the secondary server’s Health Monitor web page. You will see the secondary server transition to the state “Secondary Lost Primary”.
- Step 3** Power on the primary server and the instance of Prime Infrastructure running on it.
- Step 4** When Prime Infrastructure is running on the primary, the primary will automatically sync with the secondary. To verify this, access the primary server’s Health Monitor web page. You will see the two servers transition through the following series of HA states:

Primary HA State Transitions...	Secondary HA State Transitions...
To: Primary Lost Secondary	To: Secondary Lost Primary

Primary HA State Transitions...	Secondary HA State Transitions...
To: Primary Active	To: Secondary Syncing

- Step 5** Restart the secondary server and the instance of Prime Infrastructure running on it. This is required because not all processes will be running on the secondary at this point.
- If for some reason you cannot restart the secondary server, see “Both HA Servers Are Down and Secondary Will Not Restart” in Related Topics.
- Step 6** When Prime Infrastructure finishes restarting on the secondary server, all processes should be running. Verify this by running the `ncs status` command (see “Check Prime Infrastructure Server Status” in Related Topics).

Related Topics

- [Both HA Servers Are Down and the Secondary Will Not Restart](#), on page 293
- [Access the Health Monitor Web Page](#), on page 284
- [Respond to Other HA Events](#), on page 286
- [Check Prime Infrastructure Server Status](#), on page 112

Both HA Servers Are Down and the Secondary Will Not Restart

If both HA servers are down at the same time and the secondary will not restart, you will need to remove the HA configuration from the primary server in order to use it as a standalone until you can replace or restore the secondary server.

The following steps assume that you have already tried and failed to restart the secondary server.

-
- Step 1** Attempt to restart the primary instance of Prime Infrastructure. If the primary is able to restart at all, the restart will abort with an error message indicating that you must remove the HA configuration.
- Step 2** Open a CLI session with the primary Prime Infrastructure server (see [How to Connect Via CLI](#), on page 111).
- Step 3** Enter the following command to remove the HA configuration on the primary server:
- ```
PIServer/admin# ncs ha remove
```
- Step 4** You will be prompted to confirm that you want to remove the HA configuration. Answer **Y** to the prompt.
- You should now be able to restart the primary instance of Prime Infrastructure without the error message and use it as a standalone.
- When you are able to restore or replace the secondary server, proceed as explained in “How to Register High Availability on the Primary Server” in Related Topics.

---

#### Related Topics

- [Access the Health Monitor Web Page](#), on page 284
- [How to Register HA on the Primary Server](#), on page 273
- [Remove HA Via the CLI](#), on page 300
- [Respond to Other HA Events](#), on page 286

## How to Replace the Primary Server

Under normal circumstances, the state of your primary and secondary servers will be “Primary Active” and “Secondary Syncing”, respectively. If the primary server fails for any reason, a failover to the secondary will take place, either automatically or manually.

You may find that restoring full HA access requires you to reinstall the primary server using new hardware. If this happens, you can follow the steps below to bring up the new primary server without data loss.

- 
- Step 1** Ensure that the secondary server is currently in “Secondary Active” state. If you have set the Failover Type on the primary server to “manual”, you will need to trigger the failover to the secondary manually.
- Step 2** Ensure that the old primary server you are replacing has been disconnected from the network.
- Step 3** Ensure that the new primary server is ready for use. This will include connecting it to the network and assigning it the same server IP, subnet mask, gateway as the old primary server. You will also need to enter the same authentication key that you entered when installing the secondary server.
- Step 4** Ensure that both the primary and secondary servers are at the same patch level and if you want to replace the primary server, then you must :
- Ensure the primary and secondary server are in TOFU Mode.
  - Login to Secondary server admin CLI.
  - Execute the following command in the secondary server CLI:
  - PIServer/admin# ncs certvalidation tofu-certs deletecert host <primaryserver's-hostname>
- This is required to re-establish the communication between the Primary and Secondary servers.
- Step 5** Trigger a failback from the secondary to the newly installed primary. During failback to the new primary HA server, a full database copy will be performed, so this operation will take time to complete depending on the available bandwidth and network latency (see “Network Throughput Restrictions on HA” in Related Topics). You will see the two servers transition through the following series of HA states:

| Primary HA State Transitions... | Secondary HA State Transitions... |
|---------------------------------|-----------------------------------|
| From: HA not configured         | From: Secondary Active            |
| To: Primary Failback            | To: Secondary Failback            |
| To: Primary Failback            | To: Secondary Post Failback       |
| To: Primary Active              | To: Secondary Syncing             |

---

### Related Topics

- [How to Trigger Failover](#), on page 284
- [How to Trigger Failback](#), on page 285
- [Respond to Other HA Events](#), on page 286
- [Network Throughput Restrictions on HA](#), on page 265

## How to Recover From Split-Brain Scenario

As explained in “Automatic Versus Manual Failover” (see Related Topics), the possibility of data loss always exists on the rare occasions when a “split-brain scenario” occurs. In this case, you can choose to save the newly added data on the secondary and forget the data that was added on the primary, as explained in the following steps.

- 
- Step 1** Once the network is up, and the secondary server is up, the primary will restart itself automatically, using its standby database. The HA status of the primary server will be, first, “Primary Failover” transitioning to “Primary Syncing”. You can verify this by logging on to the primary server’s Health Monitor web page.
- Step 2** Once the primary server’s status is “Primary Syncing, confirm that a user can log into the secondary server’s Prime Infrastructure page using the web browser (for example, <https://x.x.x.x:443>). Do not proceed until you have verified this.
- Step 3** Once access to the secondary is verified, initiate a failback from the secondary server’s Health Monitor web page (see [How to Trigger Failback, on page 285](#) ). You can continue to perform monitoring activities on the secondary server until the switchover to the primary is completed.

For more information, see [Restart Prime Infrastructure Using CLI, on page 113](#).

---

### Related Topics

- [Automatic Versus Manual Failover](#), on page 268
- [Remove HA Via the CLI](#), on page 300
- [How to Register HA on the Primary Server](#), on page 273

## How to Resolve Database Synchronization Issues

To resolve the database synchronization issue, when the primary server is in "Primary Active" state and the secondary server is in "Secondary Syncing" state, do the following:

- 
- Step 1** Remove HA, see [Remove HA Via the CLI, on page 300](#) and [Remove HA Via the GUI, on page 299](#).
- Step 2** After both the primary and secondary servers reaches "HA not configured" state, perform the HA registration. See [Set Up High Availability, on page 271](#)
- 

## High Availability Reference Information

The following sections supply reference information on HA.

### Related Topics

- [HA Configuration Mode Reference](#), on page 296
- [HA State Reference](#), on page 296
- [HA State Transition Reference](#), on page 297
- [High Availability CLI Command Reference](#), on page 299
- [Reset the HA Authentication Key](#), on page 299
- [Remove HA Via the GUI](#), on page 299

- [Remove HA Via the CLI](#), on page 300
- [Remove HA During Restore](#), on page 300
- [Remove HA During Upgrade](#), on page 301
- [Using HA Error Logging](#), on page 301
- [Reset the HA Server IP Address or Host Name](#), on page 302

## HA Configuration Mode Reference

The following table lists all possible HA configuration modes.

**Table 15: High Availability Modes**

| Mode              | Description                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HA not configured | HA is not configured on this Prime Infrastructure server                                                                                                         |
| HA initializing   | The HA registration process between the primary and secondary server has started.                                                                                |
| HA enabled        | HA is enabled between the primary and secondary server.                                                                                                          |
| HA alone          | Primary server is now running alone. HA is enabled, but the primary server is out of sync with the secondary, or the secondary is down or otherwise unreachable. |

### Related Topics

- [High Availability Reference Information](#), on page 295

## HA State Reference

The following table lists all possible HA states, including those that require no response from you.

**Table 16: High Availability States**

| State                        | Server  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stand Alone                  | Both    | HA is not configured on this Prime Infrastructure server                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Primary Alone                | Primary | Primary restarted after it lost secondary. Only Health Monitor is running in this state.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| HA Initializing              | Both    | HA Registration process between the primary and secondary server has started.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Primary Active               | Primary | Primary server is now active and is synchronizing with secondary server.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Primary Database Copy Failed | Primary | Primary servers being restarted will always check to see if a data gap has occurred due to the primary being down for 24 hours or more. If it detects such a gap, it will automatically trigger a data copy from the active secondary server. In rare cases, this database copy can fail, in which case this transition state is set on the primary. All attempts to failback to the primary are blocked until the database copy completes successfully. As soon as it does, the primary state is set to "Primary Syncing". |
| Primary Failover             | Primary | Primary server detected a failure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Primary Failback             | Primary | Failback triggered by the User is currently in progress.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

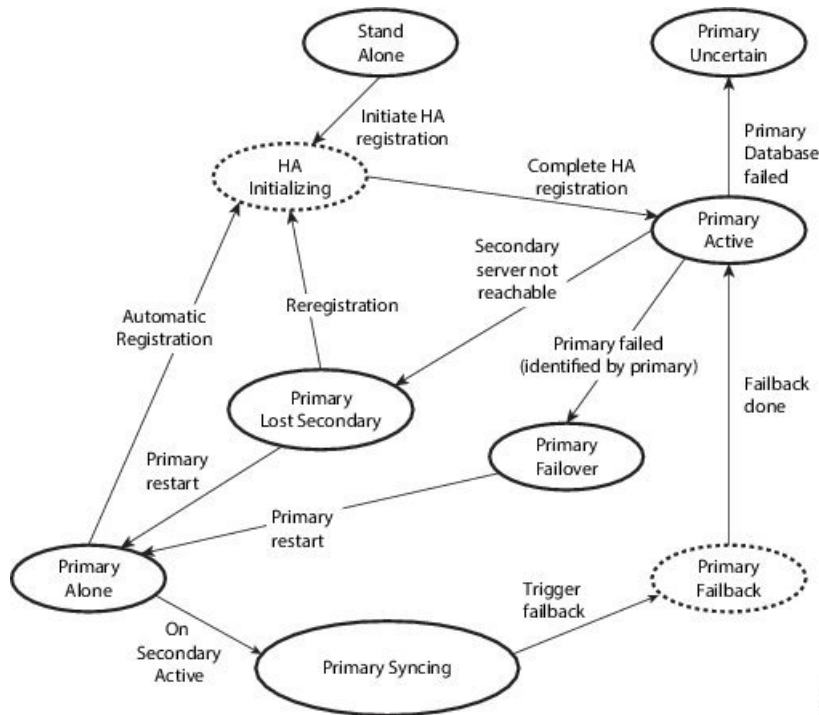
| State                          | Server    | Description                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary Lost Secondary         | Primary   | Primary server is unable to communicate with the secondary server.                                                                                                                                                                                                                                                                                                            |
| Primary Preparing for Failback | Primary   | This state will be set on primary server startup after a failover to the secondary. This state signifies that the primary server has started up in standby mode (because the secondary server is still active) and is ready for failback. Once the primary server is ready for failback, its state will be set to "Primary Syncing".                                          |
| Primary Syncing                | Primary   | Primary server is synchronizing the database and configuration files from the active secondary. Primary gets into this state when primary processes are brought up after failover to secondary and secondary is playing the active role.                                                                                                                                      |
| Primary Uncertain              | Primary   | Primary server's application processes are not able to connect to its database.                                                                                                                                                                                                                                                                                               |
| Secondary Alone                | Secondary | Primary server is not reachable from secondary after primary server restart.                                                                                                                                                                                                                                                                                                  |
| Secondary Syncing              | Secondary | Secondary server is synchronizing the database and configuration files from the primary.                                                                                                                                                                                                                                                                                      |
| Secondary Active               | Secondary | Failover from the primary server to the secondary server has completed successfully.                                                                                                                                                                                                                                                                                          |
| Secondary Lost Primary         | Secondary | Secondary server is not able to connect to the primary server (occurs when the primary fails or network connectivity is lost).<br><br>In case of automatic failover from this state, the secondary will automatically move to Active state. In case of a manual failover, the user can trigger a failover to make the secondary active.                                       |
| Secondary Failover             | Secondary | Failover triggered and in progress.                                                                                                                                                                                                                                                                                                                                           |
| Secondary Failback             | Secondary | Failback triggered and in progress (database and file replication is in progress).                                                                                                                                                                                                                                                                                            |
| Secondary Post Failback        | Secondary | This state occurs after failback is triggered, replication of database and configuration files from the secondary to the primary is complete, and Health Monitor has initiated changes of the secondary server's status to Secondary Syncing and the primary server's status to Primary Active. These status changes and associated process starts and stops are in progress. |
| Secondary Uncertain            | Secondary | Secondary server's application processes are not able to connect to secondary server's database.                                                                                                                                                                                                                                                                              |

### Related Topics

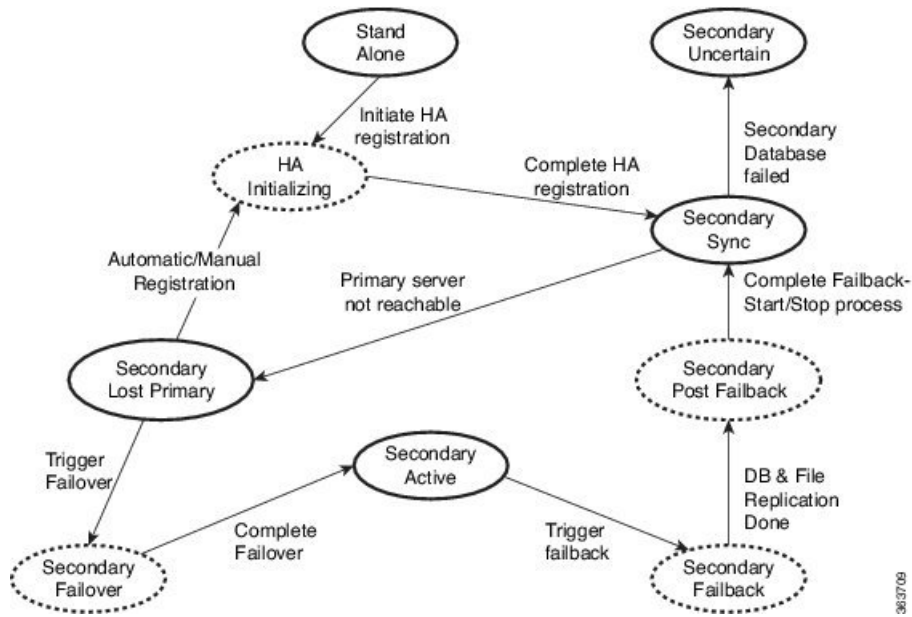
[High Availability Reference Information](#), on page 295

## HA State Transition Reference

The following figure details all possible state transitions for the primary server.



The following figure details all possible state transitions for the secondary server.



**Related Topics**

[High Availability Reference Information](#), on page 295

## High Availability CLI Command Reference

The following table lists the CLI commands available for HA management. Log in as admin to run these commands on the primary server (see [How to Connect Via CLI, on page 111](#)):

**Table 17: High Availability Commands**

| Command                | Description                                         |
|------------------------|-----------------------------------------------------|
| ncs ha ?               | Get help with high availability CLI commands        |
| ncs ha authkey authkey | Update the authentication key for high availability |
| ncs ha remove          | Remove the High Availability configuration          |
| ncs ha status          | Get the current status for High Availability        |

### Related Topics

[High Availability Reference Information](#), on page 295

## Reset the HA Authentication Key

Prime Infrastructure administrators can change the HA authentication key using the **ncs ha authkey** command. You will need to ensure that the new authorization key meets the password standards.

---

**Step 1** Connect to the primary server via CLI. Do not enter “configure terminal” mode.

**Step 2** Enter the following at the command line:

```
admin# ncs ha authkey MyNewAuthKey
```

Where *MyNewAuthKey* is the new authorization key. For more information, see [How to Connect Via CLI, on page 111](#).

---

### Related Topics

[Before You Begin Setting Up High Availability](#), on page 272

[High Availability Reference Information](#), on page 295

## Remove HA Via the GUI

The simplest method for removing an existing HA implementation is via the GUI, as shown in the following steps. You can also remove the HA setup via the command line.

Note that, to use this method, you must ensure that the primary Prime Infrastructure server is currently in the “Primary Active” state. If for any reason the secondary server is currently active, perform a failback and then try to remove the HA configuration after the failback is complete and the secondary’s automatic restart has finished.

---

**Step 1** Log in to the primary Prime Infrastructure server with a user ID that has administrator privileges.

**Step 2** Select **Administration > Settings > High Availability > HA Configuration**.

**Step 3** Select **Remove**. Removing the HA configuration takes from 3 to 4 minutes.

Once the removal is complete, ensure that the HA configuration mode displayed on the page now reads “HA Not Configured”.

---

#### Related Topics

[Remove HA Via the CLI](#), on page 300

[How to Trigger Failback](#), on page 285

[High Availability Reference Information](#), on page 295

## Remove HA Via the CLI

If for any reason you cannot access the Prime Infrastructure GUI on the primary server, administrators can remove the HA setup via the command line, using the steps below.

Note that, to use this method, you must ensure that the primary Prime Infrastructure server is currently in the “Primary Active” state. If for any reason the secondary server is currently active, perform a failback and then try to remove the HA configuration after the failback is complete and the secondary’s automatic restart has finished.

---

**Step 1** Connect to the primary server via CLI. Do not enter “configure terminal” mode.

**Step 2** Enter the following at the command line:

admin# **ncs ha remove**. For more information, see [How to Connect Via CLI](#), on page 111.

---

#### Related Topics

[Remove HA Via the GUI](#), on page 299

[How to Trigger Failback](#), on page 285

[High Availability Reference Information](#), on page 295

## Remove HA During Restore

Prime Infrastructure does not back up configuration settings related to High Availability.

In order to restore a Prime Infrastructure implementation that is using HA, be sure to restore the backed up data to the primary server only. The restored primary will automatically replicate its data to the secondary server. Running a restore on the secondary server is not needed and will generate an error message if you attempt it.

To restore a Prime Infrastructure implementation that uses HA, follow the steps below.

---

**Step 1** Use the GUI to remove the HA settings from the primary server (see “Remove HA Via the GUI” in Related Topics).

**Step 2** Restore the primary server as needed.

**Step 3** Once the restore is complete, perform the HA registration process again.



For more information, see [Restore Data, on page 57](#) and [How to Connect Via CLI, on page 111](#).

---

### Related Topics

- [Remove HA Via the GUI, on page 299](#)
- [How to Register HA on the Primary Server, on page 273](#)
- [High Availability Reference Information, on page 295](#)

## Remove HA During Upgrade

To upgrade a Prime Infrastructure implementation that uses HA, follow the steps below.

- 
- Step 1** Use the GUI to remove the HA settings from the primary server (see “Remove HA Via the GUI” in Related Topics, below).
  - Step 2** Upgrade the primary server as needed.
  - Step 3** Re-install the secondary server using the current image.  
  
Note that upgrading the secondary server from the previous version or a beta version is not supported. The secondary server must always be a fresh installation.
  - Step 4** Once the upgrade is complete, perform the HA registration process again.

**Note** After upgrade, health monitor page will display the below health monitor event message:

Primary Authentication Key was changed by Admin

For more information, see [How to Connect Via CLI, on page 111](#).

---

### Related Topics

- [Remove HA Via the GUI, on page 299](#)
- [How to Register HA on the Primary Server, on page 273](#)
- [High Availability Reference Information, on page 295](#)

## Using HA Error Logging

Error logging for the High Availability feature is disabled by default, to save disk space and maximize performance. If you are having trouble with HA, the best place to begin is by enabling error logging and to examine the log files.

- 
- Step 1** View the Health Monitor page for the server having trouble.
  - Step 2** In the **Logging** area, in the **Message Level** dropdown, select the error-logging level you want.
  - Step 3** Click **Save**.
  - Step 4** When you want to download the log files: In the **Logs** area, click **Download**. You can open the downloaded log files using any ASCII text editor.
-

**Related Topics**

[Access the Health Monitor Web Page](#), on page 284

[High Availability Reference Information](#), on page 295

## Reset the HA Server IP Address or Host Name

Avoid changing the IP address or hostname of the primary or secondary HA server, if possible. If you must change the IP address or hostname, remove the HA configuration from the primary server before making the change. When finished, re-register HA.

**Related Topics**

[Remove HA Via the GUI](#), on page 299

[How to Register HA on the Primary Server](#), on page 273

[High Availability Reference Information](#), on page 295

## Configure MSE High Availability

The Cisco Mobility Services Engine (MSE) is a platform for hosting multiple mobility applications. Under an MSE high availability (HA) configuration, an active MSE is backed up by another inactive instance of MSE. The active MSE is called the primary MSE and the inactive MSE is called the secondary MSE.

**Related Topics**

[Overview of the MSE High Availability Architecture](#), on page 302

[Set Up MSE High Availability: Workflow](#), on page 304

## Overview of the MSE High Availability Architecture

The main component of MSE high availability is the health monitor. The health monitor configures, manages, and monitors the HA setup on each MSE. Heartbeat is maintained between the primary and secondary MSE. Health monitor is responsible for setting up the database, file replication, and monitoring the application. When the primary MSE fails and the secondary MSE takes over, the virtual address of the primary MSE is switched transparently to the secondary MSE. Note that:

- Every active primary MSE is backed up by another inactive instance. The purpose of the secondary MSE is to monitor the availability and state of the primary MSE. The secondary MSE becomes active only after the failover procedure is initiated.
- One secondary MSE can support one primary MSE.

The MSEs, Synchronize Services, Synchronization History, High Availability, Context Aware Notifications, and Mobile Concierge pages on the Services tab are available only in the virtual domain in Release 7.3.

The following related topics provide additional details on the MSE high availability architecture.

**Related Topics**

[MSE High Availability Pairing Matrix](#), on page 303

[Guidelines and Limitations for MSE High Availability](#), on page 303

[Failover Scenario for MSE High Availability](#), on page 304

[Failback Scenario for MSE High Availability](#), on page 304

[Licensing Requirements for MSE High Availability](#), on page 304

[Configure MSE High Availability](#) , on page 302

## MSE High Availability Pairing Matrix

The following table lists the types of MSE servers that can be paired in a high-availability configuration.

**Table 18: MSE High Availability Server Pairing Matrix**

| Primary Server Type | Secondary Server Type |      |      |      |   |
|---------------------|-----------------------|------|------|------|---|
| 3355                | VA-2                  | VA-3 | VA-4 | VA-5 |   |
| 3355                | Y                     | N    | N    | N    | N |
| VA-2                | N                     | Y    | Y    | Y    | Y |
| VA-3                | N                     | N    | Y    | Y    | Y |
| VA-4                | N                     | N    | N    | Y    | Y |
| VA-5                | N                     | N    | N    | N    | Y |

### Related Topics

[Using the Remote Model](#), on page 267

[Guidelines and Limitations for MSE High Availability](#), on page 303

## Guidelines and Limitations for MSE High Availability

Administrators implementing MSE High Availability and planning to manage it via Prime Infrastructure should observe the following guidelines and limitations:

- Both the health monitor IP and virtual IP should be accessible from Prime Infrastructure.
- The health monitor IP and virtual IP should always be different. The health monitor and virtual interface can be on the same network interface or different interfaces.
- You can use either manual or automatic failover. Failover should be considered temporary. The failed MSE should be restored to normal as soon as possible, and failback should be re-initiated. The longer it takes to restore the failed MSE, the longer you are running with a single MSE without high availability support.
- You can use either manual or automatic failback.
- Both the primary and secondary MSE should be running the same software version.
- High Availability over WAN is not supported.
- High Availability over LAN is supported only when both the primary and secondary MSEs are in the same subnet.
- The ports over which the primary and secondary MSEs communicate must be open (not blocked with network firewalls, application firewalls, gateways, and so on). The following input/output ports should be opened: 80, 443, 8080, 8081, 22, 8001, 1521, 1411, 1522, 1523, 1524, 1525, 9006, 15080, 61617, 59000, 12091, 1621, 1622, 1623, 1624, 1625, 8083, 8084, and 8402.

### Related Topics

[Overview of the MSE High Availability Architecture](#), on page 302

[MSE High Availability Pairing Matrix](#), on page 303

[Failover Scenario for MSE High Availability](#), on page 304

## Failover Scenario for MSE High Availability

When a primary MSE failure is detected, the following events occur:

- The primary MSE is confirmed as non-functioning (hardware fail, network fail, and so on) by the health monitor on the secondary MSE.
- If automatic failover isn't enabled, the secondary MSE starts immediately.
- If manual failover is enabled, an e-mail is sent to the administrator asking if they want to manually start failover. This e-mail is sent only if the e-mail is configured for MSE alarms.
- The result of the failover operation is indicated as an event in the Health Monitor UI, and a critical alarm is sent to Prime Infrastructure.

### Related Topics

[Overview of the MSE High Availability Architecture](#), on page 302

[Guidelines and Limitations for MSE High Availability](#), on page 303

[Failback Scenario for MSE High Availability](#), on page 304

## Failback Scenario for MSE High Availability

When the primary MSE is restored to its normal state, if the secondary MSE is already in failover state for the primary, then failback can be invoked.

Failback can occur only if the secondary MSE is in one of the following states for the primary instance:

- The secondary MSE is actually failing over for the primary MSE.
- Manual failover is configured but the administrator did not invoke it.
- The primary MSE failed but the secondary MSE cannot take over because it has encountered errors.
- Failback can occur only if the administrator starts up the failed primary MSE.

### Related Topics

[Overview of the MSE High Availability Architecture](#), on page 302

[Failover Scenario for MSE High Availability](#), on page 304

[Licensing Requirements for MSE High Availability](#), on page 304

## Licensing Requirements for MSE High Availability

For high availability, an activation license is required on the primary and secondary virtual appliances. No other service license is required on the secondary MSE. It is required only on the primary MSE.

### Related Topics

[Overview of the MSE High Availability Architecture](#), on page 302

[Failback Scenario for MSE High Availability](#), on page 304

## Set Up MSE High Availability: Workflow

During the installation of the MSE software (or using the MSE setup script), configure some critical elements. Pair up the primary and secondary MSE from the Prime Infrastructure UI.

By default, all MSEs are configured as primary. If you do not want high availability support and are upgrading from an earlier release, you can continue to use the IP address for the MSE. If you want to set up high availability, then you must configure the health monitor IP address. The health monitor then becomes a virtual IP address.

Configuring MSE high availability consists of the following steps:

1. Prepare the MSEs for High Availability
2. Configure the Primary MSE
3. Configure the Secondary MSE

You may also need to reconfigure MSE high availability if you must replace the primary MSE server.

For details, see the corresponding Related Topics, below.

#### Related Topics

- [Prepare the MSEs for High Availability](#), on page 305
- [Configure MSE High Availability on Primary MSEs](#), on page 305
- [Configure MSE High Availability on Secondary MSEs](#), on page 313
- [Replace Primary MSEs](#), on page 319
- [Configure MSE High Availability](#)

## Prepare the MSEs for High Availability

To prepare your primary and secondary MSEs for high availability, follow these steps:

- 
- Step 1** Ensure that the network connectivity between the primary and secondary MSEs is functioning and that all the necessary ports are open.
  - Step 2** Install the correct version of MSE on the primary MSE.
  - Step 3** Make sure that the same MSE version is installed on the secondary MSE.
- 

#### Related Topics

- [Replace Primary MSEs](#), on page 319
- [Configure MSE High Availability](#), on page 302

## Configure MSE High Availability on Primary MSEs

To configure a primary MSE for high availability, follow these steps:

- 
- Step 1** On the intended primary MSE, enter the following command:

```
/opt/mse/setup/setup.sh
```

The setup script displays the following prompts, which you can answer using the suggested responses given in bold (in this and later steps):

```

Welcome to the Cisco Mobility Services Engine Appliance Setup.
You may exit the setup at any time by typing <Ctrl+c>.

Would you like to configure MSE using:
1. Menu mode
2. Wizard mode
```

Choose 1 or 2: **1**

-----  
 Mobility Services Engine Setup

Please select a configuration option below and enter the requested information. You may exit setup at any time by typing <Ctrl +C>.

You will be prompted to choose whether you wish to configure a parameter, skip it, or reset it to its initial default value. Skipping a parameter will leave it unchanged from its current value.

Please note that the following parameters are mandatory and must be configured at least once.

- > Hostname
- > Network interface eth0
- > Timezone settings
- > Root password
- > NTP settings
- > Prime Infrastructure password

You must select option 24 to verify and apply any changes made during this session.

-----  
 PRESS <ENTER> TO CONTINUE:

-----  
 Configure MSE:

- 1) Hostname \* 13) Remote syslog settings
- 2) Network interface eth0 settings\* 14) Host access control settings
- 3) Timezone settings\* 15) Audit Rules
- 4) Root password \* 16) Login banner
- 5) NTP settings \* 17) System console restrictions
- 6) Prime Infrastructure password \* 18) SSH root access
- 7) Display current configuration 19) Single user password check
- 8) Domain 20) Login and password settings
- 9) High availability role 21) GRUB password
- 10) Network interface eth1 settings 22) Root access control
- 11) DNS settings 23) Auto start MSE on system boot up
- 12) Future restart time 24) ### Verify and apply changes ##

Please enter your choice [1 - 24]:

**Step 2**

Configure the primary MSE hostname:

Please enter your choice [1 - 24]: **1**

Current Hostname=[mse]

Configure Hostname? (Y)es/(S)kip/(U)se default [Skip]: **y**

The host name should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.

Enter a Host name [mse]:**mse1**

**Step 3** Configure the primary MSE domain:

Please enter your choice [1-24]: **8**

Current domain=[ ]

Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: **S**

**Step 4** Configure the primary MSE network interface eth0 settings.

Please enter your choice [1 - 24]: **2**

Current eth0 interface IP address=[10.0.0.1]

Current eth0 interface netmask=[255.0.0.0]

Current IPv4 gateway address=[172.20.104.123]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]: **y**

Enter an IP address for first Ethernet interface of this machine.

Enter eth0 IP address [10.0.0.2]:

Enter the network mask for IP address 172.21.105.126

Enter network mask [255.255.255.224]:

Enter the default gateway address for this machine.

Note that the default gateway must be reachable from the first Ethernet interface.

Enter default gateway address [172.20.104.123]:

**Step 5** Configure the primary MSE root password:

Please enter your choice [1 - 24]: **4**

Root password has not been configured

Configure root password? (Y)es/(S)kip/(U)se default [Skip]: **Y**

Changing password for user root.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use an 8 character long password with characters from all of these classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used.

Enter new password: **password**

**Step 6** Configure the primary MSE's high availability role:

Current role=[Primary]

Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]: **y**

High availability role for this MSE (Primary/Secondary)

Select role [1 for Primary, 2 for Secondary] [1]: 1

Health monitor interface holds physical IP address of this MSE server.

This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to communicate among themselves

Select Health Monitor Interface [eth0/eth1] [eth0]: eth0

-----

Direct connect configuration facilitates use of a direct cable connection between the primary and secondary MSE servers.

This can help reduce latencies in heartbeat response times, data replication and failure detection times.

Please choose a network interface that you wish to use for direct connect. You should appropriately configure the respective interfaces.

"none" implies you do not wish to use direct connect configuration.

-----

Select direct connect interface [eth0/eth1/none] [none]:

Enter a Virtual IP address for the Primary MSE server

Enter Virtual IP address [1.1.1.1]: **10.10.10.11**

Enter network mask for IP address 10.10.10.1

Enter network mask [1.1.1.1]: **255.255.255.0**

Select to start the server in recovery mode.

You should choose yes only if this primary MSE was paired earlier and you have now lost the configuration from this box.

And, now you want to restore the configuration from Secondary via Cisco Prime Infrastructure

Do you wish to start this MSE in HA recovery mode?: (yes/no) [no]:no

Current IP address = [1.1.1.10]

Current eth0 netmask=[255.255.255.0]

Current gateway address=[1.1.1.1]

Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:

Enter an IP address for first Ethernet interface of this machine.

Enter eth0 IP address [1.1.1.10]: **10.10.10.12**

Enter the network mask for IP address 10.10.10.12

Enter network mask [255.255.255.0]: **255.255.255.0**

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from the first Ethernet interface. Enter default gateway address [1.1.1.1]:**10.10.10.1**

The second Ethernet interface is currently disabled for this machine.

Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: S



**Step 7**

Configure the primary MSE timezone settings:

Please enter your choice [1 - 24]: 3

Current Timezone=[America/New\_York]

Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly. Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) UTC - I want to use Coordinated Universal Time.

#? 2

Please select a country.

- 1) Anguilla 27) Honduras
- 2) Antigua & Barbuda 28) Jamaica
- 5) Bahamas 31) Montserrat
- 6) Barbados 32) Netherlands Antilles
- 7) Belize 33) Nicaragua
- 8) Bolivia 34) Panama
- 9) Brazil 35) Paraguay
- 10) Canada 36) Peru
- 11) Cayman Islands 37) Puerto Rico
- 12) Chile 38) St Barthelemy
- 13) Colombia 39) St Kitts & Nevis
- 14) Costa Rica 40) St Lucia
- 15) Cuba 41) St Martin (French part)
- 16) Dominica 42) St Pierre & Miquelon
- 17) Dominican Republic 43) St Vincent

- 18) Ecuador 44) Suriname
- 19) El Salvador 45) Trinidad & Tobago
- 20) French Guiana 46) Turks & Caicos Is
- 21) Greenland 47) United States
- 22) Grenada 48) Uruguay
- 23) Guadeloupe 49) Venezuela
- 24) Guatemala 50) Virgin Islands (UK)
- 25) Guyana 51) Virgin Islands (US)
- 26) Haiti
- #? 47

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Time - Indiana - most locations
- 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
- 7) Eastern Time - Indiana - Pulaski County
- 8) Eastern Time - Indiana - Crawford County
- 9) Eastern Time - Indiana - Pike County
- 10) Eastern Time - Indiana - Switzerland County
- 11) Central Time
- 12) Central Time - Indiana - Perry County
- 13) Central Time - Indiana - Starke County
- 14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
- 15) Central Time - North Dakota - Oliver County
- 16) Central Time - North Dakota - Morton County (except Mandan area)
- 17) Mountain Time
- 18) Mountain Time - south Idaho & east Oregon
- 19) Mountain Time - Navajo
- 20) Mountain Standard Time - Arizona
- 21) Pacific Time
- 22) Alaska Time
- 23) Alaska Time - Alaska panhandle

24) Alaska Time - Alaska panhandle neck

25) Alaska Time - west Alaska

26) Aleutian Islands

27) Hawaii

#? 21

The following information has been given:

United States

Pacific Time

Therefore TZ='America/Los\_Angeles' will be used.

Local time is now: Sun Apr 6 18:45:27 PDT 2020. Universal Time is now: Mon Apr 7 01:45:27 UTC 2020. Is the above information OK?

1) Yes

2) No

#? 1

### Step 8

Configure the primary MSE DNS settings:

Please enter your choice [1 - 24]: 11

Domain Name Service (DNS) Setup

Enable DNS (yes/no) [no]: y

Default DNS server 1=[8.8.8.8]

Enter primary DNS server IP address:

DNS server address must be in the form #.#.#.#, where # is 0 to 255 or hexadecimal :

separated v6 address

Enter primary DNS server IP address [8.8.8.8]:

Enter backup DNS server IP address (or none) [none]:

### Step 9

Configure the primary MSE NTP settings:

Please enter your choice [1 - 24]: 5

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

NTP is currently disabled.

Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the

Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: y

Default NTP server 1=[time.nist.gov] Enter NTP server name or address:

NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :  
separated v6 address.

Enter NTP server name or [time.nist.gov]:

Enter another NTP server IP address (or none) [none]:

Configure NTP Authentication? (Y)es/(S)kip/(U)se default [Skip]: y

Enter NTP Auth key Number [1]:

Enter NTP Auth key Value (String) [Secret]: Do you want to continue (yes/no) [no]: y

### Step 10

Configure the Prime Infrastructure password:

Please enter your choice [1 - 24]: 6

Cisco Prime Infrastructure communication password has not been configured. Configure Prime Infrastructure password? (Y)es/(S)kip/(U)se default [Yes]:

Enter a password for the admin user.

The admin user is used by the Prime Infrastructure and other northbound systems to authenticate their SOAP/XML session with the server. Once this password is updated, it must correspondingly be updated on the NCS page for MSE General Parameters so that the Prime Infrastructure can communicate with the MSE.

### Step 11

Verify and apply your changes:

Please enter your choice: 24

Please verify the following setup information.

-----BEGIN----- Hostname=mse1

Role= 1, Health Monitor Intercace=eth0, Direct connect interface=none

Virtual IP Address=10.10.10.11, Virtual IP Netmask=255.255.255.0

Eth0 IP address=10.10.10.12, Eth0 network mask=255.0.0.0

Default Gateway=10.10.10.1

Time zone=America/Los\_Angeles

Enable DNS=yes, DNS servers=8.8.8.8

Enable NTP=yes, NTP servers=time.nist.gov

Time zone=America/Los\_Angeles

Root password is changed.

Cisco Prime Infrastructure password is changed.

-----END-----

You may enter "yes" to proceed with configuration, "no" to make more changes.

Configuration Changed

Is the above information correct (yes or no): yes

-----

Checking mandatory configuration information...

Root password: Not configured

**\*\*WARNING\*\***

The above parameters are mandatory and need to be configured.

-----

Ignore and proceed (yes/no): yes

Setup will now attempt to apply the configuration. Restarting network services with new settings. Shutting down interface eth0:

The system is minimally configured right now. It is strongly recommended that you run the setup script under `/opt/mse/setup/setup.sh` command to configure all appliance related parameters immediately after installation is complete.

PRESS <ENTER> TO EXIT THE INSTALLER:

#### Step 12

Reboot the system:

```
[root@mse1]# reboot Stopping MSE Platform
```

```
Flushing firewall rules: [OK]
```

```
Setting chains to policy ACCEPT: nat filter [OK] Unloading iptables modules: [ok]
```

```
Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):
```

```
The system is going down for reboot NOW:
```

#### Step 13

Start the MSE services:

```
[root@mse1]# /etc/init.d/msed start
```

```
Starting MSE Platform.
```

```
Starting Health Monitor, Waiting to check the status. Starting Health Monitor, Waiting to check the status. Health Monitor successfully started
```

```
Starting Admin process... Started Admin process. Starting database
```

```
Database started successfully. Starting framework and services..... Framework and services successfully started
```

#### Step 14

After all services have started, confirm MSE services are working properly by entering the following command:

```
[root@mse1]# getserverinfo
```

---

#### Related Topics

[Prepare the MSEs for High Availability](#), on page 305

[Configure MSE High Availability on Secondary MSEs](#), on page 313

[Configure MSE High Availability](#), on page 302

## Configure MSE High Availability on Secondary MSEs

To prepare your secondary MSE for high availability, follow these steps:

- 
- Step 1** On the intended secondary MSE, enter the following command:
- ```
/opt/mse/setup/setup.sh
```
- The setup script displays the same prompts as for the primary MSE:
- Step 2** Configure the secondary MSE hostname:
- ```
Please enter your choice [1 - 24]: 1
Current hostname=[mse1]
Configure hostname? (Y)es/(S)kip/(U)se default [Yes]: yes
```
- The host name should be a unique name that can identify the device on the network. The hostname should start with a letter, end with a letter or number, and contain only letters, numbers, and dashes.
- ```
Enter a hostname [mse]: mse2
```
- Step 3** Configure the secondary MSE domain:
- ```
Please enter your choice [1-24]: 8
Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]: S
```
- Step 4** Configure the secondary MSE high availability role:
- ```
Current role=[Primary]
Configure High Availability? (Y)es/(S)kip/(U)se default [Skip]: High availability role for this MSE (Primary/Secondary)
Select role [1 for Primary, 2 for Secondary] [1]: 2
```
- Health monitor interface holds physical IP address of this MSE server.
- This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to communicate among themselves
- ```
Select Health Monitor Interface [eth0/eth1] [eth0]: eth0
```
- 
- Direct connect configuration facilitates use of a direct cable connection between the primary and secondary MSE servers. This can help reduce latencies in heartbeat response times, data replication and failure detection times. Please choose a network interface that you wish to use for direct connect. You should appropriately configure the respective interfaces.
- "none" implies you do not wish to use direct connect configuration.
- 
- ```
Select direct connect interface [eth0/eth1/none] [none]:
Current IP address=[1.1.1.10]
Current eth0 netmask=[255.255.255.0] Current gateway address=[1.1.1.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Yes]:
Enter an IP address for first Ethernet interface of this machine. Enter eth0 IP address [1.1.1.10]: 10.10.10.13
Enter the network mask for IP address 10.10.10.13
```

Enter network mask [255.255.255.0]:

Enter an default gateway address for this machine.

Note that the default gateway must be reachable from the first Ethernet interface. Enter default gateway address [1.1.1.1]:10.10.10.1

The second Ethernet interface is currently disabled for this machine. Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: S

Step 5

Configure the secondary MSE timezone settings:

Please enter your choice [1 - 24]: 3

Current Timezone=[America/New_York]

Configure Timezone? (Y)es/(S)kip/(U)se default [Skip]: y

Enter the current date and time.

Please identify a location so that time zone rules can be set correctly. Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) UTC - I want to use Coordinated Universal Time.

#? 2

Please select a country.

- 1) Anguilla 27) Honduras
- 2) Antigua & Barbuda 28) Jamaica
- 5) Bahamas 31) Montserrat
- 6) Barbados 32) Netherlands Antilles
- 7) Belize 33) Nicaragua
- 8) Bolivia 34) Panama
- 9) Brazil 35) Paraguay
- 10) Canada 36) Peru
- 11) Cayman Islands 37) Puerto Rico
- 12) Chile 38) St Barthelemy

- 13) Colombia 39) St Kitts & Nevis
- 14) Costa Rica 40) St Lucia
- 15) Cuba 41) St Martin (French part)
- 16) Dominica 42) St Pierre & Miquelon
- 17) Dominican Republic 43) St Vincent
- 18) Ecuador 44) Suriname
- 19) El Salvador 45) Trinidad & Tobago
- 20) French Guiana 46) Turks & Caicos Is
- 21) Greenland 47) United States
- 22) Grenada 48) Uruguay
- 23) Guadeloupe 49) Venezuela
- 24) Guatemala 50) Virgin Islands (UK)
- 25) Guyana 51) Virgin Islands (US)
- 26) Haiti
- #? 47

Please select one of the following time zone regions.

- 1) Eastern Time
- 2) Eastern Time - Michigan - most locations
- 3) Eastern Time - Kentucky - Louisville area
- 4) Eastern Time - Kentucky - Wayne County
- 5) Eastern Time - Indiana - most locations
- 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
- 7) Eastern Time - Indiana - Pulaski County
- 8) Eastern Time - Indiana - Crawford County
- 9) Eastern Time - Indiana - Pike County
- 10) Eastern Time - Indiana - Switzerland County
- 11) Central Time
- 12) Central Time - Indiana - Perry County
- 13) Central Time - Indiana - Starke County
- 14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
- 15) Central Time - North Dakota - Oliver County
- 16) Central Time - North Dakota - Morton County (except Mandan area)
- 17) Mountain Time
- 18) Mountain Time - south Idaho & east Oregon

- 19) Mountain Time - Navajo
- 20) Mountain Standard Time - Arizona
- 21) Pacific Time
- 22) Alaska Time
- 23) Alaska Time - Alaska panhandle
- 24) Alaska Time - Alaska panhandle neck
- 25) Alaska Time - west Alaska
- 26) Aleutian Islands
- 27) Hawaii

#? 21

The following information has been given: United States

Pacific Time

Therefore TZ='America/Los_Angeles' will be used.

Local time is now: Sun Apr 6 18:45:27 PDT 2014. Universal Time is now: Mon Apr 7 01:45:27 UTC 2014. Is the above information OK?

1) Yes

2) No

#? 1

Step 6

Configure the secondary MSE NTP settings:

Please enter your choice [1 - 24]: 5

Network Time Protocol (NTP) Setup.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

NTP is currently disabled.

Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Skip]: y

Enter whether or not you would like to set up the Network Time Protocol (NTP) for this machine.

If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time.

Enable NTP (yes/no) [no]: y

Default NTP server 1=[time.nist.gov] Enter NTP server name or address:

NTP server address must be in the form #.#.#.3, where # is 0 to 255 hexadecimal :
separated v6 address.

Enter NTP server name or [time.nist.gov]:

Enter another NTP server IP address (or none) [none]:

Configure NTP Authentication? (Y)es/(S)kip/(U)se default [Skip]: y

Enter NTP Auth key Number [1]:

Enter NTP Auth key Value (String) [Secret]: Do you want to continue (yes/no) [no]: y

Step 7

Verify and apply your changes:

Please enter your choice: 24

Please verify the following setup information.

-----BEGIN----- Hostname=mse2

Role= 2, Health Monitor Interface=eth0, Direct connect interface=none

Eth0 IP address=10.10.10.13, Eth0 network mask=255.255.255.0

Default Gateway=10.10.10.1

Time zone=America/Los_Angeles

Enable NTP=yes, NTP servers=time.nist.gov

Time zone=America/Los_Angeles

-----END-----

You may enter "yes" to proceed with configuration, "no" to make more changes.

Configuration Changed

Is the above information correct (yes or no): yes

Checking mandatory configuration information...

Root password: Not configured

****WARNING****

The above parameters are mandatory and need to be configured.

Ignore and proceed (yes/no): yes

Setup will now attempt to apply the configuration.

Restarting network services with new settings. Shutting down interface eth0:

The system is minimally configured right now. It is strongly recommended that you run the setup script under /opt/mse/setup/setup.sh command to configure all appliance related parameters immediately after installation is complete.

PRESS <ENTER> TO EXIT THE INSTALLER:

Step 8

Reboot the system:

```
[root@mse2 installers]# reboot
```

Stopping MSE Platform

Flushing firewall rules: [OK]

Setting chains to policy ACCEPT: nat filter [OK] Unloading iptables modules: [ok]

Broadcast message from root (pts/0) (Tue Apr29 14:15:27:2014):

The system is going down for reboot NOW:

Step 9

Start the MSE services:

```
[root@mse2]# /etc/init.d/msed start
```

Starting MSE Platform.

Starting Health Monitor, Waiting to check the status. Starting Health Monitor, Waiting to check the status. Health Monitor successfully started

Starting Admin process... Started Admin process. Starting database

Database started successfully. Starting framework and services..... Framework and services successfully started

Related Topics

[Prepare the MSEs for High Availability](#), on page 305

[Configure MSE High Availability on Primary MSEs](#), on page 305

[Configure MSE High Availability](#) , on page 302

Replace Primary MSEs

If for any reason you need to replace a primary MSE, you will want to recover the current pairing information to a newly configured primary MSE, as explained in the following steps.

Step 1

Configure the MSE as a primary using the setup script.

Step 2

Set up a pairing between the primary and secondary MSE using Prime Infrastructure.

Step 3

Initiate failover from the primary MSE to the secondary MSE.

Step 4

Configure the replacement MSE as a primary using the setup script. The new primary MSE must have the same version of the software as the secondary, and the same settings as the old primary MSE.

Step 5

Choose the recovery mode and follow the instructions.

Step 6

Initiate the failback to the new primary using Prime Infrastructure.

A new license is required on the this new primary MSE, as the original license will not match the UDI of the primary, and will not work.

Related Topics

[Configure MSE High Availability on Primary MSEs](#), on page 305

[Configure MSE High Availability](#) , on page 302



CHAPTER 12

Configure Wireless Redundancy

- [About Wireless Controller Redundancy, on page 321](#)
- [Prerequisites and Limitations for Redundancy, on page 321](#)
- [Configure Redundancy Interfaces, on page 322](#)
- [Configure Redundancy on Primary Controllers, on page 322](#)
- [Configure Redundancy on Secondary Controllers, on page 323](#)
- [Monitor Redundancy States, on page 324](#)
- [Configure Peer Service Port IPs and Subnet Mask, on page 324](#)
- [Add Peer Network Routes, on page 325](#)
- [Reset and Upload Files from the Secondary Server, on page 325](#)
- [Disable Redundancy on Controllers, on page 326](#)

About Wireless Controller Redundancy

In a redundancy architecture, one wireless controller is in the Active state and a second controller is in the Standby state. The Standby controller continuously monitors the health of the Active controller via 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 identification (UDI). A controller with 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.

In this release, a stateful switchover of access points (AP SSO) is supported. An AP SSO ensures that the AP sessions are intact even after a switchover.

Stateful switchover of *clients* is not supported. This means that nearly all clients are deauthenticated and forced to re-associate with the new controller in the Active state. The only exceptions to this rule are clients on locally switched WLANs on access points in FlexConnect mode.

Prerequisites and Limitations for Redundancy

Before configuring wireless controller redundancy, you must consider the following prerequisites and limitations:

- Wireless controller redundancy is supported only on the 5500, 7500, 8500, and Wism2 controllers.

- The primary and secondary controllers must be of the same hardware model.
- The primary and secondary controllers must be running the same Controller software release.
- The IP addresses of the management, redundancy management, and peer redundancy management interfaces must be in the same subnet.
- The service port IP address and route information is maintained for each device.
- If the redundancy is enabled on a controller, the Prime Infrastructure or any other device cannot manage the standby controller.
- You cannot enable the redundancy on a controller if the controller is added to the Prime Infrastructure through the service port. You must delete the controller and add it through the management interface to enable the redundancy on that controller.
- When there is an audit mismatch between a controller and the Prime Infrastructure, you must not restore the redundancy parameters from the Prime Infrastructure on to the controller. However, you can refresh the redundancy parameters in the Prime Infrastructure.
- Before you enable the redundancy, you must download the certificates for each device.
- Configuration is downloaded from the network to the active controller, and then the details are transferred to the standby controller through the redundancy interface.
- When an old active controller pairs up with the new active controller, the control is not transferred back to the old active controller and it becomes the standby controller for the new active controller.

Configure Redundancy Interfaces

There are two redundancy interfaces: redundancy-management interface and redundancy-port interface. The redundancy-management interface is a local physical management interface that shares the subnet mask, gateway, and VLAN ID from the management interface. You must configure only the IP address for the redundancy-management interface to enable redundancy on the primary and secondary controllers. The IP address for the redundancy-port interface is auto-generated and it is used internally.

-
- Step 1** Choose **Configuration** > **Network** > **Network Devices**.
- Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the group of wireless controllers that match the device you have chosen as the primary controller (for example: Cisco 5500 Series Wireless LAN Controllers). Members of this device group are displayed on the right.
- Step 4** Click on the **Device Name** of the primary controller.
- Step 5** Click the **Configuration** tab.
- Step 6** From the left sidebar menu, choose **Redundancy** > **Global Configuration**. The Global Configuration page appears.
- Step 7** In the Redundancy-Management IP text box, enter an IP address that belongs to the management interface subnet.
- Step 8** Click **Save**.
-

Configure Redundancy on Primary Controllers

-
- Step 1** Choose **Configuration** > **Network** > **Network Devices**.
- Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.

- Step 3** Select the group of wireless controllers that match the device for which you have configured the redundancy-management interface IP address (for example: Cisco 5500 Series Wireless LAN Controllers). Members of this device group are displayed on the right.
- Step 4** Click on the **Device Name** of the controller for which you have configured the redundancy-management interface IP address.
- Step 5** Click the **Configuration** tab.
- Step 6** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration page appears.
- Step 7** You must configure the following parameters before you enable the redundancy mode for the primary controller:
- Redundancy-Management IP—The IP address of the local physical management interface, which you had configured in the redundancy-management interface details page is displayed. You can also modify the IP address.
 - Peer Redundancy-Management IP—Enter the IP address of the peer redundancy-management interface.
 - Redundant Unit—Choose **Primary**.
 - Mobility MAC Address—Enter the virtual MAC address for the redundancy pair. Ensure that the mobility MAC address that you enter is the same for both primary and secondary controllers.
- Step 8** Click **Save**. The **Enabled** check box for the redundancy mode becomes available.
- Step 9** Select the **Enabled** check box for the redundancy mode to enable the redundancy on the primary controller.
- After you enable the redundancy, you cannot modify the Redundancy-Management IP, Peer Redundancy-Management IP, Redundant Unit, and Mobility MAC Address parameters.
- You cannot configure this controller during the redundancy pair-up process.
- Step 10** Click **Save**. The configuration is saved and the system reboots.
-

Configure Redundancy on Secondary Controllers

- Step 1** Choose **Configuration > Network > Network Devices**.
- Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the group of wireless controllers that match the device you have selected to act as the secondary controller (for example: Cisco 5500 Series Wireless LAN Controllers). Members of this device group are displayed on the right.
- Step 4** Click on the **Device Name** of the secondary controller.
- Step 5** Click the **Configuration** tab.
- Step 6** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration page appears.
- Step 7** You must configure the following parameters before you enable the redundancy mode for the secondary controller:
- Redundancy-Management IP—Enter the IP address of the local physical management interface. This IP address must be the same as the IP address of the peer redundancy-management interface of the primary controller.
 - Peer Redundancy-Management IP—Enter the IP address of the peer physical management interface. This IP address must be the same as the IP address of the local physical management interface of the primary controller.
 - Redundant Unit—Choose **Secondary**.

- d. **Mobility MAC Address**—Enter the virtual MAC address of the redundancy pair. Ensure that the mobility MAC address that you enter is the same for both primary and secondary controllers.

Step 8 Click **Save**. The Enabled check box for the redundancy mode becomes available for editing.

Step 9 Select the **Enabled** check box for the redundancy mode to enable the redundancy on the secondary controller.

After you enable the redundancy, you cannot modify the Redundancy-Management IP, Peer Redundancy-Management IP, Redundant Unit, and Mobility MAC Address parameters.

You cannot configure the primary controller during the redundancy pair-up process.

Step 10 Click **Save**. The configuration is saved and the system reboots.

Monitor Redundancy States

After redundancy mode is enabled on the primary and secondary controllers, the system reboots. The redundancy state for both the controllers becomes Enabled in the Wireless Controller Members list page. The following traps are triggered:

- **RF_SWITCHOVER_ACTIVITY**—This trap is triggered when the standby controller becomes the new active controller.
- **RF_PROGRESSION_NOTIFY**—This trap is triggered by the primary or active controller when the peer state changes from Disabled to StandbyCold, and then to StandbyHot.
- **RF_HA_SUP_FAILURE_EVENT**—This trap is triggered when the redundancy fails because of a discrepancy between the active and the standby controllers.

For more information about these traps, see [Cisco Prime Infrastructure Alarms and Events](#).

You can view the redundancy state details, including the local and peer state, unit, IP addresses of the redundancy management, peer redundancy management, redundancy port, peer redundancy port, and peer service port of the paired controller.

To view these details, choose **Monitor > Managed Elements > Network Devices > Device Type > Wireless Controller > Controller Group > Controller > Device Details > Redundancy > Redundancy States**.

Configure Peer Service Port IPs and Subnet Mask

You can configure a peer service port IP address and a subnet mask only when the state of the peer controller is in StandbyHot. Ensure that DHCP is disabled on the local service port before you configure the peer service port IP address.

Step 1 Choose **Configuration > Network > Network Devices**.

Step 2 In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.

Step 3 Select the group of wireless controllers that contains the primary or active controller. Members of this device group are displayed on the right.

Step 4 Click on the Device Name of the primary or active controller.

Step 5 Click the **Configuration** tab.

- Step 6** From the left sidebar menu, choose me **Redundancy > Global Configuration**. The Global Configuration page appears.
- Step 7** Complete the following fields:
- Peer Service Port IP**—Enter the IP address of the peer service port.
 - Peer Service Netmask IP**—Enter the IP address of the peer service subnet mask.
- Step 8** Click **Save**.
-

Add Peer Network Routes

You can add a peer network route on an active controller only when the state of the peer controller is in StandbyHot. A new network route table is maintained. When the standby controller becomes active, the entries of the network route table swaps with the entries of the peer network route table.

- Step 1** Choose **Configuration > Network > Network Devices**.
- Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the group of wireless controllers that contains the controller for which you have configured the redundancy-management interface IP address. Members of this device group are displayed on the right.
- Step 4** Click the Device Name of the controller for which you have configured the redundancy-management interface IP address.
- Step 5** Click the **Configuration** tab.
- Step 6** From the left sidebar menu, choose **Redundancy > Peer Network Route > .**
- Step 7** Choose **Select a command > Add Peer Network Route > Go**. The Peer Network Route Details page appears.
- Step 8** Complete the following fields:
- IP Address**—Enter the IP address of the peer network route.
 - P Netmask**—Enter the subnet mask of the peer network route.
 - Gateway IP Address**—Enter the IP address of the peer network route gateway
- Step 9** Click **Save**. The peer network route is added.
-

Reset and Upload Files from the Secondary Server

You can reset the secondary server when the secondary server is in the StandbyHot state and the high-availability pairing process is complete. You can also upload the files from the secondary server to the primary server.

- Step 1** Choose **Configuration > Network > Network Devices**.
- Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.

- Step 3** Select the group of wireless controllers that contains the controller for which you have configured the redundancy-management interface IP address. Members of this device group are displayed on the right.
- Step 4** Click on the **Device Name** of the controller for which you have configured the redundancy-management interface IP address.
- Step 5** Click the **Configuration** tab.
- Step 6** From the left sidebar menu, choose **Redundancy > Redundancy Commands**.
- Step 7** Under **Administrative Commands**, choose **Select a command > Reset Standby > Go** to reset the secondary server.
- Step 8** Under **Upload/Download Commands**:
- Choose the transport protocol you want to use when uploading files from the secondary to the primary server (**TFTP** is the default).
 - Choose **Select a command > Upload File from Standby Controller > Go** to upload files from the secondary to the primary server.
-

Disable Redundancy on Controllers

When you disable redundancy on the controller, both active and standby controllers reboot. You must refresh the configuration from the device to remove any audit mismatches in the redundancy parameters. The active controller becomes a standalone controller and the standby controller reboots with all the ports disabled.

- Step 1** Choose **Configuration > Network > Network Devices**.
- Step 2** In the **Device Groups** area, expand **Device Type**, then expand **Wireless Controller**.
- Step 3** Select the group of wireless controllers that contains the controller on which you want to disable redundancy. Members of this device group are displayed on the right.
- Step 4** Click on the **Device Name** of the controller on which you want to disable redundancy.
- Step 5** Click the **Configuration** tab.
- Step 6** From the left sidebar menu, choose **Redundancy > Global Configuration**. The Global Configuration details page appears.
- Step 7** Unselect the **Enabled** check box for the **Redundancy Mode** on the selected controller.
- Step 8** Click **Save**. The configuration is saved and the system reboots.
-



CHAPTER 13

Manage Traffic Metrics

- [How to Manage Traffic Metrics](#), on page 327

How to Manage Traffic Metrics



Note The mediatrace feature has been deprecated from the latest IOS releases.

supports tracing Real-Time Transport Protocol (RTP) and TCP application traffic paths across endpoints and sites. Tracing data paths depends on Cisco Medianet and Web Services Management Agent (WSMA). Both are built-in features of Cisco IOS software and Catalyst switches that help isolate and troubleshoot problems with RTP and TCP data streams. supports all versions of Cisco Medianet and WSMA and makes it easy to enable them on any router.

Where Cisco Network Analysis Module (NAM) traffic monitoring data is not available, supports RTP service path tracing (Mediatrace) using Cisco Medianet Performance Monitor and Cisco IOS NetFlow. When properly configured, Mediatrace can be your most valuable tool when troubleshooting RTP and TCP application problems.

Related Topics

- [Prerequisites for Traffic Metrics With Mediatrace](#), on page 327
- [Configure Mediatrace on Routers and Switches](#), on page 329
- [Configure WSMA and HTTP\(S\) Features on Routers and Switches](#), on page 329

Prerequisites for Traffic Metrics With Mediatrace

Before you can use Mediatrace feature, you must complete the prerequisite setup tasks shown under Related Topics, below. These prerequisite tasks are required to enable Cisco routers (ISRs, ISR G2s, ASRs) and NAM devices to act as data (metrics collection) sources to monitor network traffic (RTP and TCP) performance metrics.

Related Topics

- [Configure to Use NAM Devices as Data Sources](#), on page 328
- [Configure to Use Routers and Switches as Data Sources](#), on page 328

Configure to Use NAM Devices as Data Sources

If your network uses Cisco NAMs to monitor network traffic, complete the following steps to trace service paths for both RTP and TCP traffic.

-
- Step 1** Add NAMs to the system. You can do this either automatically using Discovery, or manually using bulk import or the Device Work Center (see the section *Add and Organize Devices* in [Cisco Prime Infrastructure User Guide](#)).
- Step 2** Enable NAM Data collection. To do this:
- Choose **Services > Application Visibility & Control > Data Sources**.
 - In the NAM Data Collector section, select each NAM and click **Enable** to enable data collection on the selected NAMs (see the section *Enable NAM Data Collection* in [Cisco Prime Infrastructure User Guide](#)).
- Step 3** Create a site structure for your organization and assign your principal routers to the appropriate sites:
- Choose **Maps > Site Maps**.
 - Add one or more campuses, buildings, and floors.
- Step 4** Associate your sites with authorized data sources:
- Choose **Services > Application Visibility & Control > Data Deduplication**.
 - Click **Enable Data Deduplication**, then click **Apply**. You can then assign authoritative sources for ART, Traffic Analysis and Voice/Video data (see [Enable Data Deduplication, on page 135](#)).
- Step 5** Associate your sites with endpoint subnets:
- Choose **Services > Application Visibility & Control > Endpoint Association**.
 - Associate subnets with your sites. (see the section *Associate Endpoints with a Site* in [Cisco Prime Infrastructure User Guide](#)).
- If you fail to do this, the data collected for these endpoints will have their sites set to “Unassigned.”
- Step 6** Configure your routers for Mediatrace and WSMA (see the section *Troubleshoot RTP and TCP Flows Using Mediatrace* in [Cisco Prime Infrastructure User Guide](#)).
- For more details, see [Control System Jobs](#)”.
-

Configure to Use Routers and Switches as Data Sources

If your network uses Cisco routers and switches to monitor network traffic, complete the following steps to enable path tracing for both RTP and TCP flows.

-
- Step 1** Create a site structure for your organization and assign your principal routers to the appropriate sites:
- Choose **Maps > Site Maps**.
 - Add one or more campuses, buildings, and floors (for details, see the section *Work With Site Maps* in [Cisco Prime Infrastructure User Guide](#)).
- Step 2** Associate your sites with authorized data sources:
- Choose **Services > Application Visibility & Control > Data Deduplication**.
 - Click **Enable Data Deduplication**, then click **Apply**. You can then assign authoritative sources for ART, Traffic Analysis and Voice/Video data (see [Enable Data Deduplication, on page 135](#)).
- Step 3** Associate your sites with endpoint subnets:

- a) Choose **Services > Application Visibility & Control > Endpoint Association**.
- b) Associate subnets with your sites. (see the section *Associate Endpoints with a Site* in [Cisco Prime Infrastructure User Guide](#)).

If you fail to do this, by default the data collected for these endpoints will have their sites set to “Unassigned.”

- Step 4** Configure your compatible routers for Cisco Medianet Performance Monitor (see [Configure Mediatrace on Routers and Switches](#)).
- Step 5** Configure your routers for Mediatrace and WSMA (see the section *Troubleshoot RTP and TCP Flows Using Mediatrace* in [Cisco Prime Infrastructure User Guide](#)).

Related Topics

[Enable Data Deduplication](#), on page 135

Configure Mediatrace on Routers and Switches

supplies an out-of-the-box template that configures Mediatrace on routers and switches. You must apply this configuration to every router and switch that you want to include in your results whenever you are tracing service paths.

See [Deploying Templates](#) , to get a list of all the supported routers and switches for Mediatrace.

Before You Begin

You must complete the following tasks:

- Configuring to Use NAM Devices as Data Sources
- Configuring to Use Routers and Switches as Data Sources

To configure the Mediatrace-Responder-Configuration template, follow these steps:

-
- Step 1** Choose **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > Mediatrace -Responder-Configuration**.
- Step 2** Enter the required information for the template (see the [Field reference for the template](#)).
- Step 3** Click **Save as New Template** and give the new template a name and description. Click **Save**.
- Step 4** Click **Deploy** to deploy the new template .

For more details, see [Enabling NetFlow Data Collection](#), [Field Reference: Mediatrace-Responder-Configuration](#) and [Deploying Templates](#) .

Configure WSMA and HTTP(S) Features on Routers and Switches

To trace service path details, the Web Services Management Agent (WSMA) over HTTP protocol must run Mediatrace commands on your routers and switches. Configure this feature on the same set of routers and switches as you did when following the instructions in “Configure Mediatrace on Routers and Switches” (see Related Topics).

-
- Step 1** Choose **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI > HTTP-HTTPS Server and WSMA Configuration-IOS**.
- Step 2** Enter the required information for the template (see the [Field reference for the template](#).
Be sure to enable the HTTP protocol. WSMA over HTTPS is *not supported* in the current version of Prime Infrastructure.
- Step 3** Click **Save as New Template** and give the new template a name and description. Click **Save**.
- Step 4** Click **Deploy** to deploy the new template.
When adding a device to Prime Infrastructure, you must provide the HTTP user and password for the device.
For more details, see [Field Reference: HTTP-HTTPS Server and WSMA Configuration-IOS](#), [Deploying Templates](#) and [Add Devices to Prime Infrastructure](#) .

Related Topics

[Configure Mediatrace on Routers and Switches](#), on page 329



CHAPTER 14

Plan Network Capacity Changes

- [How to Plan the Network Capacity Changes, on page 331](#)

How to Plan the Network Capacity Changes

Cisco Prime Infrastructure with Assurance allows you to view and report a variety of key performance indicators that are critical for maintaining and improving your network's operational readiness and performance quality. This information is especially critical in adapting to ever increasing network loads.



Note To use the features described in this chapter, your Prime Infrastructure implementation must include Assurance licenses. These features are supported on ASR platforms only.

In the following workflow, we take the role of a network administrator who has just been told that a large staff expansion is planned for a branch office. This change will add more users to the branch LAN, many of whom will be using WAN applications. We want to monitor the branch's key interfaces for usage and traffic congestion, so we can see if more users on the branch LAN will mean degraded WAN application performance for those users. To be certain we have an adequate picture, we will need to look at both short- and long-term performance trends for all the WAN applications the branch uses.

Before You Begin

- Set up the **Top N WAN Interfaces by Utilization** dashlet:
 - Choose **Monitor > Monitoring Policies** and create an Interface Health template.
 - Choose **Inventory > Group Management > Port Groups**, select the interfaces and click **Add to Group**, then select **WAN Interfaces** as the group.
- Enable SNMP polling.

Step 1 Choose **Dashboard > Overview > General**.

Step 2 To view the usage statistics for the WAN interfaces on the routers connecting remote branches to the WAN, choose **Network Interface**

Step 3 If it is not already there, add the **Top N Interface Utilization** dashlet. For each interface, this dashlet shows the Device Name and IP of the device hosting the WAN interface, the interface name and speed, and Transmit/Receive maximum, average and last-pollled utilization.

- Step 4** To see the utilization statistics for the past month, click the **Clock** icon next to the **Top N Interface Utilization** dashlet title to change the **Time Frame** on the **Filters** line to **Past 4 Weeks**.
- Step 5** In the **Top N Interface Utilization** dashlet, find the WAN interface for the branch to which you are adding users.
- Step 6** In the **Interface** column, click the interface's name to display the **Dashboard > Performance > Interface** page for that interface. The page shows the following dashlets for this single interface:
- Interface Details
 - Interface Tx and Rx Utilization
 - Top N Applications
 - Top N Clients
 - Number of Clients Over Time
 - DSCP Classification
 - QoS Class Map Statistics
 - oS Class Map Statistics Trend
 - Top Application Traffic Over Time
- Step 7** Concentrate on the **Top Application Traffic Over Time** dashlet on this page. This dashlet gives a color-coded map of the top ten applications with the heaviest traffic over this interface.
- Step 8** To get a better idea of the longer-term performance trend, click the **Clock** icon next to the **Top Application Traffic Over Time** dashlet title to change the **Time Frame** to **Past 24 Hours**, **Past 4 Weeks**, or **Past 6 Months**.
- To zoom in on particular spikes in the graph, use the Pan and Zoom handles in the lower graph.
- Step 9** For a quick report of the same data as the interface page, choose **Reports > Report Launch Pad**. Then choose **Performance > Interface Summary**. Specify filter and other criteria for the report, select the same interface in Report Criteria, then click **Run**.

What to do next

The following table shows the ISP profile used to test against (it is very similar to the Caida.org Internet profile).

Table 19: Internet Profile - Traffic Profile per 1Gbps

	TCP	UDP	HTTP	RTP	Total
Connection Rate (flows per second)	5,000	5,000	800	10	10,000
Concurrent Flows	150,000	150,000	50,000	300	300,000
Packet Rate	150,000	40,000	50,000	15,000	199,000
Related Bandwidth (bps)	900Mbps	100Mbps	295Mbps	25Mbps	1GBps
Packet Size (derived)	750	313	738	208	658

	TCP	UDP	HTTP	RTP	Total
Number of Parallel Active Users	60,000	Derived from the number of flows			



APPENDIX **A**

Best Practices: Server Security Hardening

The following sections explain how to enhance server security by eliminating or controlling individual points of security exposure.

- [Disable Insecure Services](#) , on page 335
- [Disable Root Access](#), on page 335
- [Use SNMPv3 Instead of SNMPv2](#), on page 336
- [Authenticate With External AAA](#), on page 338
- [Enable NTP Update Authentication](#), on page 339
- [Enable OCSP Settings on the Prime Infrastructure Server](#), on page 340
- [Set Up Local Password Policies](#), on page 340
- [Disable Individual TCP/UDP Ports](#), on page 341
- [Check On Server Security Status](#), on page 342

Disable Insecure Services

You should disable non-secure services if you are not using them. For example: TFTP and FTP are not secure protocols. These services are typically used to transfer firmware or software images to and from network devices and Prime Infrastructure. They are also used for transferring system backups to external storage. We recommend that you use secure protocols (such as SFTP or SCP) for such services.

To disable FTP and TFTP services:

-
- Step 1** Log in to Prime Infrastructure with a user ID with administrator privileges.
 - Step 2** Select **Administration > Settings > System Settings > General > Server**.
 - Step 3** Select the Disable buttons for FTP and TFTP.
 - Step 4** Restart Prime Infrastructure to apply the updated settings.
-

Disable Root Access

Administrative users can enable root shell access to the underlying operating system for trouble shooting purposes. This access is intended for Cisco Support teams to debug product-related operational issues. We

recommend that you keep this access disabled, and enable it only when required. To disable root access, run the command **root_disable** from the command line (see [How to Connect Via CLI, on page 111](#)).

During installation, Prime Infrastructure also creates a web root user account, prompting the installer for the password to be used for this account. The web root account is needed to enable first-time login to the Prime Infrastructure server and its web user interface. We recommend that you never use this account for normal operations. Instead, use it to create user IDs with appropriate privileges for day-to-day operations and network management, and administrative user IDs for managing Prime Infrastructure itself. Once these user accounts are created, disable the default “web root” account created at install time, and create user accounts using your administrative user IDs thereafter.

If you forget the shell password, you can recover (and then reset) the shell password by following the steps to recover the administrator password. See [Recovering Administrator Passwords on Virtual Appliances](#). Because recovering the administrator password requires the Prime Infrastructure server to reboot, your system might go down for approximately 20 minutes.

To disable the root accounts:

-
- Step 1** Open a CLI session with the Prime Infrastructure server (see [How to Connect Via CLI, on page 111](#)). Do not enter “configure terminal” mode.
- Step 2** Disable the web root account by entering the following command:
- ```
PIServer/admin# ncs webroot disable
```
- Prime Infrastructure disables the web root account.
- Step 3** Disable the root shell account by entering the following command at the prompt:
- ```
PIServer/admin# shell disable
```
- Prime Infrastructure will prompt you for the root shell account password. Enter it to complete disabling of the root shell account.
-

Use SNMPv3 Instead of SNMPv2

SNMPv3 is a higher-security protocol than SNMPv2. You can enhance the security of communications between your network devices and the Prime Infrastructure server by configuring the managed devices so that management takes place using SNMPv3 instead of SNMPv2.

You can choose to enable SNMPv3 when adding new devices, when importing devices in bulk, or as part of device discovery. See [Related Topics](#) for instruction on how to perform each task.

Related Topics

- [Use SNMPv3 to Add Devices](#), on page 336
- [Use SNMPv3 to Import Devices](#), on page 337
- [Use SNMPv3 to Run Discovery](#), on page 337

Use SNMPv3 to Add Devices

To specify SNMPv3 when adding a new device:

-
- Step 1** Select **Inventory > Device Management > Network Devices**
 - Step 2** Choose **Add Device**.
 - Step 3** In the SNMP Parameters area, in Version, select v3.
 - Step 4** Complete the other fields as appropriate, then click **Add**.

Related Topics

- [Use SNMPv3 to Import Devices](#), on page 337
- [Use SNMPv3 to Run Discovery](#), on page 337
- [Use SNMPv3 Instead of SNMPv2](#), on page 336

Use SNMPv3 to Import Devices

To specify use of SNMPv3 when importing devices in bulk:

-
- Step 1** Select **Inventory > Device Management > Network Devices**.
 - Step 2** Choose Bulk Import. The Bulk Import page appears.
 - Step 3** Download the device add sample template from the “here” link on the Bulk Import page.
 - Step 4** Edit the template file using any CSV-compatible application. For each row representing a device in the CSV import file:
 - a) In the snmp version column, enter 3.
 - b) Enter appropriate values in the snmpv3_user_name, snmpv3_auth_type, snmpv3_auth_password, snmpv3_privacy_type, and snmpv3_privacy_password columns.
 - c) Complete other columns as appropriate for your devices.
 - Step 5** Select **Inventory > Device Management > Network Devices**, then click Bulk Import and import your modified CSV file.

Related Topics

- [Use SNMPv3 to Add Devices](#), on page 336
- [Use SNMPv3 to Run Discovery](#), on page 337
- [Use SNMPv3 Instead of SNMPv2](#), on page 336

Use SNMPv3 to Run Discovery

To specify SNMPv3 as part of device discovery:

-
- Step 1** Select **Inventory > Device Management > Discovery**. The Discovery Jobs page appears.
 - Step 2** Click the Discovery Settings link in the upper right corner of the page. The Discovery Settings page appears.
 - Step 3** Choose **New** to add new SNMP v3 credentials.
 - Step 4** Complete the fields as needed.
 - Step 5** Click **Save** to save the SNMPv3 settings and use them thereafter.
-

Related Topics

- [Use SNMPv3 to Add Devices](#), on page 336
- [Use SNMPv3 to Import Devices](#), on page 337
- [Use SNMPv3 Instead of SNMPv2](#), on page 336

Authenticate With External AAA

User accounts and password are managed more securely when they are managed centrally, by a dedicated, remote authentication server running a secure authentication protocol such as RADIUS or TACACS+.

You can configure Prime Infrastructure to authenticate users using external AAA servers. You will need to access the **Administration > Users > Users, Roles & AAA** page to set up external authentication via the Prime Infrastructure graphic user interface (GUI). You can also set up external authentication via the command line interface (CLI). See Related Topics for instructions on how to set up AAA using each method.

Related Topics

- [Set Up External AAA Via GUI](#), on page 338
- [Set Up External AAA Via CLI](#), on page 338

Set Up External AAA Via GUI

To set up remote user authentication via the GUI:

-
- Step 1** Log in to Prime Infrastructure with a user ID that has administrator privileges.
 - Step 2** Select **Administration > Users > Users, Roles & AAA > TACACS+ or Administration > Users > Users, Roles & AAA > RADIUS**.
 - Step 3** Enter the TACACS+ or RADIUS server IP address and shared secret in the appropriate fields.
 - Step 4** Select **Administration > Users > Users, Roles & AAA > AAA Mode Settings**.
 - Step 5** Set the AAA mode as appropriate.
-

Related Topics

- [Authenticate With External AAA](#), on page 338
- [Set Up External AAA Via CLI](#), on page 338

Set Up External AAA Via CLI

To set up remote user authentication via the CLI:

-
- Step 1** Log in to Prime Infrastructure using the command line, as explained in [How to Connect Via CLI, on page 111](#) . Be sure to enter “configure terminal” mode.
 - Step 2** At the prompt, enter the following command to setup an external TACACS+ server:

```
PIServer/admin/terminal# aaa authentication tacacs+ server tacacs-ip key plain shared-secret
```

 Where:

- `tacacs-ip` is the IP address of an active TACACS+ server.
- `shared-secret` is the plain-text shared secret for the active TACACS+ server.

Step 3 At the prompt, enter the following command to create a user with administrative authority, who will be authenticated by the above AAA server:

```
PIServer/admin/terminal# username username password remote role admin email emailID
```

Where:

- `username` is the name of the user ID.
- `password` is the plain-text password for the user.
- `emailID` is the email address of the user (optional).

Related Topics

[Authenticate With External AAA](#), on page 338

[Set Up External AAA Via GUI](#), on page 338

Enable NTP Update Authentication

Network Time Protocol (NTP) version 4, which authenticates server date and time updates, is an important way to harden server security. Note that you can configure a maximum of three NTP servers with Prime Infrastructure.

To set up authenticated NTP updates:

Step 1 Log in to Prime Infrastructure using the command line, as explained in [How to Connect Via CLI, on page 111](#). Be sure to enter “configure terminal” mode.

Step 2 At the prompt, enter the following command to setup an external NTPv4 server:

```
PIServer/admin/terminal# ntp server serverIP userID plain password
```

Where:

- `serverIP` is the IP address of the authenticating NTPv4 server you want to use.
- `userID` is the md5 key id of the NTPv4 server.
- `password` is the corresponding plain-text md5 password for the NTPv4 server.

For example: `ntp server 10.81.254.131 20 plain MyPassword`

Step 3 To ensure that NTP authentication is working correctly, test it by executing the following commands:

- To check the NTP update details: `sh run`
- To check NTP sync details: `sh ntp`

Enable OCSP Settings on the Prime Infrastructure Server

Online Certificate Status Protocol (OCSP) enables certificate-based authentication for web clients using OCSP responders. Typically, the OCSP responder's URL is read from the certificate's Authority Information Access (AIA). As a failover mechanism, you can configure the same URL on the Prime Infrastructure server as well.

To set up a custom URL of an OCSP responder, follow the steps below.

Step 1 Log in to the Prime Infrastructure server using the command line, as explained in [How to Connect Via CLI, on page 111](#). Do not enter "configure terminal" mode.

Step 2 At the prompt, enter the following command to enable client certificate authentication:

```
PIServer/admin# ocspp responder custom enable
```

Step 3 At the prompt, enter the following command to set the custom OCSP responder URL:

```
PIServer/admin# ocspp responder set url Responder#URL
```

Where:

- *Responder#* is the number of the OCSP responder you want to define (e.g., 1 or 2).
- *URL* is the URL of the OCSP responder, as taken from the client CA certificate.

Note that there should be no space between the *Responder#* and *URL* values.

Step 4 To delete an existing custom OCSP responder defined on the Prime Infrastructure server, use the following command:

```
PIServer/admin# ocspp responder clear url Responder#
```

If you do not already know the number of the OCSP responder you want to delete, use the **show security-status** command to view the OCSP responders currently configured on the server. For details, see [Check On Server Security Status, on page 342](#).

Set Up Local Password Policies

If you are authenticating users locally, using Prime Infrastructure's own internal authentication, you can enhance your system's security by enforcing rules for strong password selection.

Note that these policies affect only the passwords for local Prime Infrastructure user IDs. If you are authenticating Prime Infrastructure users via a centralized or remote AAA server, you can enforce similar protections using the functions of the AAA server.

To enforce local password policies:

Step 1 Log in to Prime Infrastructure with a user ID that has administrator privileges.

Step 2 Select **Administration > Users > Users, Roles & AAA > Local Password Policy**.

Step 3 Select the check boxes next to the password policies you want to enforce, including:

- The minimum number of characters passwords must contain.
- No use of the username or “cisco” as a password (or common permutations of these).
- No use of “public” in root passwords.
- No more than three consecutive repetitions of any password character.
- Passwords must contain at least one character from three of the following character classes: upper case, lower case, digit, and special character.
- Whether the password must contain only ASCII characters.
- Minimum elapsed number of days before a password can be reused.
- Password expiration period.
- Advance warnings for password expirations.

If you enable any of the following password policies, you can also specify:

- The minimum password length, in number of characters.
- The minimum elapsed time between password re-uses.
- The password expiry period.
- The number of days in advance to start warning users about future password expiration.

Step 4 Click **Save**.

Disable Individual TCP/UDP Ports

The following table lists the TCP and UDP ports Prime Infrastructure uses, the names of the services communicating over these ports, and the product’s purpose in using them. The “Safe” column indicates whether you can disable a port and service without affecting Prime Infrastructure’s functionality.

Table 20: Prime Infrastructure TCP/UDP Ports

Port	Service Name	Purpose	Safe?
21/tcp	FTP	File transfer between devices and server	Y
22/tcp	SSHD	Used by SCP, SFTP, and SSH connections to and from the system	N
69/udp	TFTP	File transfer between devices and the server	Y
80/tcp	HTTP	Provisioning of Nexus devices	Y
162/udp	SNMP-TRAP	To receive SNMP Traps	N
443/tcp	HTTPS	Primary Web Interface to the product	N
514/udp	SYSLOG	To receive Syslog messages	N

Port	Service Name	Purpose	Safe?
1522/tcp	Oracle	Oracle/JDBC Database connections: These include both internal server connections and for connections with the High Availability peer server.	N
8082/tcp	HTTPS	Health Monitoring	N
8087/tcp	HTTPS	Software updates on HA Secondary Systems	N
9991/udp	NETFLOW	To receive Netflow streams (enabled if Assurance license installed)	N
9992/tcp	PI Tomcat Process	Lync Monitoring in Assurance	N
61617/tcp	JMS (over SSL)	For interaction with remote Plug&Play Gateway server	Y

Check On Server Security Status

Prime Infrastructure administrators can connect to the server via CLI and use the **show security-status** command to display the server's currently open TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. For example:

Step 1 Log in to Prime Infrastructure using the command line, as explained in Connecting Via CLI . Do not enter “configure terminal” mode.

Step 2 Enter the following command at the prompt:

```
PIServer/admin# show security-status
```

Depending on your settings, you will see output like the following:

```
Open TCP Ports : 21 22 80 443 1522 8082 9992 11011:11014 61617
```

```
Open UDP Ports : 69 162 514 9991
```

```
FIPS Mode : disabled
```

```
TFTP Service : enabled
```

```
FTP Service : enabled
```

```
JMS port (61617) : enabled
```

```
Root Access : disabled
```

```
Client Auth : enabled
```

```
OCSP Responder1 : http://10.77.167.65/ocsp
```

```
OCSP Responder2 : http://10.104.178.99/ocsp
```



APPENDIX **B**

Internal SNMP Trap Generation

- [About Internal Trap Generation, on page 343](#)
- [Prime Infrastructure SNMP Trap Types, on page 344](#)
- [Generic SNMP Trap Format, on page 346](#)
- [Northbound SNMP Trap-to-Alarm Mappings, on page 347](#)
- [Prime Infrastructure SNMP Trap Reference, on page 350](#)
- [Configure Prime Infrastructure Traps , on page 355](#)

About Internal Trap Generation

When properly configured, Prime Infrastructure will send SNMP traps to notification destination, to notify them on the following events, occurring within the Prime Infrastructure system itself:

- Any crash or failure of an internal software process on the Prime Infrastructure server.
- High Availability (HA) state changes, including Registration, Failover, and Failback.
- High CPU, memory or disk utilization.
- CPU, disk, fan, or Power Supply Unit (PSU) failures.
- Backup failure, certification expiry and licenses violations.

You can edit the severity associated with each of these internal SNMP traps. You can also change the threshold limits on CPU, memory and disk utilization traps (these SNMP traps are sent when the system hardware exceeds the configured thresholds).

For other events (such as CPU, disk, fan, and PSU failures, or HA state changes), an SNMP trap is sent as soon as the failure or HA state-change is detected.

SNMP traps are generated based on customized threshold and severities for the following:

- Server Process Failures
- High Availability Operations
- CPU Utilization
- Memory Utilization
- Disk Utilization
- Disk Failure
- Fan Failure
- PSU Failure
- Backup Failure

- Certificate Expiry

Prime Infrastructure does not send SNMPv2 Inform or SNMPv3 notifications.

Prime Infrastructure SNMP Trap Types

The following table lists the SNMP traps that Prime Infrastructure generates for its own functions. The listing is by trap type. The table describes the circumstances under which each trap is generated as well as suggested operational responses (where applicable).

Table 21: Prime Infrastructure SNMP Trap Types

Trap Type	Trap	Description
Appliance Process Failure	FTP, MATLAB, TFTP	Whenever the FTP, MATLAB, or TFTP process on Prime Infrastructure server fails, the server will generate a failure trap and the server's instance of Health Monitor will try to restart the process automatically. If Health Monitor cannot restart it after 3 tries, the HA server will send another failure trap.
Appliance Process Failure	NMS	Whenever the NMS process on a server starts or fails, the Prime Infrastructure server's Health Monitor thread will generate a corresponding trap. To stop or restart the process, connect to the server via CLI and log in as admin. Then execute the nms stop or nms start command, as appropriate.
HA Operations	Registration Trigger	Prime Infrastructure generates this trap whenever the primary server initiates HA registration (whether registration fails or succeeds). Once HA registration is triggered, the primary server generates the trap, indicating the start of the operation.
HA Operations	Registration Success	When HA registration is successful, the primary server generates this trap, indicating success.
HA Operations	Registration Failure	When HA registration fails for any reason, the primary or secondary server on which the failure occurred, generates a trap indicating the failure. The trap contains details about the failure. For assistance, contact the Cisco Technical Assistance Center (TAC).
HA Operations	Failover Trigger	This trap is generated whenever the Prime Infrastructure primary server fails and, as part of a failover, the secondary server tries to become active (whether failover fails or succeeds, and whether the secondary server comes up or fails to do so). If the HA configuration (set during registration) has a Manual failover type, users must trigger the failover. Otherwise, the Health Monitor will trigger failover to the secondary server automatically. One trap will be generated to indicate that the failover was triggered. Because the trap is sent before the failover completes, it will not be logged on the secondary server.
HA Operations	Failover Success	When the triggered failover operation is successful, the secondary server generates a trap indicating success. Users can view the trap in the secondary server's alarm browser.

Trap Type	Trap	Description
HA Operations	Failover Failure	When the triggered failover operation fails, a trap will be generated indicating the failure. Users can view the trap in the hm-#-#.log (see How to Troubleshoot Prime Infrastructure SNMP Traps, on page 360). The trap contains details about the failure. For assistance, contact Cisco TAC. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.
HA Operations	Failback Trigger	This trap is generated whenever a failback to the primary server is triggered on the secondary server (whether or not the failback is successful). Once the primary server is restored, a user must trigger a failback from the secondary server to the primary server using the Failback button on the secondary server Health Monitor web page (there is no automatic Failback option). Once triggered, the secondary server generates the trap indicating the start of the operation.
HA Operations	Failback Success	When the triggered failback operation is successful, the secondary server generates a trap indicating success. Failback success sets the primary server to the ‘Active’ state and the secondary server to the ‘Sync’ state.
HA Operations	Failback Failure	When the triggered failback operation fails, a trap will be generated indicating this failure. Since the failure can occur on either server, the server on which it occurred will generate the trap. Users can view the trap in the hm-#-#.log and on the northbound management server. A failback failure triggers an automatic rollback, in which the secondary server tries to return to its previous ‘Active’ state. Failure of this operation will cause the secondary server to generate an additional trap indicating rollback failure. The failure traps contain details about the failures. For assistance, contact Cisco TAC. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.
Hardware Traps	CPU Utilization	Traps will be sent only when the usage exceeds the preset threshold value for CPU utilization. To view these traps, check the jobs and active sessions for the server that generated the trap.
Hardware Traps	Disk Utilization	Traps will be sent only when the disk usage exceeds the set threshold limit for Disk utilization. To respond, try to free up disk space under the /opt and /localdisk partitions. Do not delete folders under /opt/CSCOLumos without guidance from Cisco TAC.
Hardware Traps	Memory Utilization	Traps will be sent to the SNMP trap receiver, only when memory usage exceeds the set threshold limit for memory utilization.
Hardware Traps	Disk Failure	Traps will be sent to the SNMP trap receiver when disk failure is detected. Contact your local system administrator for corrective action. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.
Hardware Traps	Fan Failure	Traps will be sent to the SNMP trap receiver when fan failure is detected. The bad or missing fan will be identified in the trap or alarm message. Contact your local system administrator for corrective action. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.
Hardware Traps	PSU Failure	Traps will be sent to the SNMP trap receiver when PSU failure is detected. The problematic power supply will be identified in the trap or alarm message. Contact your local system administrator for corrective action. As with other failure traps, alarms and a “clear” trap are sent if the failure corrects itself.

Trap Type	Trap	Description
Threshold Traps	Backup Failure	Traps will be sent to the SNMP trap receiver when failure of the daily background task of Prime Infrastructure server backup is detected. The background task runs everyday and takes a backup of the server at the scheduled time. If the backup fails due to insufficient disk space, the event will be processed. If the backup is taken successfully, the alarm will be cleared.
Threshold Traps	Backup Threshold	Informs users when Prime Infrastructure scheduled daily backup has not been taken for a threshold number of days. The default threshold is seven days. If no backup has been taken for seven days, users are notified by this event.
Threshold Traps	Certificate Expiry	Traps will be sent to the SNMP trap receiver when the certificate is about to expire. A critical trap is sent when the certificate is set to expire in 15 days and a major trap is sent when the certificate expiry is in 60 days.
System Traps	Lifecycle	Lifecycle license is used to manage devices. Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.
System Traps	Assurance	Assurance License is used to display the devices that pump NetFlow to Prime Infrastructure. Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.
System Traps	Collector	Collector License is used to display the volume of NetFlow pumped to Prime Infrastructure. Alarm is generated when the license usage exceeds the configured threshold percentage. By default, traps will be sent when the usage exceeds 80%. However, this can be customized.
System Traps	Lifecycle License	Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License.
System Traps	Assurance License	Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License.
System Traps	Collector License	Traps will be sent when the expiry period of the License goes below the threshold limit. By default, traps will be sent when the limit is 30 days. However, you can customize the limit between 1-99 days. This event is considered only when you use Evaluation License.

Generic SNMP Trap Format

The following shows the syntax of SNMP trap notifications for Prime Infrastructure:

Component: Component Name, **Server:** Primary, Secondary or Standalone, **Type:** Process, Sync, Activity, etc., **Service:** Service Name, **When:** Phase in the Prime Infrastructure Lifecycle, **State:** HA and HM state of

the server, **Result:** Warning, Failure, Success, Information, Exception, **MSG:** Free-form text of the message for a given SNMP Trap

Table A-2 describes possible values for each of the generic trap format attributes.

Table 22: Values for Generic SNMP Trap Format Attributes

Attribute	Value
Component	Health Monitor or High Availability
Server	From which server (Primary, Secondary or Standalone) was this trap sent?
Type	Which type of action (Process, Sync, Activity, etc.) resulted in this trap?
Service	Which Prime Infrastructure service reported this issue? The possible values include Registration, Failover, Failback, NMS, NCS, Health Monitor, All, Prime Infrastructure, Database, Disk Space, and so on.
When	At what point in the Prime Infrastructure server's life cycle (Startup, Shutdown, etc.) did this happen?
State	What is the server state (Standalone, Failover, Failback, Registration, etc.)?
Result	For which condition is this SNMP trap being reported?
MSG	Freeform text providing more details specific to each SNMP trap.

Northbound SNMP Trap-to-Alarm Mappings

The following table describes how northbound traps are mapped to Prime Infrastructure events and alarms. The entries in the “Events” column in the table below refer to the names of columns in the “Events” tab of the Prime Infrastructure Supported Events document that contain additional information. For example, for the MIB variable “cWNotificationSubCategory” in this table, you would look in the “Event/Alarm Condition” column of the *Supported Events* document to look up the type of problem being reported or resolved in the forwarded event or alarm.

Table 23: Northbound SNMP Trap-to-Alarm Mappings

MIB Variable Name	Field From Associated Alarm	GUI Name	Events	Details
cWNotificationIndex	None. Uniquely generated for each trap.	None	None	Index value that increases with each northbound trap sent until it wraps back to one.
cWNotificationTimestamp	alarmCreationTime	Alarm Found At	None	Time that the associated alarm was created.
cWNotificationUpdatedTimestamp	lastModifiedTimestamp	Timestamp (column), Alarm Last Updated At	None	Time that the associated alarm was last updated.

MIB Variable Name	Field From Associated Alarm	GUI Name	Events	Details
cWNotificationKey	applicationSpecificAlarmID	None	None	An (opaque) string that uniquely identifies the alarm condition. This is basically the alarm “identifier”. If two northbound traps are received (first one with non-cleared severity, second one with cleared severity) with the same cWNotificationKey, it can be determined that the second trap clears issue reported in the first.
cWNotificationCategory	category	Category	Default Category	Category of the associated alarm. The actual value is a numeric and can be mapped to the actual category name contained in the <i>Prime Infrastructure Supported Events</i> document. The mapping is available in the MIB.
cWNotificationSubCategory	eventType	Condition	Event/Alarm Condition	Indication of the type of problem being reported or resolved.
cWNotificationObjectAddressType	None	None	None	Indicates IPV4.
cWNotificationObjectAddress	reportingEntityAddress	None	None	Address of device reporting the issue. May not be the actual address the trap was sent from. If a device is added to Prime Infrastructure with one address as its management address but sends traps from a different address, this value will be the address the device had when it was added.
cWNotificationSourceDisplayName	displayName	Failure Source	None	A representation of the name of the affected resource.

MIB Variable Name	Field From Associated Alarm	GUI Name	Events	Details
cWNotificationDescription	description (ciscoLwappIpsType, ciscoLwappIpsDescId, ciscoLwappIpsDescriptionParams)	Message	Prime Infrastructure Message	A message indicating the issue or resolution that occurred. This usually comes from the alarm description, but in the case of WIPS alarms, it is pulled from other fields (see the “Field from Associated Alarm” column at left).
cWNotificationSeverity	severity	Severity	Default Severity	The severity of the alarm. This is a numerical representation of the alarm severity defined in the CISCO-TC MIB. The values are: cleared(1), indeterminate(2), critical(3), major(4), minor(5), warning(6), info(7). Since you can change the desired severity for an event type, the value may not match the severity in <i>Prime Infrastructure Supported Events</i> if the severity has been modified. Severity can be modified as a way to control which alarm changes are notified via northbound traps (that is, you could specify only CRITICAL alarms should become northbound traps, and change the severity for an unwanted alarm from CRITICAL to MAJOR).
cWNotificationSpecialAttributes	All alarm fields	Various, based on specific alarm field	Various, based on specific alarm field	Contains the contents of the alarm itself (fields and values)

MIB Variable Name	Field From Associated Alarm	GUI Name	Events	Details
cWNotificationType	None	None	None	Indication if trap is based on alarm creation/update or event creation. Since some events (if severity is Informational) do not create alarms, it is possible to get north bound traps for these informational events.
cWNotificationVirtualDomains	None	None	None	From the MIB: "This object represents the name of one or multiple virtual domains (comma separated) the source of the network condition represented by cWNotificationType is logically assigned to". For example, "root, California, San Jose" indicates that the source of the network condition is logically assigned to these multiple virtual domains.

Prime Infrastructure SNMP Trap Reference

The tables below provide details for each class of SNMP trap notification generated in Prime Infrastructure. The mapped OID for the WCS northbound notification MIB is 1.3.6.1.4.1.9.9.712.1.1.2.1.12. This OID is referenced by Prime Infrastructure's software- and hardware-related traps. The trap OID for the northbound MIB will always be 1.3.6.1.4.1.9.9.712.0.1. For more details, consult the listing for CISCO-WIRELESS-NOTIFICATION-MIB and the related topic, Northbound SNMP Trap-to-Alarm Mappings

Table 24: Appliance Process Failure

Purpose	Informs users that a specific Prime Infrastructure server service is down and that the Health Monitor is attempting to restart it.
When Sent	The trap is sent when Health Monitor tries to restart the process.
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12

Example	Component: Health Monitor, Server: Primary, Type: Process, Service: NCS, When: Startup, State: Stand Alone, Result: Warning, MSG: FTP service is down and an attempt will be made to automatically restart the service
MSG Content	PI servername : serviceName service is down; an attempt will be made to automatically restart the service.
Value Type, Range and Constraints	The servername parameter in the MSG attribute will take the value of the Prime Infrastructure server's host name. This parameter can take one of the following values: NMS Server, FTP, TFTP or MATLAB.

Table 25: Failback

Purpose	Informs users that a failback from the secondary server to the primary server has been initiated.
When Sent	This trap is sent when a failback is initiated from the secondary server to the primary server, irrespective of whether the failback operation fails or succeeds.
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
Example	Component: High Availability, Server: Secondary, Type: Process, Service: Database, When: Failback, State: Primary Failback, Result: Failure, MSG: Error in Failback: Failed to recover the primary database using Duplicate DB.

Table 26: Failover

Purpose	Informs users when the secondary server comes up.
When Sent	When the primary server is down and, as part of failover, the secondary server comes up, traps are generated, irrespective of whether the failover operation fails or succeeds.
OID	1.3.6.1.4.1.9.9.712.1.1.2.1.12
Example	Component: High Availability, Server: Secondary, Type: Process, Service: Failover, When: Failover, State: Secondary Syncing, Result: Success, MSG: Completed failover from primaryAddressInfo to secondaryAddressInfo.
MSG Content	The primaryAddressInfo and secondaryAddressInfo in the MSG attribute will take the IP address or host name of the servers.

Table 27: CPU Utilization

Purpose	Informs users that CPU utilization has crossed the set threshold limit.
---------	---

When Sent	After the CPU utilization crosses the set threshold, the trap is generated on the next polling cycle. The system poller job runs every 5 minutes. A trap is also generated when the threshold limit is changed on the Prime Infrastructure Event Configuration web page.
OID	.1.3.6.1.4.1.9.9.712.0.1.
Example	CPU Utilization is at 85% and has violated threshold limit of 80%.
Value Type, Range and Constraints	All percentage ranges are from 1 to 99. Do not enter the percentage character ("%") when specifying a threshold limit.
Wire Format	[OctetString] applicationSpecificAlarmID=Appliance_CPU, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=8178170, severity=4, eventType=APPLIANCE_CPU_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=CPU, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: CPU Utilization is at 3% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle.

Table 28: Disk Utilization

Purpose	Informs users that disk utilization has crossed the set threshold limit.
When Sent	After the disk utilization crosses the set threshold, the trap is generated on the next polling cycle. The system poller job runs every 5 minutes. A trap is also generated when the threshold limit is changed on the Prime Infrastructure Event Configuration web page.
OID	.1.3.6.1.4.1.9.9.712.0.1
Examples	PI opt disk volume utilization is at 85% and has violated threshold limit of 0%. PI opt disk volume is within the recommended disk usage range, less than 80% used. PI local disk volume utilization is at 85% and has violated threshold limit of 80%. PI local disk volume is within the recommended disk usage range, less than 80% used.
Value Type, Range and Constraints	All percentage ranges are from 1 to 99. Do not enter the percentage character ("%") when specifying a threshold limit.
Wire Format	[OctetString] applicationSpecificAlarmID=LocaldiskDiskSpace, reportingEntityAddress=10.77.240.246, lastModifiedTimestamp=Sun Mar 23 08:44:06 UTC 2014, alarmCreationTime=2014-03-14 13:29:31.069, eventCount=1, mayBeAutoCleared=false, instanceId=483484, severity=1, eventType=NCS_LOW_DISK_SPACE, authEntityId=93093, previousSeverity=MAJOR, category=System(17), transientNameValue={}, source=10.77.240.246, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=PI localdisk volume is within the recommended disk usage range, less than 70% used., isAcknowledged=false, authEntityClass=983576643, displayName=NCS 10.77.240.246
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle.

Table 29: Memory Utilization

Purpose	Informs users that memory utilization has crossed the set threshold limit.
When Sent	After the memory utilization crosses the set threshold, the trap is generated on the next polling cycle. The system poller job runs every 5 minutes. A trap is also generated when the threshold limit is changed on the Prime Infrastructure Event Configuration web page.
OID	.1.3.6.1.4.1.9.9.712.0.1.
Examples	Memory Utilization is at 85% and has violated threshold limit of 80%.
Value Type, Range and Constraints	All percentage ranges are from 1 to 99. Do not enter the percentage character ("%") when specifying a threshold limit.
Wire Format	[OctetString] applicationSpecificAlarmID=Appliance_MEMORY, lastModifiedTimestamp=12 Jun 2014 11:12:32 UTC, alarmCreationTime=12 Jun 2014 11:12:32 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=8178171, severity=4, eventType=APPLIANCE_MEM_VIOLATED_THRESHOLD, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=MEMORY, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: primary, Type: Hardware, Message: MEMORY Utilization is at 38% and has violated threshold limit of 1%, isAcknowledged=false, displayName=NMS:192.168.115.141
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle.

Table 30: Disk Failure

Purpose	Informs users that a drive is missing or bad.
When Sent	Once a disk drive issue is detected, a trap will be generated on the next polling cycle. The system poller job runs every 5 minutes.
OID	.1.3.6.1.4.1.9.9.712.0.1
Example	Component: Appliance, Server: Standalone, Type: Hardware, Message: A problem was detected in the RAID device. A rebuild is in progress. Device at enclosure 252 slot ZERO is bad or missing. Drive0 is missing or bad.
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle. If the drive is unplugged at the time of system restart, the trap is generated.

Table 31: Fan Failure

Purpose	Informs users when a fan fails.
When Sent	When a fan fails, a trap is generated on the next polling cycle. The system poller job runs every 5 minutes.
OID	.1.3.6.1.4.1.9.9.712.0.1
Example	Fan is either bad or missing.

Wire Format	[OctetString] applicationSpecificAlarmID=Appliance_Fan1, lastModifiedTimestamp=Sun Apr 13 15:24:11 IST 2014, alarmCreationTime=Sun Apr 13 15:24:11 IST 2014, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=2875873, severity=4, eventType=APPLIANCE_FAN_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=Fan1, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Fan is either bad or missing, isAcknowledged=false, displayName=NMS:10.77.240.246
Constraints and Caveats	Traps are not generated if the issue is resolved before the next polling cycle, or the fan is unplugged at the time of system restart.

Table 32: PSU Failure

Purpose	Informs users that a power supply unit is unplugged.
When Sent	When a power supply is unplugged, a trap is generated on the next polling cycle. The system poller job runs every 5 minutes.
OID	.1.3.6.1.4.1.9.9.712.0.1
Example	Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing.
Wire Format	[OctetString] applicationSpecificAlarmID=Appliance_PS1, lastModifiedTimestamp=19 Aug 2015 01:41:26 UTC, alarmCreationTime=19 Aug 2015 01:41:26 UTC, ownerID=, eventCount=1, mayBeAutoCleared=false, instanceId=1424089, severity=4, eventType=APPLIANCE_POWER_SUPPLY_BAD_OR_MISSING, previousSeverity=CLEARED, category=System(17), transientNameValue={}, source=x.x.x.x, notificationDeliveryMechanism=SYNTHETIC_EVENT, instanceVersion=0, description=Component: Appliance, Server: Standalone, Type: Hardware, Message: Power supply: PSx is either bad or missing, isAcknowledged=false, displayName=NMS:x.x.x.x
Constraints and Caveats	If the PSU is unplugged, a Power Supply alarm will be seen in Prime Infrastructure and a trap will be sent. If the PSU is unplugged at the time of system shutdown, and Prime Infrastructure is not up till restart, an alarm will not be generated.

Table 33: Identify Services Engine down

Purpose	Informs users when an ISE is unreachable.
When Sent	When an ISE is down or unreachable, the trap is generated via polling. Note This is a system generated trap. Hence it does not have any corresponding OID.
Example	Identity services engine ISEIPAddress is unreachable.

Table 34: License violation

Purpose	Informs users when the number of devices Prime Infrastructure is actually managing exceeds the number of devices it is licensed to manage.
---------	--

When Sent	At 2:10AM, on the day following the completion of the job that added the extra devices to Prime Infrastructure inventory Note This is a system generated trap. Hence it does not have any corresponding OID.
Example	Number of managed devices N is greater than licensed devices N . Please purchase and install a license that will cover the number of managed devices, or remove unused devices from the system.

Table 35: Prime Infrastructure does not have enough disk space for backup

Purpose	Informs users when Prime Infrastructure does not have sufficient space in the specified directory to perform a backup.
When Sent	Whenever Prime Infrastructure runs a server backup job and the backup repository specified (or “defaultrepo”) is 100 percent full. The trap is generated after the job completes. Note This is a system generated trap. Hence it does not have any corresponding OID.
Example	Prime Infrastructure with address localIPAddress does not have sufficient disk space in directory directoryName for backup. Space needed: Needed GB, space available Free GB.

Table 36: Prime Infrastructure email failure

Purpose	Informs users that an attempt to send an email notification has failed.
When Sent	This trap is generated by polling when Prime Infrastructure attempts to send an email notification to an invalid user, or email notification is enabled without specifying the email server in Prime Infrastructure. Note This is a system generated trap. Hence it does not have any corresponding OID.
Example	Prime Infrastructure with address localIPAddress failed to send email. This may be due to possible SMTP misconfiguration or network issues.

Table 37: Northbound OSS server unreachable

Purpose	Informs users that a northbound notification server is unreachable.
When Sent	This trap is generated by polling when a destination northbound notification server is down or unreachable.
OID	.1.3.6.1.4.1.9.9.712.0.1
Example	Northbound notification server OSSIPAddress is unreachable. NCS alarms will not be processed for this server until it is reachable.

Configure Prime Infrastructure Traps

The following sections explain how to configure and use Prime Infrastructure trap notifications.

Related Topics

[Configure Notifications](#), on page 356

[Port Used To Send Traps](#), on page 357

[Configure Email Notifications for SNMP Traps](#), on page 357

[View Events and Alarms for SNMP Traps](#), on page 358

[Filter Events and Alarms for SNMP Traps](#), on page 358

[Purge Alarms for SNMP Traps](#), on page 359

[How to Troubleshoot Prime Infrastructure SNMP Traps](#), on page 360

Configure Notifications

For Prime Infrastructure to send northbound SNMP trap notifications, you must configure the correct settings on both the Prime Infrastructure Event Notification and Notification Destination pages. Once configured, traps will be generated based on the values associated with the Threshold and Severity for the following SNMP Events:

- Appliance Process Failure
- HA Operations
- CPU, disk and memory utilization
- Disk, fan and PSU Failure
- Backup failure, certification expiry and licenses violations

You can edit the threshold and severity associated with each event, and enable or disable trap generation for the associated event.

-
- Step 1** Log in to Prime Infrastructure using a user ID with root domain privileges.
- Step 2** Select **Administration > Settings > System Settings > Alarms and Events > System Event configuration**.
- Step 3** For each SNMP event you want to configure:
- a) Click on the row for that event.
 - b) Set the **Event Severity** level to Critical, Major, or Minor, as needed.
 - c) For the CPU, disk, memory utilization, life cycle, assurance, and collector traps: Enter the **Threshold** percentage (from 1-99). These events will send the associated SNMP traps when the utilization exceeds the threshold limit. You cannot set thresholds for events for which the threshold setting is shown as NA. These events send traps whenever the associated failure is detected.
 - d) For backup threshold, certificate expiry, certificate expiry (critical), lifecycle license, assurance license, and collector license trap: Enter the **Threshold** in days (from x-y, where x is the minimum value and y is the maximum value in days).
 - e) Set the **Event Status** to Enabled or Disabled. If set to Enabled, the corresponding trap will be generated for this event.
 - f) For the CPU, disk, memory utilization, enter the **Create and Clear Alarm Iteration** value. The default value is two. The first polling after setting the iteration value will take two times the iteration value entered in minutes. All the future polling will take 20 minutes only.

The default polling time is 20 minutes.
- Step 4** When you are finished, click **Save** to save your changes.

Related Topics

[Configure Alarms Notification Destination](#), on page 219

Port Used To Send Traps

Prime Infrastructure sends traps to notification destination on port 162. This port cannot be customized at present. The northbound management system has to register itself through the Notification destination web page (see [Configure Alarms Notification Destination, on page 219](#)).

Configure Email Notifications for SNMP Traps

You can configure Prime Infrastructure to send email notification for alarms and events generated in response to SNMP traps. All of these alarms and events are considered part of the System event category. You can also customize the severity level for which such notifications will be sent.

Note that, for these email notifications to be sent, the Prime Infrastructure administrator must configure at least a primary SMTP email server.

-
- Step 1** Log in to Prime Infrastructure.
 - Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**
 - Step 3** Click **Email Notification** tab. Prime Infrastructure displays the first Email Notification Settings page.
 - Step 4** In the **Alarm Category** column, click on the **System** category's name. Prime Infrastructure displays a second Email Notification Settings page.
 - Step 5** Under **Send email for the following severity levels**, select all of the severity levels for which you want Prime Infrastructure to send email notifications.
 - Step 6** In **To**, enter the email address to which you want Prime Infrastructure to send email notifications. If you have multiple email addresses, enter them as a comma-separated list.
 - Step 7** Click **Save**. Prime Infrastructure displays the first Email Notification Settings page.
 - Step 8** In the **Enable** column, make sure System is selected, then click **Save**.

Related Topics

[Configure Email Server Settings](#) , on page 357

Configure Email Server Settings

To enable Prime Infrastructure to send email notifications, the system administrator must configure a primary SMTP email server (and, preferably, a secondary email server).

-
- Step 1** Log in to Prime Infrastructure using a user ID with administrator privileges.
 - Step 2** Select **Administration > Settings > System Settings > Mail and Notification > Mail Server Configuration**.
 - Step 3** Under **Primary SMTP Server**, complete the **Hostname/IP**, **User Name**, **Password**, **Port**, and **Confirm Password** fields as appropriate for the email server you want Prime Infrastructure to use. Enter the IP address of the physical server. You cannot enter a virtual IP address in the Hostname/IP field, and the IP address cannot be behind a load balancer.
 - Step 4** (Optional) Complete the same fields under **Secondary SMTP Server**.
 - Step 5** Under **Sender and Receivers**, enter a legitimate email address for the Prime Infrastructure server.
 - Step 6** (Optional) Enter a subject line in the **Subject** text box.
 - Step 7** When you are finished, click **Save**.
-

Related Topics

- [View Events and Alarms for SNMP Traps](#), on page 358
- [Filter Events and Alarms for SNMP Traps](#), on page 358
- [Purge Alarms for SNMP Traps](#), on page 359
- [How to Troubleshoot Prime Infrastructure SNMP Traps](#), on page 360
- [Configure Notifications](#), on page 356
- [Port Used To Send Traps](#), on page 357
- [Configure Email Notifications for SNMP Traps](#), on page 357

View Events and Alarms for SNMP Traps

Events and Alarms for all of Prime Infrastructure’s internal SNMP traps fall under the System category. You can view them in the Prime Infrastructure Alarms and Events dashboard.

-
- Step 1** Log in to Prime Infrastructure.
 - Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**.
-

Filter Events and Alarms for SNMP Traps

You can use the Prime Infrastructure Filter feature to narrow the display of alarms to just those in the System category, or use a combination of criteria and operators to focus the list on very specific alarms. The following sections explain how to do this.

Related Topics

- [Filter for SNMP Traps Using Quick Filters](#), on page 358
- [Filter for SNMP Traps Using Advanced Filters](#), on page 358

Filter for SNMP Traps Using Quick Filters

Prime Infrastructure's Quick Filters allow you to quickly focus on the data inside a table by applying a filter for a specific table column or columns.

-
- Step 1** Log in to Prime Infrastructure.
 - Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**.
 - Step 3** From the **Show** drop-down list, select **Quick Filter**. Prime Infrastructure displays a table header listing fields on which you can perform a quick filter, including **Severity**, **Message**, and **Category**.
 - Step 4** In the **Category** field, enter **System**. Prime Infrastructure displays only System alarms.
 - Step 5** To clear the Quick Filter, click the funnel icon shown next to the **Show** box.
-

Filter for SNMP Traps Using Advanced Filters

Prime Infrastructure's Advanced Filter allows you to narrow down the data in a table by applying a filter combining multiple types of data with logical operators (such as “Does not contain”, “Does not equal”, “Ends

with”, and so on). For example, you can choose to filter the table of alarms based on the Category, then further reduce the data by filtering on Severity (as shown in the steps below). You can also save an Advanced Filter for later re-use.

-
- Step 1** Log in to Prime Infrastructure.
- Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**.
- Step 3** From the **Show** drop-down list, select **Advanced Filter**. Prime Infrastructure displays a table header showing criteria for the first rule in the filter.
- Step 4** Complete the first rule as follows:
- In the first field, select **Category** from the drop-down list.
 - In the second field, select **Contains** from the drop-down list.
 - In the third rule field, enter **System**.
 - Click **Go**. Prime Infrastructure displays only System alarms.
- Step 5** Click the plus sign icon to add another rule, then complete the second rule as follows:
- In the first field, select **Severity** from the drop down list
 - In the second field, select **equals (=)** from the drop-down list.
 - In the third rule field, select **Major** from the drop-down list.
 - Click **Go**. Prime Infrastructure displays only System alarms with Major Severity.
- Repeat this step as needed.
- Step 6** To save the Advanced filter, click the **Save** icon and supply a name for the filter.
- Step 7** To clear the Advanced Filter, click **Clear Filter**.
- For more details, see [Purge Alarms for SNMP Traps, on page 359](#).

Related Topics

- [How to Troubleshoot Prime Infrastructure SNMP Traps, on page 360](#)
- [Configure Notifications, on page 356](#)
- [Port Used To Send Traps , on page 357](#)
- [Configure Email Notifications for SNMP Traps, on page 357](#)
- [View Events and Alarms for SNMP Traps, on page 358](#)
- [Filter Events and Alarms for SNMP Traps, on page 358](#)

Purge Alarms for SNMP Traps

You can remove an alarm from the list of alarms by changing its status to Acknowledged or Cleared. No e-mails will be generated for these alarms.

-
- Step 1** Log in to Prime Infrastructure.
- Step 2** Select **Monitor > Monitoring Tools > Alarms and Events**.
- Step 3** Select an alarm, then choose **Change Status > Acknowledge** or **Change Status > Clear**.
-

How to Troubleshoot Prime Infrastructure SNMP Traps

If you are having trouble with Prime Infrastructure's internal traps and related notifications, check the following:

Step 1 Ping the notification destination from the Prime Infrastructure server, to ensure that there is connectivity between Prime Infrastructure and your management application.

Step 2 Check if any firewall ACL settings are blocking port 162, and open communications on that port if needed.

Step 3 Log in to Prime Infrastructure with a user ID that has administrator privileges. Select **Administration > Settings > Logging** and download the log files. Then compare the activity recorded in these log files with the activity you are seeing in your management application:

- `ncs_nb.log`: This is the log of all the northbound SNMP trap messages Prime Infrastructure has sent. Check for messages you have not received.
- `ncs-#-#.log`: This is the log of other recent Prime Infrastructure activity. Check for hardware trap messages you have not received.
- `hm-#-#.log`: This is the complete log of Health Monitor activity. Check for recent messages about High Availability state-changes and application-process failures that you have not received.

The messages you see in these logs should match the activity you see in your management application. If you find major differences, open a support case with Cisco Technical Assistance Center (TAC) and attach the suspected log files with your case.

Related Topics

[Prime Infrastructure SNMP Trap Types](#), on page 344

[Prime Infrastructure SNMP Trap Reference](#), on page 350

[Configure Prime Infrastructure Traps](#), on page 355



APPENDIX **C**

Configure High Availability for Plug and Play Gateway

- [How Cisco Plug and Play Gateway HA Works](#), on page 361
- [Cisco Plug and Play Gateway HA Prerequisites](#), on page 361
- [Set up Standalone Cisco Plug and Play Gateway for Prime Infrastructure HA](#), on page 362
- [Cisco Standalone Plug and Play Gateway Server HA Setup](#), on page 363
- [Cisco Plug and Play Gateway Status](#), on page 364
- [Remove Cisco Plug and Play Gateway in HA](#), on page 365
- [Cisco Plug and Play Gateway HA and Combinations](#), on page 366
- [Limitations of Cisco Plug and Play Gateway HA](#), on page 366

How Cisco Plug and Play Gateway HA Works

Earlier releases of supported a single Cisco Plug and Play Gateway in either of these modes:

- Plug and Play Gateway standalone server mode
- Plug and Play Gateway integrated server mode

HA was not available in both these solutions, and Cisco Plug and Play Gateway does not connect to the secondary server automatically. It has to be manually redirected to the secondary server.

supports Plug and Play Gateway in HA in current release. The Cisco Plug and Play HA feature aims at providing the following:

- HA on a standalone server Plug and Play Gateway by providing a secondary standby Plug and Play Gateway.
- HA support between the standalone Plug and Play Gateway and HA.
- HA support for integrated Plug and Play Gateway.

Cisco Plug and Play Gateway HA Prerequisites

Before using the HA feature on Cisco Plug and Play Gateway, you must:

- Configure the primary and secondary servers and these must be accessible from Plug and Play Gateway standalone servers. See [Configure High Availability](#), on page 257 for more details.

- Ensure that the primary and secondary SSL server certificates used for Message Queue Ports 61617 and Health Monitor port 8082 are available for extraction from primary and secondary servers for HA mode with different IP addresses. See [Set Up High Availability, on page 271](#) for more details.
- For virtual IP Address based HA, both primary and secondary servers must have the virtual IP address and certificates. See [Using Virtual IP Addressing With HA, on page 262](#) for more details.
- At least one of the server Message Queue port 61617 port must be active at all times depending on the service which will take the HA role.
- Install the primary and secondary Plug and Play Gateway Virtual Machines. See the latest [Cisco Prime Infrastructure Quick Start Guide](#) for details of installation of virtual machines from OVA file.

Set up Standalone Cisco Plug and Play Gateway for Prime Infrastructure HA

The Cisco Prime Infrastructure server in HA can be configured in two modes:

- Virtual IP addresses for primary and secondary servers. See [Using Virtual IP Addressing With HA, on page 262](#) for more details.
- Different IP addresses for primary and secondary servers. See [Set Up High Availability, on page 271](#) for more details.

The standalone Cisco Plug and Play Gateway can be configured to work in both of these modes with a slight modification in the setup procedure.

Related Topics

- [in HA with Virtual IP Address, on page 362](#)
- [in HA with Different IP Address, on page 362](#)

in HA with Virtual IP Address

can be configured with a virtual IP address which floats across the primary and secondary servers, depending on the server that is active. Enter the virtual IP address of in HA while setting up Cisco Plug and Play Gateway.

Integrated Plug and Play Gateway within will work if the same virtual IP address is transferred to the active node. Cisco Plug and Play Gateway integrated with Prime Infrastructure will be configured automatically to use the virtual IP address. No specific configuration is required to configure Cisco Plug and Play Gateway.

Related Topics

- [in HA with Different IP Address, on page 362](#)

in HA with Different IP Address

can be configured with primary and secondary servers having different IP addresses. For configuring Cisco Plug and Play Gateway, run the **pnp setup advance** command in the advanced setup and enter the following information:

- Primary IP address.
- Enter y, when prompted if a secondary server is to be configured.
- Secondary IP address.

See [Command Reference Guide for Cisco Prime Infrastructure](#) for more details about running the commands.



Note Cisco Plug and Play Gateway integrated with will not work when the primary and secondary servers have different IP addresses because the bootstrap configuration needs to be changed according to the active node.

Related Topics

- [Cisco Plug and Play Gateway HA Prerequisites](#), on page 361
- [Set up Standalone Cisco Plug and Play Gateway for Prime Infrastructure HA](#), on page 362
- [Remove Cisco Plug and Play Gateway in HA](#), on page 365
- [Cisco Standalone Plug and Play Gateway Server HA Setup](#), on page 363
- [Cisco Plug and Play Gateway HA and Combinations](#), on page 366

Cisco Standalone Plug and Play Gateway Server HA Setup

Cisco Standalone Plug and Play Gateway can also be configured in HA with a secondary server for failover. Cisco Plug and Play Gateway in HA is always configured with a virtual IP address on the active node. For setting up the standalone Plug and Play Gateway in HA you must:

- Install two reachable Cisco Plug and Play Gateways with different IP addresses.
- Run the **pnpl setup** or **pnpl setup advance** command on the primary Cisco Plug and Play Gateway. See [Command Reference Guide for Cisco Prime Infrastructure](#) for more details. The primary server will automatically configure secondary Cisco Plug and Play Gateway at the end of the setup.
- Enter **y** when prompted, if you want to configure HA with primary Cisco Plug and Play Gateway HA server.



Note The standalone Cisco Plug and Play Gateway with in HA has automatic failover from primary to secondary. Manual failover is not available.

The standalone Cisco Plug and Play Gateway with in HA can be configured to failback manually or automatically from the secondary to primary server.

Enter the Cisco Plug and Play Gateway virtual IP address, virtual host name, IP address and username and password of the secondary server as part of pnp setup. Enter **0** for manual failback and **1** for automatic failback when prompted during the setup.



Note We recommend manual failback. Automatic failback is not recommended because in case of scenarios like flapping interface, failover and failback happens continuously.

Related Topics

- [Cisco Plug and Play Gateway Status](#), on page 364
- [How Cisco Plug and Play Gateway HA Works](#), on page 361
- [Setting up Cisco Plug and Play Gateway HA](#)
- [Cisco Plug and Play Gateway HA and Combinations](#), on page 366

Cisco Plug and Play Gateway Status

The Cisco Plug and Play Gateway status interface provides additional information regarding the following:

HA Status:

- If the virtual IP address has been entered during setup, the status will display only the address. Cisco Plug and Play Gateway status cannot identify whether it is connected to the primary or secondary server.
- Cisco Plug and Play HA Status:

Along with the status for the different Cisco Plug and Play Gateway processes, it will also display the Cisco Plug and Play Gateway in active mode when both the gateways are up. The status will also show the connection status between the primary and secondary servers as an additional value in the table.

To check the status of the Cisco Plug and Play Gateway server, log in to the gateway server and run the **pnpl status** command. The gateway server status is displayed.

See [Command Reference Guide for Cisco Prime Infrastructure](#) for more details on running the commands.

SERVICE	MODE	STATUS	ADDITIONAL INFO
System		UP	
Event Messaging Bus	PLAIN TEXT	UP	pid: 6808
CNS Gateway Dispatcher 11011	PLAIN TEXT	UP	pid: 7189, port:
CNS Gateway 11013	PLAIN TEXT	UP	pid: 7223, port:
CNS Gateway 11015	PLAIN TEXT	UP	pid: 7262, port:
CNS Gateway 11017	PLAIN TEXT	UP	pid: 7306, port:
CNS Gateway 11019	PLAIN TEXT	UP	pid: 7410, port:
CNS Gateway 11021	PLAIN TEXT	UP	pid: 7493, port:
CNS Gateway Dispatcher 11012	SSL	UP	pid: 7551, port:
CNS Gateway 11014	SSL	UP	pid: 7627, port:
CNS Gateway 11016	SSL	UP	pid: 7673, port:
CNS Gateway 11018	SSL	UP	pid: 7793, port:
CNS Gateway 11020	SSL	UP	pid: 7905, port:
CNS Gateway 11022	SSL	UP	pid: 7979, port:
HTTPD		UP	
Image Web Service	SSL	UP	
Config Web Service	SSL	UP	
Resource Web Service	SSL	UP	
Image Web Service	PLAIN TEXT	UP	
Config Web Service	PLAIN TEXT	UP	
Resource Web Service	PLAIN TEXT	UP	
Prime Infrastructure Broker	SSL	UP	Connection: 1,
Connection Detail: ::ffff:10.104.105.170:61617 bgl-dt-pnp-ha-216/admin#			
SERVICE	MODE	STATUS	ADDITIONAL INFO


```

System | | UP |
-----|-----|-----|-----
Event Messaging Bus | PLAIN TEXT | UP | pid: 6426
CNS Gateway Dispatcher | PLAIN TEXT | UP | pid: 7107, port:
11011
CNS Gateway | PLAIN TEXT | UP | pid: 7141, port:
11013
CNS Gateway | PLAIN TEXT | UP | pid: 7180, port:
11015
CNS Gateway | PLAIN TEXT | UP | pid: 7224, port:
11017
CNS Gateway | PLAIN TEXT | UP | pid: 7263, port:
11019
CNS Gateway | PLAIN TEXT | UP | pid: 7309, port:
11021
CNS Gateway Dispatcher | SSL | UP | pid: 7381, port:
11012
CNS Gateway | SSL | UP | pid: 7537, port:
11014
CNS Gateway | SSL | UP | pid: 7581, port:
11016
CNS Gateway | SSL | UP | pid: 7685, port:
11018
CNS Gateway | SSL | UP | pid: 7855, port:
11020
CNS Gateway | SSL | UP | pid: 7902, port:
11022
HTTPD | | UP |
Image Web Service | SSL | UP |
Config Web Service | SSL | UP |
Resource Web Service | SSL | UP |
Image Web Service | PLAIN TEXT | UP |
Config Web Service | PLAIN TEXT | UP |
Resource Web Service | PLAIN TEXT | UP |
Prime Infrastructure Broker | SSL | UP | Connection: 1,
Connection Detail: ::ffff:10.104.105.170:61617
PnP Gateway Monitoring | SSL | UP | port: 11010
PnP Gateway HA | SSL | UP | Primary Server
is in Active state
bgl-dt-pnp-ha-217/admin#

```

Remove Cisco Plug and Play Gateway in HA

To delete the HA configuration for with different primary and secondary IP addresses in the standalone Cisco Plug and Play Gateway, run the **pnp setup advance** advanced setup command and enter n when prompted.

For deleting Cisco Plug and Play Gateway HA, run the pnp setup or pnp setup advance command and enter n when prompted.

See [Command Reference Guide for Cisco Prime Infrastructure](#) for more details.



Note When deleting Cisco Plug and Play Gateway HA, the administrator must manually modify the dynamic port allocation **cms event** command and decommission the secondary server, if HA is being turned off. The Cisco Plug and Play Gateway secondary server will continue to run with the virtual IP address if it is not decommissioned.

Related Topics

[Cisco Plug and Play Gateway HA and Combinations](#), on page 366

[Limitations of Cisco Plug and Play Gateway HA](#), on page 366

[How Cisco Plug and Play Gateway HA Works](#), on page 361

[Setting up Cisco Plug and Play Gateway HA](#)

Cisco Plug and Play Gateway HA and Combinations

The Cisco Plug and Play Gateway functionality allows different configurations for HA with . The various combinations, as per the configuration options available, are:

- Standalone Cisco Plug and Play Gateway without HA (Single Cisco Plug and Play Gateway)
 - The server without HA.
 - The server with HA with the virtual IP address.
 - server with HA with the primary and secondary servers having two IP addresses.
- Standalone Cisco Plug and Play Gateway with HA and virtual IP address (Two Cisco Plug and Play Gateways)
 - server without HA.
 - server with HA with the virtual IP address.
 - server with HA with the primary and secondary servers having two IP addresses.
- Integrated Cisco Plug and Play Gateway within
 - server without HA.
 - server with HA with the virtual IP Address.

Related Topics

[Limitations of Cisco Plug and Play Gateway HA](#), on page 366

[How Cisco Plug and Play Gateway HA Works](#), on page 361

[Setting up Cisco Plug and Play Gateway HA](#)

[Remove Cisco Plug and Play Gateway in HA](#), on page 365

[Cisco Plug and Play Gateway Status](#), on page 364

Limitations of Cisco Plug and Play Gateway HA

The Cisco Plug and Play Gateway HA feature has the following limitations:

- Any Plug and Play requests that are partially completed on the Cisco Plug and Play Gateway during failover and failback (the and Cisco Plug and Play Gateway standalone server) will remain incomplete in the server and these may not be configured successfully on the device.
- Failover and failback takes five to ten minutes during which Cisco Plug and Play Gateway provisioning does not happen. Devices that have received bootstrap with cns config initial will continue to reach Cisco Plug and Play Gateway for provisioning. [Command Reference Guide for Cisco Prime Infrastructure](#) for more details.
- Devices take time to connect to the backup server once the IP address is moved from the active to standby server depending on the configuration available in the cns event command for reconnect time.

- integrated Plug and Play Gateway will support HA if the HA configuration in Prime is based on a virtual IP address. HA with different IP addresses for primary and secondary servers will not support the Plug and Play Gateway HA functionality in the integrated server.
- For the integrated Plug and Play Gateway, SSLv3 is disabled by default on all Gateway SSL ports (for example, ports 11012, 11014, and so on).
- Related Topics

Related Topics

[How Cisco Plug and Play Gateway HA Works](#), on page 361

[Setting up Cisco Plug and Play Gateway HA](#)

[Remove Cisco Plug and Play Gateway in HA](#), on page 365

[Cisco Plug and Play Gateway HA and Combinations](#), on page 366

