



Cisco Edge 340 Series Software Configuration Guide, Release 1.2

August 18, 2016

Cisco Systems, Inc.

www.cisco.com

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

Text Part Number: OL-31688-01

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.

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. 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. (1110R)

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.

Cisco Edge 340 Series Software Configuration Guide, Release 1.2
© 2014 Cisco Systems, Inc. All rights reserved.



Preface vii

Conventions vii

Related Publications viii

Obtaining Documentation and Submitting a Service Request viii

CHAPTER 1

Cisco Edge 340 Series Overview 1-1

Cisco Edge 340 Series Overview 1-1

 Cisco Edge 340 Series Features and Application Support 1-2

Logging in to the System 1-2

Management and Configuration Support 1-3

 Web GUI 1-3

 Local CLI—CLISH 1-3

System Installation and Upgrade 1-4

 USB Mode Installation and Upgrade 1-4

 Remote Upgrade from the Web GUI 1-6

 BIOS Upgrade 1-6

CHAPTER 2

Configuring the Web GUI 2-1

Logging In to the Web GUI 2-1

Language Setting 2-2

System Configuration 2-3

 Configuring Basic Information 2-3

 Configuring Power Management 2-4

 Configuring Resolution 2-8

 Configuring Date and Time 2-12

 Configuring Syslog 2-14

 Configuring Coredump 2-16

 Configuring Proxy 2-17

Network Configuration 2-17

 Configuring DNS 2-18

 Configuring Wired Settings 2-18

 Configuring Wireless Settings 2-23

 Configuring SNMP 2-30

 Configuring VPN 2-36

- Monitoring the Status of System and Network 2-45
 - Monitoring the System 2-45
 - Monitoring the Network 2-46
- Administration 2-47
 - Configuring Account Information 2-47
 - Configuring Radius Information 2-49
 - Configuring Image Upgrade 2-52
 - Configuration Archive 2-55
 - Restart or Reset 2-57

CHAPTER 3

Configuring Local CLI - CLISH 3-1

- Configuration Guidelines 3-1
- Command Reference 3-4
 - User Configuration Mode Commands 3-4
 - Global Configuration Mode Commands 3-10
 - System Configuration Mode Commands 3-18
 - Ethernet Interface Configuration Mode Commands 3-37
 - WiFi AP Interface Configuration Mode Commands 3-44
 - SSID Configuration Mode 3-75
 - show Commands 3-82

APPENDIX A

Troubleshooting A-1

- Boot and Login A-1
 - Forget Root Password A-1
 - System Starts Slowly A-2
 - System Locked After Using Wrong Password Five Times A-2
- Reset and Upgrade A-2
 - Having Trouble Updating the System A-3
 - Restore Factory Settings Action Fails in Web GUI A-3
- Display Issues A-4
 - No Signal Output A-4
 - Screen Blurred After Resolution is Changed A-4
- Network Issues A-4
 - Connection Status Not Refreshed in the WiFi Station Mode A-4
 - Wake On LAN Not Effective A-4
 - DNS Not Parsed A-5
 - Third-Party Device Cannot be Connected A-5
 - Unstable Connection Due to Multiple SSIDs A-5
 - Wait Before Reconnecting A-5

Power Issues	A-5
Power Shortage of Peripheral Equipment	A-5
USB Ports on the Rear Panel Not Working	A-6

APPENDIX B**SNMP Information** B-1

Compatibility	B-1
Supported MIB Information	B-1

APPENDIX C**Configuring SCEP and Obtaining and Enrolling the Certificate** C-1

APPENDIX D**Importing the SHA2 Certificate** D-1

Certificate API	D-1
SCEP API	D-3



Preface

This document describes how to configure the Cisco Edge 340 Series in your network.

This guide does not describe how to install the Cisco Edge 340 Series. For information about how to install the Cisco Edge 340 Series, see the hardware installation guide pertaining to your device.

Conventions

This publication uses these conventions to convey instructions and information.

For command descriptions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ({ | }) mean a required choice within an optional element.

For interactive examples:

- Terminal sessions and system displays are in `screen` font.
- Information that you enter is in **boldface screen** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and warnings use these conventions and symbols:



Note

Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Publications

- *Cisco Edge 340 Series Installation Guide*
- *Release Notes for the Cisco Edge 340 Series*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:
<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.



Cisco Edge 340 Series Overview

- [Cisco Edge 340 Series Overview](#)
- [Logging in to the System](#)
- [Management and Configuration Support](#)
- [System Installation and Upgrade](#)

Cisco Edge 340 Series Overview

Cisco Edge 340 Series is the next-generation device for vertical and enterprise-connected room deployments that provide rich media-enablement capabilities and vertical-specific application support. It integrates rich connectivity to enable all the essential components of a digital connected room experience with Ethernet LAN uplink, wireless access, rich media, and application computing. It is also an open application platform that allows you to customize it to enable vertical solutions.

Digital Media Player

The Cisco Edge 340 Series device functions as a next-generation digital media player for the following solutions:

- Digital media signage
- Sports and entertainment
- iServices

In the digital media signage solution, the Cisco Edge 340 Series device acts as a Digital Media Player (DMP) to provide the functions of both video and audio player. Additionally, it also provides high computing capability and local storage for the content.

Application Support

The Cisco Edge 340 Series supports vertical applications and provides computing power, storage, and simple connectivity functions.

Home Automation Gateway

The Cisco Edge 340 Series functions as a home service gateway that is deployed at homes, sitting behind a residential gateway device, to provide home automation service through WiFi, to connect and control smart electric appliances.

Cisco Edge 340 Series Features and Application Support

The Cisco Edge 340 Series provides these features and application support:

- VLC player
- SM player
- Document viewer
- Visual Presenter
- Video conference
- Screen capture
- VPN client support
- SNMP support

For detailed information about these features and applications, refer to *Release Notes for the Cisco Edge 340 Series* for your version.

Logging in to the System

To power on and log in to the Cisco Edge 340 Series system, follow these steps:

-
- Step 1** Connect the power cord of the Cisco Edge 340 Series to an electrical outlet.
 - Step 2** Connect the monitor, keyboard, and mouse to the Cisco Edge 340 Series.
 - Step 3** Press the **Power** button to power on the Cisco Edge 340 Series. The following screen is displayed:

Figure 1-1 Log In Screen - User name



- Step 4** Enter **user** in the Username field and click **Log In**. The following screen is displayed:

Figure 1-2 Log In Screen - User name



Step 5 Enter **User123!** in the Password field and click the **Log In** button to log in to the system.



Note Change the default password immediately after you have successfully logged in to the system.



Note If you try to log in to the system with a wrong user name or password, the system will be locked for 15 seconds. During this period, although you use the correct user name and password, you still cannot log in successfully. You must wait for 15 seconds and try again.

Management and Configuration Support

The Cisco Edge 340 Series supports the following management and configuration methods:

- [Web GUI](#) (Recommended)
- [Local CLI—CLISH](#) (Optional)

Web GUI

You are recommended to use the web GUI to configure the Cisco Edge 340 Series and monitor the status locally or remotely. For more information, see [Chapter 2, “Configuring the Web GUI.”](#)

Local CLI—CLISH

As an option, you can also use CLISH to configure the Cisco Edge 340 Series for the local CLI configuration. The CLI uses only those commands that are specific to the Cisco Edge 340 Series. Although the syntax is similar to the Cisco IOS CLI, the commands are *incompatible* with Cisco IOS commands. For more information, see [Chapter 3, “Configuring Local CLI - CLISH.”](#)

System Installation and Upgrade

The Cisco Edge 340 Series supports the following installation and upgrade types:

- [USB Mode Installation and Upgrade](#)
- [Remote Upgrade from the Web GUI](#)
- [BIOS Upgrade](#)

USB Mode Installation and Upgrade

The Cisco Edge 340 Series software releases a self-extract installer. The file name of the self-extract installer is `Cisco-Edge-version-i386-DVD.bin`, where *version* is the software release version. It is an executive file that helps you to perform the installation automatically. When you execute the self-extract installer, the installation-related files are extracted to the hard drive of the Cisco Edge 340 Series, and a `livecd` is created in the internal USB. The system then boots from the internal USB (also known as the factory mode) and performs the installation automatically.

If the internal USB has already been created as a `livecd`, you can press the factory mode pinhole on the front panel of the Cisco Edge 340 Series to enter the factory mode and perform the installation procedure automatically.



Note

Usually, the internal USB is created as a `livecd` in the factory. Executing the self-extract installer will overwrite the original `livecd` and create a new one.

Prerequisites

Before you execute the self-extractor installer, perform the following steps to make sure that the installation will be successful.

-
- Step 1** Locate your target self-extract installer (`Cisco-Edge-xxx-i386-DVD.bin`).
- Step 2** Make sure that the `livecd-tools` has been installed using the following command:
- ```
rpm -q livecd-tools
```
- Step 3** Make sure there is at least 1.5G free space on HOME or ROOT partition. If you execute the self-extractor installer without enough space on the partition, you will see the either of the following message displayed: *No enough disk free space* Or *Failed to extract ISO!*
- Use the following command to check the available space on the HOME partition:
 

```
df -h /home
```
  - Use the following command to check the available space on the ROOT partition:
 

```
df -h /
```
- Step 4** If you want to use an external USB as the target USB, make sure the first partition of the USB has at least 1.5G free space. The `ext4` format is recommended, and `ext3/fat32` format is also supported.
- Step 5** Make sure the self-extract-installer (`Cisco-Edge-xxx-i386-DVD.bin`) has the executable attribute. Set the attribute with the following command:
- ```
chmod a+x /path/to/ Cisco-Edge-xxx-i386-DVD.bin
```

Step 6 Make sure no other installation or upgrade process is ongoing.

**Note**

If another installation or upgrade process is ongoing, and you execute the self-extractor installer, you will see the following message displayed: *an install process is ongoing*. You can wait until the ongoing upgrade process is finished, or you can reboot the system, and then execute the self-extractor installer again.

**Note**

When you select the internal USB as target livecd, if power failure happens during the process of command execution, the old livecd on the internal USB will be wiped. You have to rebuild a livecd disk on the internal USB.

Command Description

You can use the `Cisco-Edge-version-i386-DVD.bin` command with different parameters to implement installation or upgrade, print help, or create livecd only. In the command, *version* indicates the image version, which will be 1.1 for this release. For the installation and upgrade of the releases other than 1.1, refer to the software configuration guide of corresponding releases.

**Note**

When you use this method to install or upgrade the system, make sure there is 1.5G free space at least.

1. To select the internal USB as a livecd disk and boot into factory mode to finish the installation automatically, use the following command:
2. To print help and then exit, use the following command:
3. To create livecd only, without entering factory mode nor executing the system installation program, use the following command:

```
Cisco-Edge-1.1-i386-DVD.bin
```

```
Cisco-Edge-1.1-i386-DVD.bin --help|-h
```

```
Cisco-Edge-1.1-i386-DVD.bin -t|--target <dev>
```

<dev> is the full path of the target u-disk into which the livecd will be burned, for example, /dev/sdb1.

4. To wipe the home partition before the system is installed, use the following command:

```
Cisco-Edge-1.1-i386-DVD.bin -w|--wipe
```

**Note**

When the home partition is wiped, user data will be lost.

Remote Upgrade from the Web GUI

You can perform a remote upgrade for the Cisco Edge 340 Series using the web GUI if you have the address to download the self-extract installer. When you choose to perform the remote upgrade, the system will automatically download the self-extract-installer from the URL that you provide and execute the self-extract-installer to finish the installation.

BIOS Upgrade

BIOS upgrade can only be performed by manually installing the package and executing the commands in the Linux environment. BIOS is a critical part of the system, and there is no software recovery method if it crashes. To ensure successful BIOS upgrade, make sure that the external power supply is always connected, and do *not* perform any power cycle action during the upgrade process.



Configuring the Web GUI

The web-based GUI is used to configure a Cisco Edge 340 Series device and monitor the status of the Cisco Edge 340 Series locally or remotely.

To configure a Cisco Edge 340 Series device using the web-based GUI, follow the steps described in these sections:

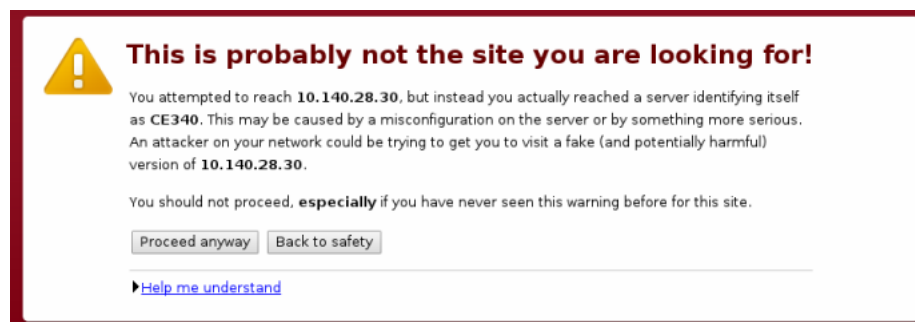
- [Logging In to the Web GUI, page 2-1](#)
- [Language Setting, page 2-2](#)
- [System Configuration, page 2-3](#)
- [Network Configuration, page 2-17](#)
- [Monitoring the Status of System and Network, page 2-45](#)
- [Administration, page 2-47](#)

Logging In to the Web GUI

There are two ways to access the Web GUI:

- Access the web-based GUI at `https://[Cisco Edge 340's IP address]` and log in to the web portal locally or remotely. A warning page is displayed, as shown in [Figure 2-1](#). Click **Proceed anyway** to continue. Enter the username and password of the system account ([Figure 2-2](#)). The default username is **admin**, and the default password of the admin account is **aDMIN123#**.

Figure 2-1 **Warning Page**



- Click **Preference** on desktop and log in by entering the username and password of system account (Figure 2-2). The default username is **admin**, and the default password of the admin account is **aADMIN123#**.

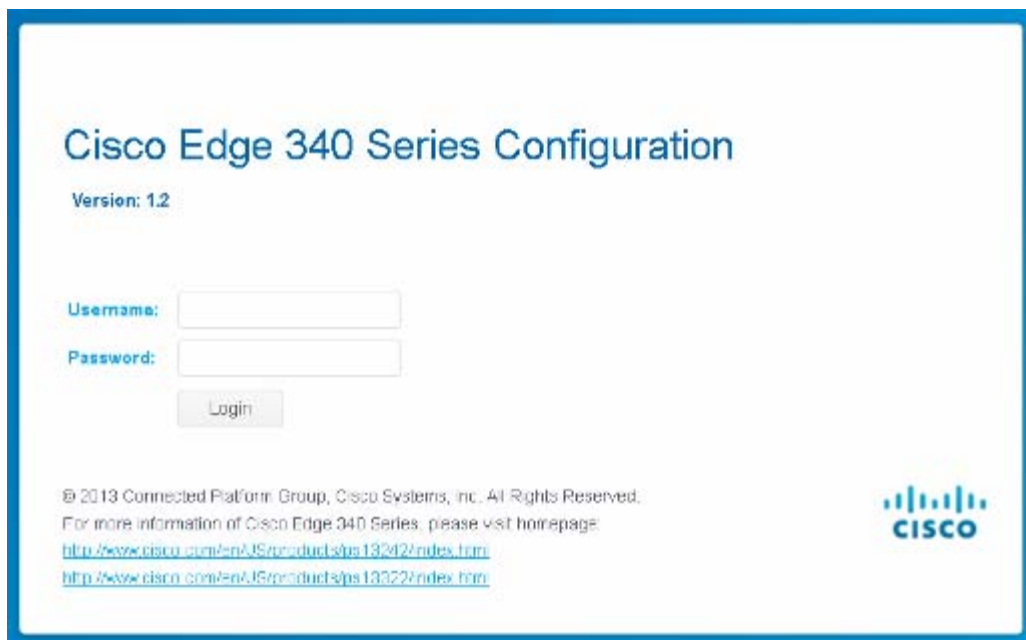
**Note**

Change the default password immediately after you have successfully logged in to the system for the first time. You can also refer to the steps in the “Configuring Account Information” section on page 2-47 to change the Web GUI login name.

**Note**

When the password of web GUI admin is changed, the password of system ROOT user (OS admin user) is also changed. In fact, the web GUI admin account is exactly the ROOT user of the OS.

Figure 2-2 Log in Page



Language Setting

After you log in, choose the language that you want to use with the web GUI. At the top of the GUI, choose a language from the drop-down list (Figure 2-3).

Figure 2-3 Language Setting of the Web GUI



System Configuration

After you log in to the web GUI, the System configuration window is displayed. You can configure the basic system options, including hostname, auto-login, IR, Bluetooth, locale, grub screen message, volume indicator and so on. You can also view the device model number, related operating system version, and RPM version in this section.

Configuring Basic Information

You can configure the basic system options, such as hostname, auto-login, Bluetooth, and locale on the **Basic** tab. This page also shows the device model number, related operating system version, and RPM version (Figure 2-4).

Figure 2-4 Basic Information

The screenshot displays the 'Basic' configuration page in the Cisco Edge 340 Series web GUI. On the left is a navigation menu with categories: System (Basic, Power Management, Resolution, Date And Time, Syslog, CoreDump, Proxy), Network (DNS, Wired, Wireless, SNMP, VPN), Monitor (System, Network), and Administration (Account, Radius, Image Upgrade, Configuration Archive). The 'Basic' tab is selected. The main content area is titled 'Basic' and includes a description: 'This page allows you to set basic system option, including hostname, auto-login, bluetooth, locale and so on.' Below this are several configuration fields: Model (CS-E340W-G32-C-K9), Hostname (text input with 'CE340'), Auto-login (dropdown with 'Disable'), IR (dropdown with 'On'), Bluetooth (dropdown with 'On'), Locale (dropdown with 'en_US.utf8'), Grub screen message (dropdown with 'Enable'), and Volume Indicator (dropdown with 'Enable'). At the bottom, there are 'Apply' and 'Reset' buttons. The OS Version is shown as 'Cisco-Edge 340 release 1.1.10162300' and the RPM Version as '4.9.1.3'.

Follow these steps to configure the basic information:

- Step 1** Click **Basic** under System in the left pane.
- Step 2** Enter a valid hostname in the Hostname field. Make sure the format is acceptable.
- Step 3** Choose **Enable** or **Disable** from the Auto-login drop-down list.
- Step 4** Choose **Enable** or **Disable** from the IR drop-down list.
- Step 5** Choose **Off** or **On** from the Bluetooth drop-down list.
- Step 6** Choose a locale for the system language from the Locale drop-down list.

**Note**

Change of locale needs reboot of the device to take effect. The locale options are defined in the following format: [language[_territory]][.codeset][@modifier]]. Each option represents a language. For example, en_US.UTF-8 means U.S. English using the UTF-8 encoding.

- Step 7** Choose **Enable** or **Disable** from the Grub screen message drop-down list.
- Step 8** Choose **Enable** or **Disable** from the Volume Indicator drop-down list.
- Step 9** Click **Apply** to save the changes and **Reset** to restore the previous values.

Configuring Power Management

In the Power Management tab, you can obtain current power supply option and apply power in the Power over Ethernet (PoE) mode. You can also enable or disable the USB ports in this page.

Upgrading Power Supply in the PoE Mode

In the PoE Mode, you can request more power supply.

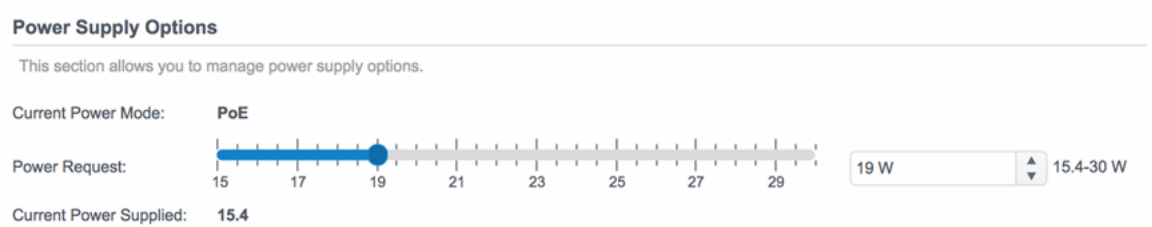
Follow these steps to request upgrading the power supply in the PoE mode:

- Step 1** Click **Power Management** under System in the left pane.
- Step 2** Check whether the Current Power Mode is PoE, as shown in [Figure 2-5](#). You can also get the current power in the Current Power Supplied field.

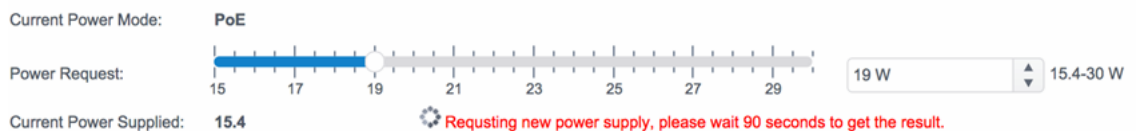
Figure 2-5 Power Management Tab

The screenshot shows the Cisco Edge 340 Series Configuration web GUI. The left navigation pane has 'Power Management' selected. The main content area is titled 'Power Management' and contains a 'Power Supply Options' section. Below this section, it states 'This section allows you to manage power supply options.' The 'Current Power Mode' is set to 'PoE'. The 'Power Request' field features a slider and an input box showing '15.4 W'. The 'Current Power Supplied' field shows '15.4'.

- Step 3** Drag the slide bar in the Power Request field, or input new power value in the input box at the end of the Power Request field. For example, in [Figure 2-6](#), the power is upgraded from 15.4 W to 19 W.

Figure 2-6 Upgrading Power Supply in the PoE Mode

- Step 4** Click the **Apply** button. It may take about 90 seconds to complete a new power supply request, as shown in [Figure 2-7](#).

Figure 2-7 Power Upgrade in Process

- Step 5** When the power upgrade request is completed, the result will be displayed on the screen, as shown in [Figure 2-8](#).

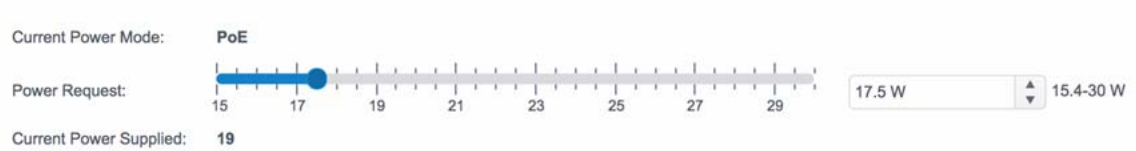
Figure 2-8 Power Upgrade Succeeded

Downgrading Power Supply in the PoE Mode

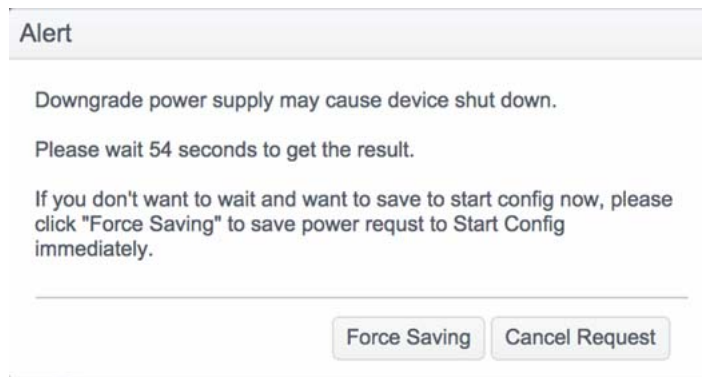
In the PoE Mode, you can request less power supply.

Follow these steps to request downgrading the power supply in the PoE mode:

- Step 1** Click **Power Management** under System in the left pane.
- Step 2** Check whether the Current Power Mode is PoE, as shown in [Figure 2-5](#). You can also get the current power in the Current Power Supplied field.
- Step 3** Drag the slide bar in Power Request, or input new power value in the input box at the end of the Power Request item. For example, in [Figure 2-9](#), the power is downgraded from 19 W to 17.5 W.

Figure 2-9 Downgrading Power Supply in the PoE Mode

- Step 4** Click the **Apply** button. An alert message box will be displayed, as shown in [Figure 2-10](#). It may take about 90 seconds to complete a new power supply request.

Figure 2-10 Power Downgrade Alert Message Box**Note**

Downgrading power supply may cause the device to reboot. Only when the downgrade request succeeds, the new power request will be stored in the Startup-Config. If you want to save the new power request in the Startup-Config disregarding the result, click the **Force Saving** button in the alert message box. If you want to cancel the request, click the **Cancel Request** button in the alert message box.

- Step 5** When the power downgrade request is completed, the result will be displayed on the screen, as shown in [Figure 2-11](#).

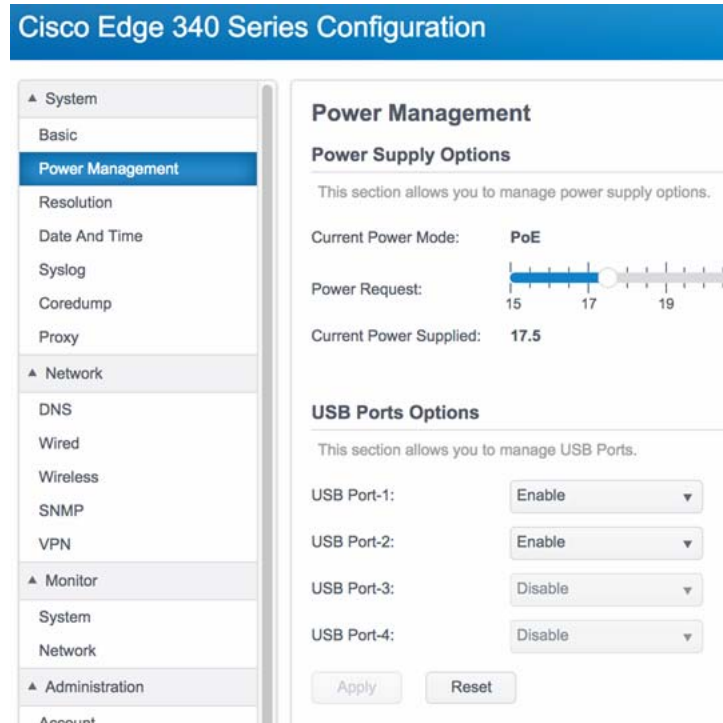
Figure 2-11 Power Downgrade Succeeded

Configuring the USB Ports

You can enable or disable USB ports in the USB Ports Options section on the Power Management page. Follow these steps to enable or disable a USB port:

- Step 1** Click **Power Management** under System in the left pane. The USB Ports Options section is displayed in the right pane under the Power Supply Options section, as shown in [Figure 2-12](#).

Figure 2-12 USB Ports Options

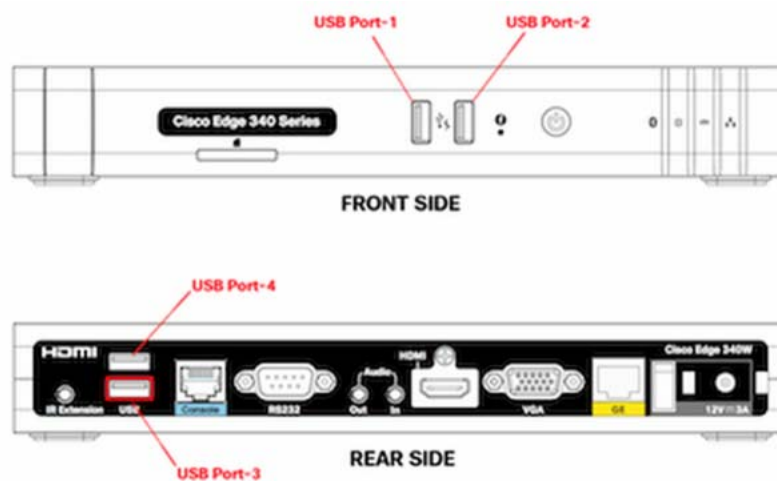


- Step 2** Choose **Enable** or **Disable** from the drop-down list for each USB port.
- Step 3** Click **Apply** to save the changes and **Reset** to restore the previous values.



Note In PoE mode, USB port 3 and port 4 on the rear panel of the device are disabled. [Figure 2-13](#) shows the locations of the USB ports.

Figure 2-13 USB Port Locations on the Panels



Configuring Resolution

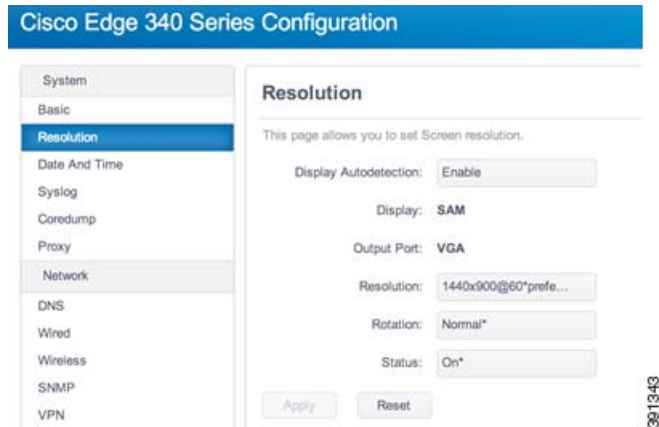
In the **Resolution** tab, you can configure Display Auto detection, Resolution, Rotation, Reflection, and Status of the connected monitor, and view the Screen model and Output port of the monitor. When two monitors are connected, you can configure dual screen settings.

Configuring Single Monitor With Auto Detection Enabled

Follow these steps to configure the resolution information of single monitor when auto detection is enabled:

- Step 1** Click **Resolution** under System in the left pane.
- Step 2** Choose **Enable** from the Display Autodetection drop-down list.

When you choose **Enable** to enable auto detection, you will see different page layout according to the number of monitors that are connected to the Cisco Edge 340 Series. When one monitor is connected, you will see the page as shown in [Figure 2-14](#).

Figure 2-14 Resolution Tab of One Connected Monitor

Step 3 You can view or configure the following information of the monitor:

- **Display**—Displays the name of the monitor. Cannot be configured in auto detection mode.
- **Output Port**—Displays the output port of the monitor: VGA or HDMI. Cannot be configured in auto detection mode.
- **Resolution**—Displays the current resolution of the monitor. You can configure a different resolution in this field.
- **Rotation**—Displays the current rotation mode of the monitor. You can configure a different rotation value in this field.
- **Status**—Displays the current status of the monitor. You can turn on or turn off the monitor in this field.

Step 4 Click **Apply** to save the changes and **Reset** to discard the unsaved changes.

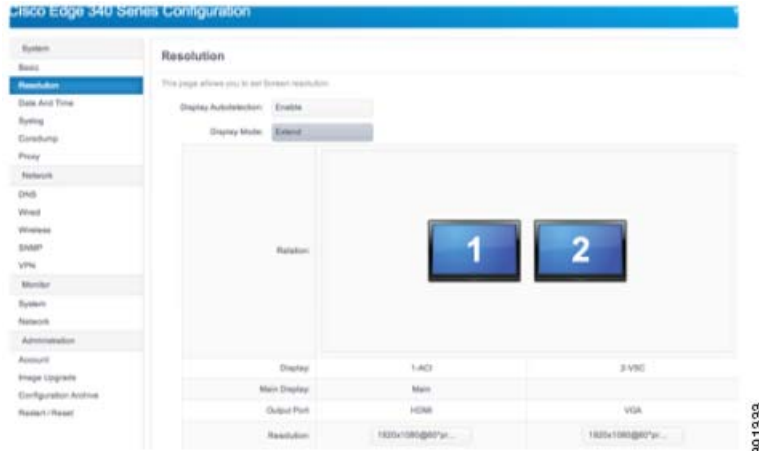
Configuring Dual Monitors With Auto Detection Enabled

Follow these steps to configure the resolution information of dual monitors when auto detection is enabled:

Step 1 Click **Resolution** under System in the left pane.

Step 2 Choose **Enable** from the Display Autodetection drop-down list.

When you choose **Enable** to enable auto detection, you will see different page layout according to the number of monitors that are connected to the Cisco Edge 340 Series. When two monitors are connected to the Cisco Edge 340 Series, you will see the page as shown in [Figure 2-15](#).

Figure 2-15 Resolution Tab of Two Connected Monitors

Step 3 You can view or configure the following information of the monitors:

- **Display Mode**—Displays the current mode of the two monitors. You can configure a different mode in this field. Valid values are Duplicate, Extend, Only Display On Screen 1, Only Display On Screen 2, and Turn Off Display.
- **Relation**—Displays the relation of the two monitors by pictures. Monitor 1 represents the HDMI monitor and monitor 2 represents the VGA monitor. If the value of Display Mode is Extend, you can configure the relation of the two monitors by dragging them directly.
- **Main Display**—Displays the current main monitor.
- **Output Port**—Displays the output port of the monitor: VGA or HDMI. Cannot be configured in auto detection mode.
- **Resolution**—Displays the current resolution of each monitor. You can configure a different resolution in this field.

Step 4 Click **Apply** to save the changes and **Reset** to discard the unsaved changes.

Configuring Resolution With Auto Detection Disabled

When auto detection is disabled, all modes (single, duplicate, and extend) can be configured no matter whether the monitors are connected or not. The resolution list is retrieved from the file `/usr/etc/.force_resolution_list.txt`. There are four modes that you can choose with the options Display Number and Display Mode.

Follow these steps to configure the resolution information when auto detection is disabled:

Step 1 Click **Resolution** under System in the left pane.

Step 2 Choose **Disable** from the Display Autodetection drop-down list. You will see the page as shown in [Figure 2-16](#).

Figure 2-16 Resolution Tab With Auto Detection Disabled


Resolution

This page allows you to set Screen resolution.

Display Autodetection:

Display Number:

Display Mode:

Relation:	
Display:	1&2
Output Port:	HDMI,VGA
Resolution:	<input type="text" value="640x480@60"/>
Rotation:	<input type="text" value="Normal*"/>

381334

Step 3 You can view or configure the following information of the monitors:

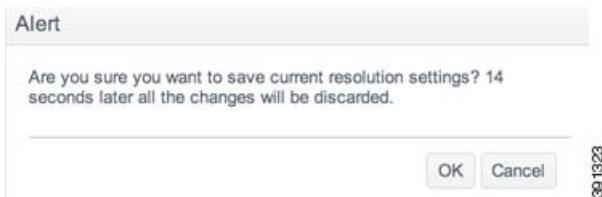
- Display Number—Configures the number of monitors that are connected to the system. Valid values are:
 - No Display—Turns off both monitors.
 - Single Display—Sets a specific monitor and turns off the other.
 - Dual Display—Sets two monitors.
- Display Mode—Displays mode of dual screen when Dual Display is chosen for the Display Number field. You can configure Duplicate or Extend in this field.
- Relation—Displays the relation of the two monitors by pictures.
- Output Port—Configures the output port of the monitor. If Single Display is chosen for the Display Number field, there are three options, HDMI, VGA, and Any. Any means no matter what kind of port the connected monitor has, the setting will take effect.
- Resolution—Configures the resolution of the monitor.
- Rotation—Configures the rotation mode of the monitor.

Step 4 Click **Apply** to save the changes and **Reset** to discard the unsaved changes.

**Note**

When you finish configuring the resolution information, click **Apply** at the bottom of the tab to save the changes. After a few seconds, a dialog will pop up. Click **OK** to confirm the configuration to take effect. If you click **Cancel**, or do not click in 15 seconds, the configuration will be discarded and the last configuration will be restored, as shown in [Figure 2-17](#).

Figure 2-17 Applying the Changes



Configuring Date and Time

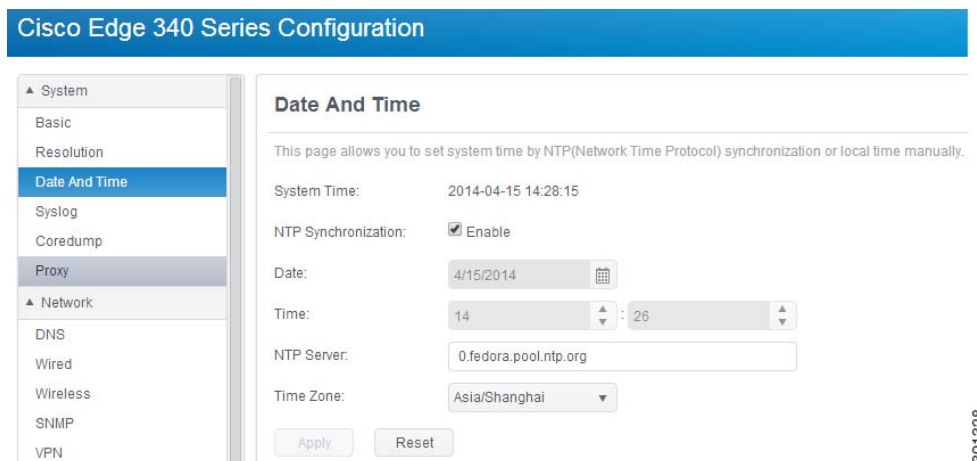
You can configure system date and time, NTP servers and time zone information in the **Date and Time** tab.

Configuring System Time Manually

Follow these steps to configure system time manually:

- Step 1** Click **Date and Time** under System in the left pane. The Date and Time tab is displayed, as shown in [Figure 2-18](#).

Figure 2-18 Date and Time Information



- Step 2** Uncheck the NTP Synchronization option, as shown in [Figure 2-19](#).

Figure 2-19 Configuring Date and Time Manually

NTP Synchronization: Enable

Date:

Time: :

NTP Server:

Time Zone:

391330

- Step 3** In the Date field, enter a date in the format of mm/dd/yyyy, or choose a date by clicking the calendar icon.
- Step 4** In the Time field, enter the current hour and minute in turn, or choose the value of hour and minute by clicking the arrows near the text box.
- Step 5** Choose a time zone from the Time Zone drop-down list.
- Step 6** Click **Apply** to save the changes or **Reset** to restore the previous values.

Configuring System Time by Auto-Sync With NTP Servers

Follow these steps to configure system time by auto-sync with NTP servers:

- Step 1** Click **Date and Time** under System in the left pane. The Date and Time tab is displayed as shown in [Figure 2-18](#).
- Step 2** Check the NTP Synchronization option, as shown in [Figure 2-20](#).

Figure 2-20 Configuring Date and Time by Auto-Sync with NTP Servers

NTP Synchronization: Enable

Date:

Time: :

NTP Server:

Time Zone:

391329

- Step 3** In the NTP Server field, enter the NTP server addresses. Make sure each address is valid. Multiple addresses should be separated by comma.
- Step 4** Choose a time zone from the Time Zone drop-down list.

Step 5 Click **Apply** to save the changes or **Reset** to restore the previous values.

Configuring Syslog

Click **Syslog** under System in the left pane to configure the setting of syslog, as shown in [Figure 2-21](#).

Figure 2-21 Syslog Information

Cisco Edge 340 Series Configuration

System

- Basic
- Resolution
- Date And Time
- Syslog**
- Coredump
- Proxy

Network

- DNS
- Wired
- Wireless
- SNMP
- VPN

Monitor

- System
- Network

Administration

- Account
- Image Upgrade
- Configuration Archive
- Restart / Reset

Log Settings

Options

This page allows you to set local log settings.

Level:

Size: MB

Rotate:

Remote Log

This page allows you to set remote log settings.

Enable: Enable

Server:

Protocol:

Port:

Level:

Systems, Inc. All Rights Reserved. 381346

Configuring Local Syslog

Follow these steps to configure local syslog. The syslog file is `/var/log/messages`.

Step 1 Choose the level of syslog from the **Level** drop-down list:

- Debug
- Info
- Notice
- Warning
- Error
- Critical

- Alert
- Emergency

**Note**

These options are listed in the order from low to high priority. When you specify a priority, the one you choose and all the others that are higher than the one you choose are selected too.

- Step 2** In the Size field, enter the size of the syslog in the left column and choose the unit of the log size from the right drop-down list.
- Size has three units: KB, MB, and GB. The maximum log size is 50 MB, and the default size is 10 MB. If the value you provide exceeds 50 MB, the change fails and the original size is retained.
- Step 3** In the Rotate field, enter the rotation number you want to set. If the log file size exceed the size you set in [Step 2](#), the old log file will be backed up as .tar.gz.1 file and a new file will be created to record syslog. Next time, .tar.gz.1 will be renamed as .tar.gz.2, and the log file will be renamed as .tar.gz.1. The total backup log file will not exceed the rotation number.
- Step 4** Click **Apply** to save the changes and **Reset** to restore the previous values.

Configuring Remote Syslog

Follow these steps to configure remote syslog.

- Step 1** Check the Enable check box to enable remote syslog.
- Step 2** In the Server field, enter the IP address or hostname of the syslog server.
- Step 3** In the Protocol field, choose the protocol, UDP or TCP, that you will use to connect to the syslog server.
- Step 4** Set the port of syslog server in Port field.
- Step 5** Choose the level of syslog from the **Level** drop-down list:
- Debug
 - Info
 - Notice
 - Warning
 - Error
 - Critical
 - Alert
 - Emergency

**Note**

These options are listed in the order from low to high priority. When you specify a priority, the one you choose and all the others that are higher than the one you choose are selected too.

- Step 6** Click **Apply** to save the changes and **Reset** to restore the previous values.

Configuring Coredump

Click **Coredump** under System in the left pane to configure the setting of core dump, as shown in [Figure 2-22](#).

Figure 2-22 Coredump Information

Follow these steps to configure Coredump.

- Step 1** In the Size field, enter the size of the core dump in the left column and choose the unit of the core dump size from the right drop-down list. Setting the size to 0 will disable Coredump. Setting the size to ∞ means the Coredump file size is unlimited.
- Step 2** Click **Apply** to save the changes and **Reset** to restore the previous values. The setting will take effect after you reboot the device.



Note

The existing coredump files are listed in the Coredump Files table. Click **Download** to download the coredump file to your local drive. The download process may be different for different web browser.

Configuring Proxy

Click **Proxy** under System in the left pane to configure HTTP, HTTPS, and FTP proxy, as shown in Figure 2-23.

Figure 2-23 Proxy Information

Follow these steps to configure the setting of proxy.

-
- Step 1** Enter the IP address or hostname and port of the proxy you want to set for an HTTP connection. The port is mandatory when setting proxy. If the IP address or hostname field is left empty, the HTTP Proxy setting will be cleared. If the proxy requires authentication, the IP address or hostname field should be in the format: *username:password@hostname*.
- Examples of Proxy address are as following:
- 10.14.40.14:8080
 - http://username:password@myproxy.com:80
 - proxy.google.com:80
- Step 2** Enter the IP address or hostname and port of the proxy you want to set for an HTTPS connection. The port is mandatory when setting proxy. If the IP address or hostname field is left empty, the HTTPS proxy setting will be cleared. If the proxy requires authentication, the IP address or hostname field should be in the format: *username:password@hostname*.
- Step 3** Enter the IP address or hostname and port of the proxy you want to set for FTP connection. The port is mandatory when setting proxy. If the IP address or hostname field is left empty, the FTP proxy setting will be cleared. If the proxy requires authentication, the IP address/hostname field should be in the format: *username:password@hostname*.
- Step 4** Enter the IP address or hostname in the Bypass Proxy field if you want to connect without proxy. Use a comma to separate multiple proxies.
- Step 5** Click **Apply** to save the changes and **Reset** to restore the previous values. The setting will take effect after you reboot the device.
-

Network Configuration

You can configure DNS, wired, wireless, SNMP, and VPN settings in the Network section.

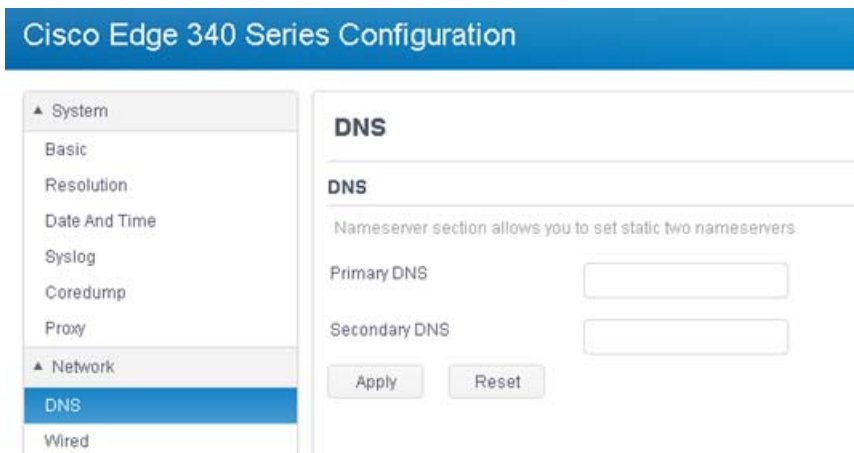
Configuring DNS

You can configure the primary and secondary name servers in the DNS tab. These two DNS servers have the highest priorities of all DNS servers, including DHCP DNS, VPN DNS, and others.

Follow these steps to configure the DNS settings.

- Step 1** Click DNS under Network in the left pane. The DNS tab is displayed, as shown in [Figure 2-24](#).

Figure 2-24 DNS Information



- Step 2** Enter the IPv4 or IPv6 address of the primary and secondary name server in the Primary DNS and Secondary DNS field.



Note When the Primary DNS field is empty, the Secondary DNS must be Empty too.

- Step 3** Click **Apply** to save the changes and **Reset** to restore the previous values.

Configuring Wired Settings

Under the Network tab, click **Wired** in the left pane to configure Link Settings, enable or disable Wake on Lan, configure the IPv4 mode and the IPv6 mode, and configure the 802.1x settings. See [Figure 2-25](#).

Figure 2-25 Wired Information

Cisco Edge 340 Series Configuration

System

- Basic
- Power Management
- Resolution
- Date And Time
- Syslog
- Coredump
- Proxy
- Network
- DNS
- Wired**
- Wireless
- SNMP
- VPN
- Monitor
- System
- Network
- Administration
- Account
- Radius

Wake on Lan:

IPv4 Configuration

This section allows you to set wired IPv4.

Mode:

Address: Netmask:

Gateway:

IPv6 Configuration

This section allows you to set wired IPv6.

Mode:

Address: Subnet Prefix Length:

Gateway:

802.1x Configuration

This section allows you to set wired 802.1x authentication. 802.1x is not supported in WiFi AP mode.

802.1x status:

Follow these steps to configure wired link and address settings.

- Step 1** (Optional) Configure wired link settings.
- Choose a link negotiation mode from the Mode drop-down list. Valid options are:
 - Auto—Auto negotiation on speed and duplex.
 - Manual—Manually set speed and duplex.
 - If you choose Manual mode, choose speed and duplex mode from the Speed and Duplex drop-down list.
 - Choose **Enable** or **Disable** from the Wake on Lan drop-down list, to enable or disable the wake on Lan function.
- Step 2** Set IPv4 address.
- Choose the IPv4 mode from the Mode drop-down list. Valid options are:
 - Automatic (DHCP)—Use DHCP to get IPv4 information and DNS information.
 - Manual—Manually set IPv4 information. The Address and Netmask fields are mandatory. The gateway and IP address must be in the same network.
 - If you choose Manual for the IPv4 mode, enter the IP address, netmask, and gateway address manually.

- Step 3** Set IPv6 address.
- a. Choose the IPv6 mode from the Mode drop-down list. Valid options are:
 - Automatic (DHCP)—Use DHCP to get IPv6 information and DNS information.
 - Manual—Manually set IPv6 information. The Address and Netmask fields are mandatory. The gateway and IP address must be in the same network.
 - b. If you choose **Manual** for the IPv6 mode, enter the IP address, netmask, and gateway address manually.
- Step 4** Configure 802.1x settings—Choose **Enable** or **Disable** from the 802.1x status drop-down list.
- a. If you choose **Enable** from the 802.1x status drop-down list, the screen is displayed as shown in [Figure 2-26](#).

Figure 2-26 Configuring 802.1x Settings

802.1x Configuration

This section allows you to set wired 802.1x authentication. 802.1x is not supported in WiFi AP mode.

802.1x status:	<input type="text" value="Enable"/>	
Authentication Mode:	<input type="text" value="Protected EAP(PEAP)"/>	
Anonymous Identity:	<input type="text"/>	
CA Certificate:	<input type="text"/>	
Inner Authentication:	<input type="text" value="MSCHAPv2"/>	
Username:	<input type="text" value="user2"/>	ACS internal User
Password:	<input type="password" value="....."/>	Password For User2

You need to configure the following parameters,:

- Authentication Mode—EAP method. Valid values are Fast, and Protected EAP (PEAP).
- Username—Used for EAP authentication methods.
- Password—Used for EAP authentication methods.
- Anonymous Identity—Used for EAP authentication methods.
- Identity—Identity string for EAP authentication methods.
- User Certificate—Path of the specified file that contains the user certificate.
- CA Certificate—Path of the specified file that contains the CA certificate.
- Private Key—Path of the specified file that contains the private key.
- Private Key Password—Used to decrypt the private key specified in the Private Key file.

- Automatic PAC Provisioning—Valid value is Disable or Authenticated.
- PAC File—Path of the specified file that contains PAC for EAP-FAST.
- Inner Authentication—Phase two authentication.



Note The fields displayed on the screen are different for each Authentication Mode field. When you choose an authentication mode, the related fields will be displayed.

After you finish all the settings, click **Apply** to save the changes and make the current settings take effect.

- b. To disable the 802.1x function, choose **Disable** from the 802.1x status drop-down list and click **Apply**.

Step 5 Click **Apply** to save the changes and **Reset** to restore the previous values.

Configuring 802.1x - PEAP

Components Used

The information in this document is based on these software and hardware versions:

The Cisco Catalyst Switch 3750E (version 12.2(53) SE2), Cisco Edge 340 Series (version 1.2) and Cisco ACS server (version 5.7) are used in this configuration.



Note The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

On the switch, enter the following commands:

```
interface GigabitEthernet1/0/4
 switchport mode access
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 10
```

Use the following steps to configure the CE340:

- Step 1** Under the Network tab, click **Wired** in the left pane.
- Step 2** Choose **Enable** from the 802.1x status drop-down list.
- Step 3** Choose **Protected EAP (PEAP)** from the Authentication Mode drop-down list.

Figure 2-27 Configuring 802.1x - PEAP Settings

802.1x Configuration

This section allows you to set wired 802.1x authentication. 802.1x is not supported in WiFi AP mode.

802.1x status: Enable

Authentication Mode: Protected EAP(PEAP)

Anonymous Identity:

CA Certificate:

Inner Authentication: MSCHAPv2

Username: user2 ACS internal User

Password: •••••••• Password For User2

Apply
Reset

Step 4 Choose the Inner Authentication that you want, which should be enabled on the ACS server.

Figure 2-28 Inner Authentication Setting

MSCHAPv2 ▼

MSCHAPv2

MD5

GTC

Step 5 The device will get the DHCP IP address once the negotiation is successfully completed between ACS and CE340. This can be confirmed on the ACS server by the menu Monitoring and Reports -> Radius Authentication (see [Figure 2-29](#) for example).

Figure 2-29 Configuring DHCP IP Address on ACS Server

ACSView Timestamp	ACS Timestamp	RADIUS Status	NAS Failure	Details	User Name	MAC/IP Address	Access Service	Authentication Method	Network Device Name	NAS IP	NAS Port Id
2015-08-12 07:01:35.367	2015-08-12 07:01:35.361	✔			user1	1C-AA-07-99-7D-E0	ACS-WIRED	MSCHAPV2	switch	10.104.188.13	GigabitEthernet1

For CE340, choose Wired Information under Monitor, to check the wired IP information. See [Figure 2-30](#).

Figure 2-30 *Wired IP Information on CE340*

Wired IP Information			
IPv4 connection type:	Auto		
IPv4 address:	10.104.188.5	IPv4 netmask:	255.255.255.0
IPv4 default gateway:	10.104.188.1		
IPv6 connection type:	Auto		
IPv6 address:		Subnet prefix length:	
IPv6 default gateway:			

Configuring Wireless Settings

The Cisco Edge 340 Series device supports the following wireless modes:

- Access Point (AP)—A device that allows wireless devices to connect to a wired network using Wi-Fi.
- Station—A wireless connection to connect to the other networks.
- Off—The wireless function is disabled.

To select a desired wireless mode, click **Wireless** in the left pane and configure the settings for each mode.

Configuring AP Mode

If you select **Wi-Fi Access Point** from the **Wi-Fi Operating Mode** drop-down list, you can configure the SSID name, broadcast SSID, wireless mode, channel bandwidth, channel number, security settings, and advanced settings for the AP mode. See [Figure 2-31](#).



Note

The country and region for Wi-Fi AP cannot be selected.

Figure 2-31 AP Mode Settings

Follow these steps to configure the AP mode settings:

-
- Step 1** Enter the SSID name in the SSID field. The length must be within 1–32.
- Step 2** Choose ON or OFF from the Broadcast SSID drop-down list, to enable or disable the broadcast of SSID information.
- Step 3** Choose one of the following mode from the Wireless mode drop-down list:
- 802.11 B/G mixed
 - 802.11 B only
 - 802.11 A only
 - 802.11 G only
 - 802.11 N only
 - 802.11 G/N mixed
 - 802.11 A/N mixed
 - 802.11 B/G/N mixed
 - 802.11 A/G/N mixed (not support)
 - 802.11 N in 5G band only

Step 4 Choose 20MHz or 40MHz from the Channel bandwidth drop-down list.



Note Some wireless mode does not support 40MHz channel bandwidth.

Step 5 Choose a channel number from the Channel number drop-down list. 0 means automatically select wireless channel.

Step 6 Click the **Advanced** button in [Figure 2-31](#) to configure the following settings:

- Transmit power—Wireless Tx power. Valid value is in the range of 1–100.



Note The antenna transmission setting is not provided on WEB GUI. Use the Transmit power drop-down list to set WLAN radio transmit power in percentage.

- Enable IGMP snooping—Enable or disable IGMP snooping.
- AP isolation—Enable or disable AP isolation function.
- Enable WMM APSD—Enable or disable Wi-Fi Multimedia Automatic Power Save Delivery (WMM APSD) function.
- Enable WMM DLS—Enable or disable WMM DLS function.
- Beacon interval—Valid value is in the range of 20–1000.
- DTIM Interval—Valid value is in the range of 1–255.
- Enable Transmit burst—Enable or disable the transmit burst function.
- Preamble Type—Choose one of the following types: Long, Short, and Auto.

Click **Hide** to get back to the simplified mode.

Step 7 Configure the security settings in the Security Settings section:

a. Authentication mode and Encryption mode:

- OPEN
 - NONE
 - WEP
- SHARED
 - WEP
- WPAPSK/WPA2PSK/WPAPSKWPAPSK2/WPA/WPA2/WPAWPA2
 - TKIP
 - AES
 - TKIPAES



Note Some wireless mode may not support all encryption modes.

- b. KeyType—ASCII or HEX. Only valid for OPEN/WEP and SHARED mode. Default key index 1.
- c. Key—All printable ASCII. The length of key should follow these rules:
 - WEP HEX length: 10 or 26
 - WEP ASCII length: 5 or 13

- WPAPSK/WPA2PSK/WPA2PSK length: 8–63
- WPA/WPA2/WPA2 length: 0–64

- d. Radius Server IP—Radius Server IP address.
- e. Radius Server Port—Default value is 1812.

Step 8 Click **Apply** to save the changes and **Reset** to restore the previous values.

Configuring Station Mode

If you select **Wi-Fi Station** from the **Wi-Fi Operating Mode** drop-down list, you can add, edit, remove, connect, and refresh wireless connections in the Station mode, and configure the default route, as shown in [Figure 2-32](#).

Figure 2-32 Wi-Fi Station Settings

The screenshot shows the Cisco Edge 340 Series Configuration web GUI. The main content area is titled "Wireless" and includes the following configuration options:

- Wi-Fi Operating Mode:** Wi-Fi Station
- Default Route:** Wired (connected)
- Wireless Station Set:** Wired (connected), Wireless (not connected)

Below these options is a table of wireless networks with the following columns: SSID, Security Type, Signal Strength, and Status.

SSID	Security Type	Signal Strength	Status
7c4ee9	WPA-PSK-TKIP+AES,WPA2-PSK-TKIP+AES	34%	
7c4f02	WPA-PSK-TKIP+AES,WPA2-PSK-TKIP+AES	29%	
b26e3e	WPA-PSK-TKIP+AES,WPA2-PSK-TKIP+AES	55%	
b27210	WPA-PSK-TKIP+AES,WPA2-PSK-TKIP+AES	50%	
baq911	OPEN	65%	
blizzard	WPA2-EAP-AES	70%	
CiscoCPE	OPEN	39%	
CMCC	OPEN	100%	
CMCC-AUTO	WPA2-EAP-AES	100%	

Configuring Default Route

The Cisco Edge 340 Series has two uplink interfaces, wireless and wired Ethernet. Default route can be either wireless or wired Ethernet.

To configure the default route, choose **Wired** or **Wireless** from the Default Route drop-down list, as shown in [Figure 2-32](#).



Note

The default route configuration is only applicable in Wi-Fi station mode. If you choose wireless for the default route, the device can switch to a wired Ethernet automatically when wireless connection gets lost. If you choose wired Ethernet for the default route, the device cannot detect whether the Ethernet gateway is unreachable. The device will not switch to a wireless route.

Add a Wireless Connection

To add a wireless connection, follow these steps:

- Step 1** Click **Join other network** in the Network Site Survey tab (Figure 2-33), or click **Add new profile** in the Network Connections tab (Figure 2-34).

Figure 2-33 Network Site Survey Tab

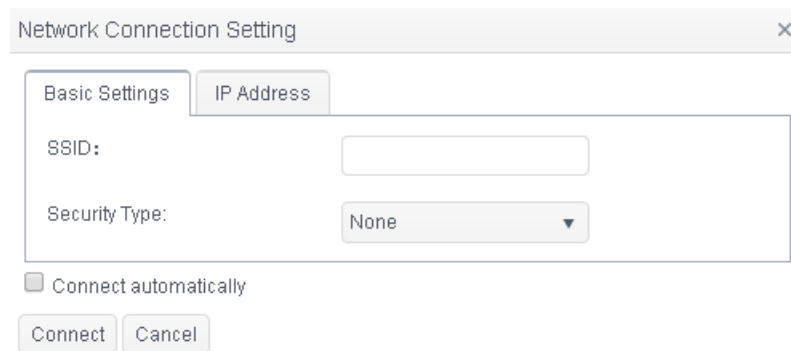


Figure 2-34 Network Connections Tab



- Step 2** The Network Connection Setting screen is displayed, as shown in Figure 2-35.

Figure 2-35 Network Connection Setting



- Step 3** Under the Basic settings tab, enter the name of the wireless connection in the SSID field and choose a security type from the Security Type drop-down list. According to the different security type, different fields will be displayed. Detailed instructions are provided below:

- a. None
- b. WEP
 - WEP Encryption—Control the interpretation of WEP keys.
 - HEX/ASCII—Interpret WEP keys as hexadecimal or ASCII keys.
 - Passphrase—Interpret WEP keys as passphrase.
 - Key—WEP key.
 - Key Index—WEP key index.

- Authentication Mode—Open System/Shared Key.
 - c. WPA Personal/WPA2 Personal/WPA & WPA2 Personal
 - Encryption Type—Set the pairwise encryption capabilities of the specified wireless network.
 - Passphrase—Preshared key for WPA network. The key must be between 8 and 63 ASCII characters.
 - d. WPA Enterprise/WPA2 Enterprise/WPA & WPA2 Enterprise
 - Encryption Type—Set the pairwise encryption capabilities of the specified wireless network.
 - Authentication Mode—Phase1 authentication. Valid values are: TLS/ MSCHAPv2/ Fast/ Tunneled TLS/ Protected EAP.
 - Username—Username used for EAP authentication methods.
 - Password—Password used for EAP authentication methods.
 - Anonymous Identity—Used for EAP authentication methods.
 - Identity—Identity string for EAP authentication methods.
 - User Certificate—Path of the specified file containing the user certificate.
 - CA Certificate—Path of the specified file containing the CA certificate.
 - Private Key—Path of the specified file containing the private key.
 - Private Key Password—The password used to decrypt the private key specified in the Private Key field.
 - Automatic PAC Provisioning—Disable/Anonymous/Authenticated/Both
 - PAC File—Path of the specified file containing PAC for EAP-FAST.
 - Inner Authentication—Phase2 authentication. The value of this field is related to the Authentication Mode field.
- Step 4** (Optional) If you do not have a DHCP server, click the **IP Address** tab to enter IPv4 or IPv6 address information.
- Step 5** If you check the **Connect automatically** option, the wireless network will be connected automatically when the wireless network is available.
- Step 6** Click **Connect** or **Add** to add the wireless network.
-

Edit a Wireless Connection

To edit a wireless connection, follow these steps:

- Step 1** Choose the wireless connection that you want to edit and click **Edit a profile** in the Network Connections tab (Figure 2-34). The Network Connection Setting screen is displayed.
- Step 2** Choose the Security Type option or edit the IP address information as required, then click **Save**.



Note For detailed information about security options, see the [“Add a Wireless Connection”](#) section on page 2-27.

**Note**

If a wireless network is connected successfully, it cannot be edited or removed unless it is disconnected.

Remove a Wireless Connection

To remove a wireless connection, follow these steps:

- Step 1** Select the wireless connection that you want to remove from the Network Connections tab.
- Step 2** Click **Delete** to remove the wireless connection.

**Note**

A connection that has been connected will not be deleted directly. It will be restored after rebooting.

Connect a Wireless Network

To connect a wireless network, follow these steps:

- Step 1** Select a wireless network in the Network Site Survey tab or select a network connection in the Network Connections tab.
- Step 2** Click **Connect** to connect the wireless network.
- If you have entered incorrect settings information when you add or edit wireless connections, the message “Connection failed” is displayed in red. The edit dialog box will also be displayed. Correct the settings and click **Connect** to connect the wireless network again.
- Step 3** If the connection is successful, the Connected status will be displayed in the Status column of the Network Site Survey table, as shown in [Figure 2-36](#).

Figure 2-36 Network Connected Successfully

SSID	Security Type	Signal Strength	Status
blizzard	WPA2-EAP-AES	100%	Connected
10001	WPA-PSK-TKIP+AES,WPA2-PSK-TKIP+AES	52%	
10010	WPA-PSK-TKIP+AES,WPA2-PSK-TKIP+AES	70%	

Refresh Network Site Survey

Click **Refresh** in the Network Site Survey tab to rescan the wireless networks.

Disconnect From Connected Wireless Network

To disconnect from a connected wireless network, follow these steps:

-
- Step 1** Select a connected wireless network in the Network Site Survey tab, or select the network connection which is in use in the Network Connections tab.
 - Step 2** Click **Disconnect** to disconnect the wireless network.
-

Disable the Wireless Function

To disable the wireless function, choose **Wi-Fi off** from the **Wi-Fi Operating Mode** drop-down list in the Wireless tab.

Configuring SNMP

Cisco Edge 340 series supports SNMP v1,v2, and v3. By default, SNMP v1 or v2 support is disabled.

To configure the SNMP service, click **SNMP** in the left pane, as shown in [Figure 2-37](#).

Figure 2-37 Enabling SNMP

The screenshot displays the Cisco Edge 340 Series Configuration web interface. The top navigation bar includes the title 'Cisco Edge 340 Series Configuration', the user 'Admin', and language options 'English' and 'Log out'. The left sidebar shows a tree view with 'SNMP' highlighted under the 'Network' section. The main content area is titled 'SNMP' and contains the following configuration options:

- SNMP Option:** Enable
- SNMP Trap:**
 - Trap Option:** Enable
 - Trap Receiver:** 10.0.1.1
 - Trap Version:** V2
 - CPU Usage Threshold:** 50 %
 - Temperature Threshold:** 50 C
 - Memory Threshold:** 50 %
 - Disk Usage Threshold:** 50 %
 - Monitor Frequency:** 40 s
 - Syslog Severity:** Critical
 - Interface Monitor:** HDMI or VGA USB Device SD Card






Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

Enabling SNMP

To enable SNMP, check the **Enable** check box next to the SNMP Option field in [Figure 2-37](#).

Configuring SNMP Trap

To configure an SNMP trap, follow these steps:

-
- Step 1** Click the SNMP Trap tab as shown in [Figure 2-37](#).
- Step 2** Check or uncheck the Enable check box next to the Trap Option field. The check box is disabled by default.
- Step 3** Enter the IP address or hostname in the Trap receiver field.
- Step 4** Choose v1, v2 or v3 from the Trap version drop-down list. Default is v2.
-  **Note** To enable SNMP v1 or v2, at least one community string should be added in the Community Strings tab.
-
- Step 5** Enter a CPU usage percentage in the CPU Usage Threshold field. Default is 50%, and the minimum is 10%.
- Step 6** Enter a CPU temperature threshold value in the Temperature Threshold field. Default is 50 C. The range is from 50 C to 200 C.
- Step 7** Enter a memory usage threshold value in the Memory Threshold field. Default is 50%, and the minimum is 10%.
- Step 8** Enter a disk use percentage in the Disk Usage Threshold field. Default is 50%, and the minimum is 10%.
-  **Note** Disk usage monitoring includes only / and /home usages.
-
- Step 9** Enter a trap monitor frequency value in the Monitor Frequency field. Default is 60 seconds. The range is from 50 s to 200 s.
- Step 10** Choose a syslog severity level from the Syslog Severity field. Default is critical.
-  **Note** Syslog level sets the rsyslog level which will be sent over SNMP trap to the trap receiver.
-
- Step 11** Enable or disable HDMI/USB/SD card monitor by checking or unchecking the Enable check boxes next to the **HDMI or VGA**, **USB Device**, and **SD Card** fields. Default is disabled.
- Step 12** Click **Apply** to save the changes and **Reset** to restore the previous values.
-  **Note** Enabling USB trap will cause SNMP service to restart a bit slowly. USB trap reports all attached internal and external devices.
-
-  **Note** The SNMP trap configuration change will cause SNMP service to restart for changes to take effect.
-

Adding an SNMP User

To add an SNMP user, follow these steps:

- Step 1** Click the Users tab in [Figure 2-37](#) and then click **Add new user**, as shown in [Figure 2-38](#).

Figure 2-38 Configuring SNMP Users

The screenshot shows the Cisco Edge 340 Series Configuration web interface. The top navigation bar includes 'Cisco Edge 340 Series Configuration', 'Welcome Admin', 'English', 'Log out', and the Cisco logo. A left-hand navigation menu is visible, with 'SNMP' selected under the 'Network' section. The main content area is titled 'SNMP' and contains the following elements:

- A sub-header: 'This page allows you to set SNMP.'
- An 'SNMP Option' section with an 'Enable' checkbox.
- Three tabs: 'SNMP Trap', 'Users' (selected), and 'Community Strings'.
- A 'Users' section with '+ Add new user' and 'X Delete user' buttons.
- A table with the following data:

ID	User Name
1	abcd12345

© 2013 Connected Platform Group, Cisco Systems, Inc. All Rights Reserved.

- Step 2** The Add snmp user screen is displayed, as shown in [Figure 2-39](#).

Figure 2-39 Adding SNMP User

The screenshot shows the 'Add New SNMP User' form. The form is titled 'Add New SNMP User' and contains the following fields and controls:

- Username:** A text input field.
- Authentication:** A dropdown menu with 'SHA' selected.
- Authentication Password:** A text input field.
- Private Key:** A dropdown menu with 'AES' selected.
- Private Key Password:** A text input field.
- Buttons:** 'Add' and 'Cancel' buttons at the bottom left.

391318

- Step 3** Enter username, authentication password, and private key password with any strings which contain more than 8 characters without space or tab.
- Step 4** Click **Save** to create the SNMP user. Now you can use any SNMP client which supports SNMP v3 to access Cisco Edge 340 series.



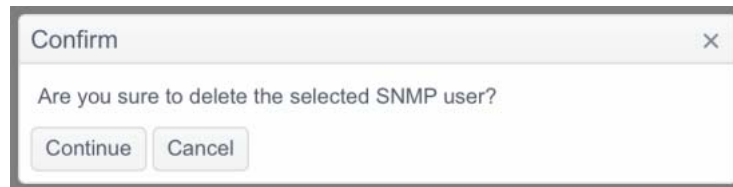
Note For the adding SNMP user to take effect, the SNMP service need to be restarted.

Delete an SNMP User

To delete an SNMP user, follow these steps:

- Step 1** Select the SNMP user that you want to delete.
- Step 2** Click **Delete**. A confirmation window is displayed, as shown in [Figure 2-40](#).

Figure 2-40 Deleting an SNMP User



- Step 3** Click **Continue** to delete the SNMP user or **Cancel** to abort the deleting operation.



Note For the deleting SNMP user to take effect, the SNMP service need to be restarted.

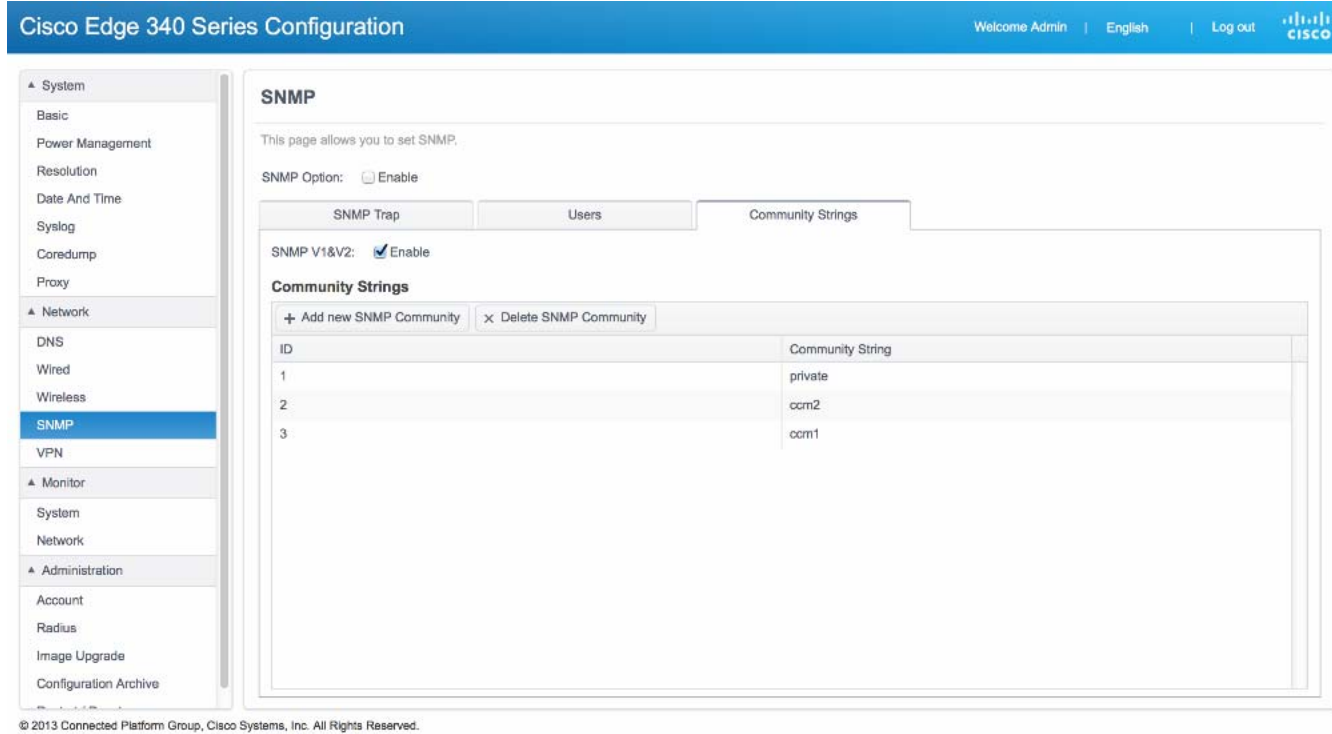
Changing User Password

Cisco Edge 340 series does not support to change user password. However, you can delete the user from the database, then add the user with the same user name but with a different password and private key.

Enabling SNMP V1 and V2

To enable SNMP V1 or V2, check the Enable check box next to the SNMP V1&V2 field as shown in [Figure 2-41](#).

Figure 2-41 Enabling SNMP V1 and V2



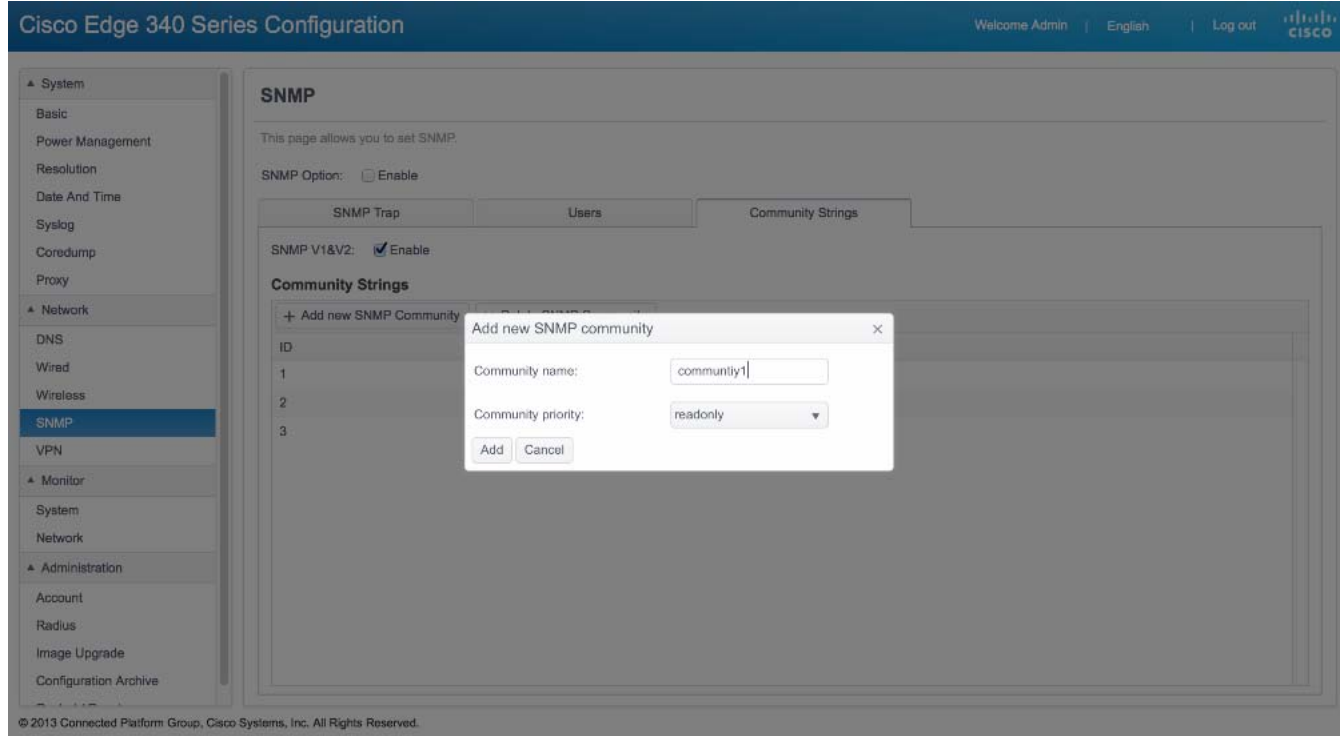
Adding Community Strings

Community string is used for SNMP version 1 and version 2. At least one community string should be configured if you want to query SNMP MIB through v1 or v2.

To add an SNMP community string, follow these steps:

-
- Step 1** Click the Community Strings tab in the SNMP window and then click **Add new SNMP community**. The Add new SNMP community screen is displayed, as shown in [Figure 2-42](#).

Figure 2-42 Adding Community Strings



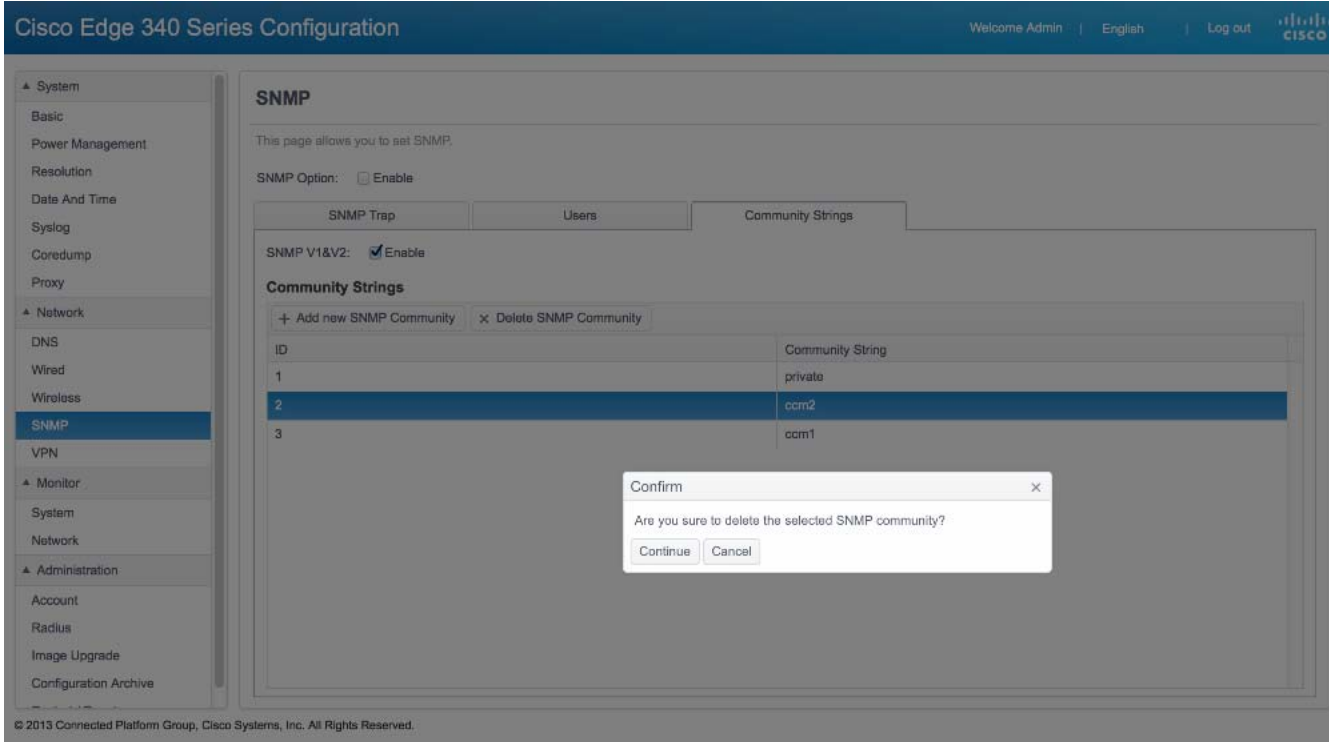
- Step 2** Enter a name in the Community name field.
- Step 3** Choose the priority from the Community priority drop-down list.
- Step 4** Click **Add** to save the new SNMP community.

Deleting an SNMP Community String

To delete an SNMP community string, follow these steps:

- Step 1** Select the SNMP community string that you want to delete from the Community Strings list.
- Step 2** Click **Delete SNMP Community** and then click **Continue** in the Confirm window as shown in [Figure 2-43](#).

Figure 2-43 Deleting Community Strings



Configuring VPN

Cisco Edge 340 Series supports the following types of VPN connections:

- PPTP
- IPSEC/L2TP/PSK
- IPSEC/L2TP/RSA
- CISCO (supports PSK and Hybrid for authentication mode)

To add, edit, and remove a VPN connection, or connect to a VPN, click **VPN** in the left pane. The VPN information window is displayed, as shown in [Figure 2-44](#).

Figure 2-44 VPN Information

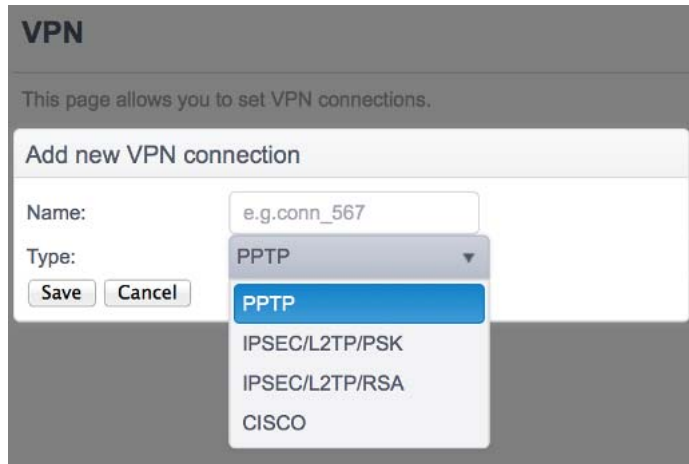
The screenshot shows the Cisco Edge 340 Series Configuration web GUI. The left navigation pane is expanded to the 'VPN' section under the 'Network' tab. The main content area is titled 'VPN' and contains a table of VPN connections. The table has columns for 'VPN Name', 'VPN Type', 'VPN Server', and 'VPN Status'. There is one entry with the name 'test1', type 'CISCO', and status 'DISCONNECTED'. Above the table are buttons for '+ Add', 'Edit', 'x Delete', 'Connect', and 'Disconnect'. Below the table is a 'Restart / Reset' link. The footer of the page reads '© 2013 Connected Platform Group, Cisco Systems, Inc. All Rights Reserved.'

VPN Name	VPN Type	VPN Server	VPN Status
test1	CISCO		DISCONNECTED

Adding a VPN connection of PPTP Type

To add a VPN connection of PPTP type, follow these steps:

-
- Step 1** Click **VPN** in the left pane under the Network tab.
 - Step 2** Click **Add** in the right pane. A new window is displayed, as shown in [Figure 2-45](#).

Figure 2-45 Add New VPN Connection

The screenshot shows a web interface titled "VPN" with a sub-header "This page allows you to set VPN connections." Below this is a form titled "Add new VPN connection". The form has two main fields: "Name:" with a text input containing "e.g.conn_567", and "Type:" with a dropdown menu. The dropdown menu is open, showing a list of options: "PPTP" (highlighted in blue), "IPSEC/L2TP/PSK", "IPSEC/L2TP/RSA", and "CISCO". Below the form are two buttons: "Save" and "Cancel".

- Step 3** Enter the name of the VPN connection that you want to add in the Name field.
 - Step 4** Choose the type of the VPN connection from the Type drop-down list.
 - Step 5** Click **Save** to add the VPN connection.
 - Step 6** The VPN connection table is updated to show the name and status of the new VPN connection.
-

Editing a VPN connection of PPTP Type

To edit a VPN connection of PPTP type, follow these steps:

- Step 1** Click **VPN** in the left pane under the Network tab.
- Step 2** Select the target connection in the right pane and click **Edit**. The Edit a connection window is displayed, as shown in [Figure 2-46](#).

Figure 2-46 Edit a VPN Connection of PPTP Type

Edit a connection

Name: test_link1

Type: PPTP

Server: IP address or hostname

MTU: 0

MRU: 0

Username: e.g.bob2008, or Joe_v5

Password: space is not allowed

Show password

Protocol: PAP CHAP MSCHAP MSCHAPv2

MPPE: None

Connect automatically

Default route

Save Cancel

391354

- Step 3** If the type of the target connection is PPTP, enter the required VPN server address, username, and password in the Server, Username, and Password fields. Check the Show password check box if you want the password to be displayed in plain text.



Note The fields other than server, username, and password are optional. You can obtain the information from your VPN service provider.

- Step 4** (Optional) Enter the value of the Maximum Transmission Unit (MTU) and the Maximum Receive Unit (MRU).
- Step 5** (Optional) Choose the protocols that you want to use with this VPN connection.
- Step 6** (Optional) Choose the MPPE encryption type from the MPPE drop-down list.
- Step 7** Check the Connect automatically check box if you want the Cisco Edge 340 Series device to automatically connect to this VPN.
- Step 8** Click **Save** to save the changes and **Cancel** to restore the previous values.

Editing a VPN connection of IPSEC/L2TP/PSK Type

To edit a VPN connection of IPSEC/L2TP/PSK type, follow these steps:

- Step 1** Click **VPN** in the left pane under the Network tab.
- Step 2** Select the target connection in the right pane and click **Edit**. The Edit a connection window is displayed, as shown in [Figure 2-47](#).

Figure 2-47 Edit a VPN Connection of IPSEC/L2TP/PSK Type

Edit a connection

Name:

Type:

Server:

MTU:

MRU:

Username:

Password:

Show password

Protocol: PAP
 CHAP
 MSCHAP
 MSCHAPv2

MPPE:

Pre-shared Key:

Show password

Length Bit:

Redial:

Connect automatically
 Default route

381355

- Step 3** Enter the name of the VPN connection in the Name field.
- Step 4** Enter the VPN server address, username, and password in the Server, Username, and Password fields. Check the **Show password** check box if you want the password to be displayed in plain text.
- Step 5** (Optional) Enter the value of the MTU and the MRU.
- Step 6** (Optional) Choose the protocols that you want to use with this VPN connection.
- Step 7** (Optional) Choose the MPPE encryption type from the MPPE drop-down list.
- Step 8** Enter the preshared key in the Pre-shared Key field.
- Step 9** (Optional) Choose Yes or No from the Redial drop-down list. If you choose Yes, you should enter values for the Timeout and Attempts fields ([Figure 2-48](#)).

Figure 2-48 Redial Information

Redial:	Yes
Timeout:	
Attempts:	

- Timeout—The maximum time to connect the VPN server every time.
- Attempts—The maximum number of attempts made to connect the VPN server.

The value of Timeout multiplied by the value of Attempts is the time taken to connect the VPN server.

- Step 10** Check the Connect automatically check box if you want the Cisco Edge 340 Series device to automatically connect to this VPN.
- Step 11** Click **Save** to save the changes and **Cancel** to restore the previous values.
-

Editing a VPN connection of IPSEC/L2TP/RSA Type

To edit a VPN connection of IPSEC/L2TP/RSA type, follow these steps:

- Step 1** Click **VPN** in the left pane under the Network tab.
- Step 2** Select the target connection in the right pane and click **Edit**. The Edit a connection window is displayed, as shown in [Figure 2-49](#).

Figure 2-49 Edit a VPN Connection of IPSEC/L2TP/RSA Type

Edit a connection

Name:

Type:

Server:

MTU:

MRU:

Username:

Password:
 Show password

Protocol: PAP
 CHAP
 MSCHAP
 MSCHAPv2

MPPE:

Private Key File:

Client Certificate File:

Server Certificate File:

CA Certificate File(optional):

Length Bit:

Redial:

Connect automatically
 Default route

381356

- Step 3** Enter the name of the VPN connection in the Name field.
- Step 4** Enter the VPN server address, username, and password in the Server, Username, and Password fields. Check the **Show password** check box if you want the password to be displayed in plain text.
- Step 5** (Optional) Enter the value of the MTU and the MRU.
- Step 6** (Optional) Choose the protocols that you want to use with this VPN connection.
- Step 7** (Optional) Choose the MPPE encryption type from the MPPE drop-down list.
- Step 8** Enter the paths of the private key file, client certificate file, and server certificate file.
- Step 9** (Optional) Enter the path of CA certificate file.
- Step 10** Choose Yes or No from the Redial drop-down list. If you choose Yes, enter the relevant values in the Timeout and Attempts fields. The value of Timeout multiplied by the value of Attempts is the time taken to connect the VPN server.

Step 11 Click **Save** to save the changes and **Cancel** to restore the previous values.

Editing a VPN connection of CISCO Type

To edit a VPN connection of CISCO type, follow these steps:

- Step 1** Click **VPN** in the left pane under the Network tab.
- Step 2** Select the target connection in the right pane and click **Edit**. The Edit a connection window is displayed, as shown in [Figure 2-50](#).

Figure 2-50 Edit a VPN Connection of CISCO Type

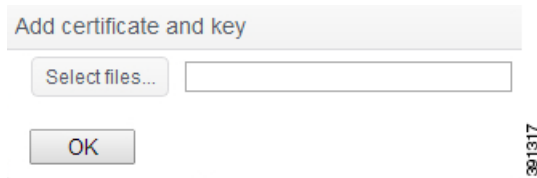
The screenshot shows the 'Edit a connection' window with the following fields and options:

- Name: test2
- Type: CISCO
- Server: IP address or hostname
- MTU: 0
- MRU: 0
- Authentication Mode: PSK
- Group Name: (empty)
- Group Password: (empty) with a Show password checkbox.
- Username: e.g. bob2008, or Joe_v5
- Password: space is not allowed with a Show password checkbox.
- Domain: (empty)
- Encryption: Secure
- NAT Traversal: Cisco
- IKE DH Group: 2
- Connect automatically
- Default route
- Buttons: Save, Cancel

- Step 3** Enter the name of the VPN connection in the Name field.
- Step 4** Enter the VPN server address, group name, username, and password in the Server, Group name, Username, and Password fields. Check the **Show password** check box if you want the password to be displayed in plain text.
- Step 5** (Optional) Enter the value of the MTU and the MRU.

- Step 6** Select PSK or Hybrid from the Authentication Mode drop-down list.
- If you choose PSK, enter the group password.
 - If you choose Hybrid, enter the group password and add the certificate file (Figure 2-51).

Figure 2-51 Add Certificate File



- Step 7** Click **Save** to save the changes and **Cancel** to restore the previous values.
-

Connecting a VPN Connection

To connect a VPN connection, select the VPN connection that you want to connect from the connection list in the VPN tab, and click **Connect**.

Disconnecting a VPN Connection

To disconnect a VPN connection, select the VPN connection that you want to disconnect from the connection list in the VPN tab, and click **Disconnect**.

Deleting a VPN Connection

To delete a VPN connection, select the VPN connection that you want to delete from the connection list in the VPN tab, and click **Delete**. You cannot delete a connection which is in connected or connecting status. You must disconnect it from the VPN server at first, then delete it again.

Monitoring the Status of System and Network

You can monitor the status of the Cisco Edge 340 Series system and the network using the Monitor tab.

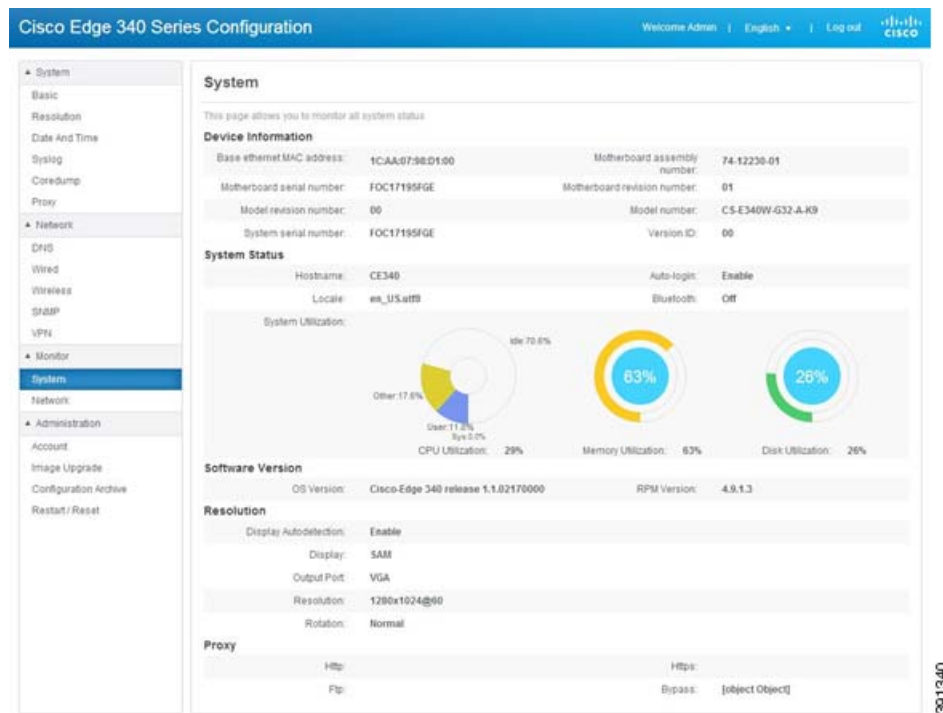
Monitoring the System

Click **System** under Monitor in the left pane to monitor the system status. The System tab is displayed as shown in [Figure 2-52](#).

The System tab shows the basic device information, system status, software version information, current resolution settings, and the proxy settings.

The three pie charts in the System Utilization section indicate the CPU, memory, and disk usage.

Figure 2-52 System Information



Monitoring the Network

Click **Network** under Monitor in the left pane to monitor the network status. The Network tab is displayed as shown in [Figure 2-53](#).

Figure 2-53 Network Information

The screenshot shows the Cisco Edge 340 Series Configuration web GUI. The left navigation pane has 'Network' selected under the 'Monitor' section. The main content area displays the following information:

Network

This page allows you to monitor all network status.

Wired

Link status:	Connected	Speed:	1000
Duplex:	Full Duplex		

Wired IP Information

IPv4 connection type:	Auto		
IPv4 address:	64.104.163.15	IPv4 netmask:	255.255.255.128
IPv4 default gateway:	64.104.163.1		
IPv6 connection type:	Auto		
IPv6 address:		Subnet prefix length:	
IPv6 default gateway:			

DNS

Primary DNS Server:	64.104.123.245		
Secondary DNS Server:	171.70.168.183	Alternative DNS Server:	

Wireless Station

Current work mode is Station

CDP Information

Device ID:	shn15-21-sw2.cisco.com	IP address:	64.104.163.6
Port ID:	GigabitEthernet2/21	Capabilities:	Router,Switch,IGMP
IP network prefix:	64.104.163.0/25	Vip management domain:	shn15-21-sw2
Native VLAN ID:	302	Duplex:	Full Duplex
App VLAN ID:	402	Management address:	64.104.163.6
Power available:	0,-1	Hardware model:	cisco WS-C4510R+E
Software version:	Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500e-UNIVERSALK9-M), Version 15.1(2)SG1, RELEASE SOFTWARE (fc3) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2013 by Cisco Systems, Inc. Compiled Tue 23-Jul-13 09:53 by prod_rel_team		

VPN

Status:	Disconnected
---------	--------------

The Network tab contains information about wired connection, wired IP, wireless mode, wireless connection status, wireless IP, DNS information, and CDP in the following sections:

- **Wired section**—Displays the basic wired link status, speed and duplex.
- **Wired IP information section**—Displays address related items for both IPv4 and IPv6.
- **Wireless section**—Displays different contents in different Wi-Fi mode: Off mode, Station mode, and AP mode.
- **CDP Information Section**—Displays received information from the CDP PSE device(s).
- **VPN Section**—Displays VPN connection status. If connected, displays the connection profile name.

Administration

You can manage the account information, perform image upgrade and configuration archive, and restart or reset the Cisco Edge 340 Series device in the Administration section.

Configuring Account Information

You can configure the following account information on this page:

- [Configuring System Account Information, page 2-47](#)
- [Configuring System Account Reimage Passcode, page 2-48](#)
- [Configuring Web GUI Account Information, page 2-48](#)

Configuring System Account Information

Follow these steps to configure the system account information:

- Step 1** Click **Account** in the left pane. The Account page is displayed ([Figure 2-54](#)).

Figure 2-54 Account Information

Cisco Edge 340 Series Configuration

Account

System Account

This section allows you to manage system account.

User Type:

* Current Root Password:

New Password:

Confirm Password:

Reimage Passcode:

Show Passcode

WebGUI Account

This section allows you to set WebGUI account. The WebGUI login password is the same as the system root password.

WebGUI Login Name:

Notice
All fields with * are required

- Step 2** From the User Type drop-down list, choose the user type that you want to change the username or password for it.
- Step 3** In the Current Root Password field, enter the password of **root**.

Step 4 (Optional) In the Username field, enter a new username for the user account.



Note Follow these rules when you change the username:
 Username should start with alphabet, digit, “_” or “.”;
 Other letters in username could be alphabet, digit, “_”, “-” or “.”;
 Username should be less than 32 letters.

Step 5 (Optional) In the New Password field, enter a new password. In the Confirm Password field, enter the new password again.



Note Follow these rules when you change the password:
 Password should not be less than 8 characters;
 The new password should contain characters from at least three of the following classes: lower case letters, upper case letters, digits, and special characters;
 No character in the new password should be repeated more than three times consecutively;
 The new password should be neither the same as the associated username, nor the reversed username.

Step 6 Click **Apply** to save the changes and **Reset** to restore the previous values.

Configuring System Account Reimage Passcode

Follow these steps to configure the Reimage Passcode information:

Step 1 Click **Account** in the left pane.

Step 2 From the User Type drop-down list, select the user type **Root**.

Step 3 In the Current Root Password field, enter the password of **root**.

Step 4 In the Reimage Passcode field, enter a new passcode.



Note Follow these rules when you configure Reimage Passcode:
 Passcode should be 6 numbers.
 When you click Show Passcode checkbox, the Passcode will be showed.

Step 5 Click **Apply** to save the changes and **Reset** to restore the previous values.



Note Reimage Passcode can be configured with other parts in this page.

Configuring Web GUI Account Information

In the Web GUI Account section, you can change the Web GUI login name.

Follow these steps to configure the Web GUI account information:



Note The Web GUI login password is the same as the system root password.

Step 1 Click **Account** in the left pane.

Step 2 In the Web GUI Login Name field, enter a new login name.



Note Follow these rules when you change the Web GUI login name:
 The Web GUI login name should start with alphabet, digit, '_' or '-'.
 Other letters in the Web GUI login name could be alphabet, digit, '_', '-' or '.'.
 The Web GUI login name should be less than 32 letters.

Step 3 Click **Apply** to save the changes and **Reset** to restore the previous values.

Configuring Radius Information

To configure the Radius information, click **Radius** in the left pane. The Radius information window is displayed, as shown in [Figure 2-55](#).

Figure 2-55 Radius Information

The screenshot shows the Cisco Edge 340 Series Configuration web GUI. The page title is "Cisco Edge 340 Series Configuration" and the user is "Admin". The left navigation pane shows "Radius" selected under "Administration". The main content area shows the "Radius" configuration page. The "Radius Option" checkbox is checked, indicating that the Radius service is enabled. Below this is a "Radius Server" table with one server entry.

Index	Server IP/Domain	Port	Timeout(s)
1	192.168.12.12	50	5

Enabling Radius

To enable Radius service, check the Enable check box next to the Radius Option field as shown in [Figure 2-55](#).

Configuring Radius Server

To identify whether the Radius users have administrative permissions of the Cisco Edge 340 series, Radius server admin should add a predefined authorization profile to the specific admin group in the current system.

The profile should be configured as the specification shown in [Figure 2-56](#).

Figure 2-56 Example of Radius Authorization Profile

Attribute-ID:	26(Vendor-Specific)
Vendor-ID:	9(Cisco)
Vendor-Type:	1(Cisco-AV-Pairs)
Vendor-Content:	ce340-admin

Adding Radius Server

Follow these steps to add a Radius server:

-
- Step 1** Click **Add new server** as shown in [Figure 2-55](#).
 - Step 2** The Add new radius sever screen is displayed, as shown in [Figure 2-57](#)

Figure 2-57 Add New Radius Server

- Step 3** Enter values in the Sever IP/Domain, Port, Timeout and Key fields.
- Step 4** Click **Save** to create the radius server and the new server will be displayed in the server list in [Figure 2-55](#); Or click **Cancel** to exit the Add new radius server screen.



Note

The maximum number of Radius Server is 5. If you check the Show Key checkbox, the key will be showed.

Editing Radius Server

Follow these steps to edit a Radius server:

-
- Step 1** Click **Edit a server** as shown in [Figure 2-55](#).
 - Step 2** The Edit a radius sever screen is displayed, as shown in [Figure 2-58](#)

Figure 2-58 Edit Radius Server

- Step 3** Edit the Timeout and Key fields. The Server IP/Domain and Port fields cannot be changed.
- Step 4** Click **Save** to update the radius server or **Cancel** to exit the Edit radius server screen.

Deleting Radius Server

Follow these steps to delete a Radius server:

- Step 1** Select the radius server that you want to delete in the server list in [Figure 2-55](#).
- Step 2** Click **Delete**. A confirmation window is displayed, as shown in [Figure 2-59](#).

Figure 2-59 Confirmation Message to Delete a Radius Server

- Step 3** Click **Continue** to delete the radius server or **Cancel** to abort the delete operation.

Changing the Priority of Radius Sever

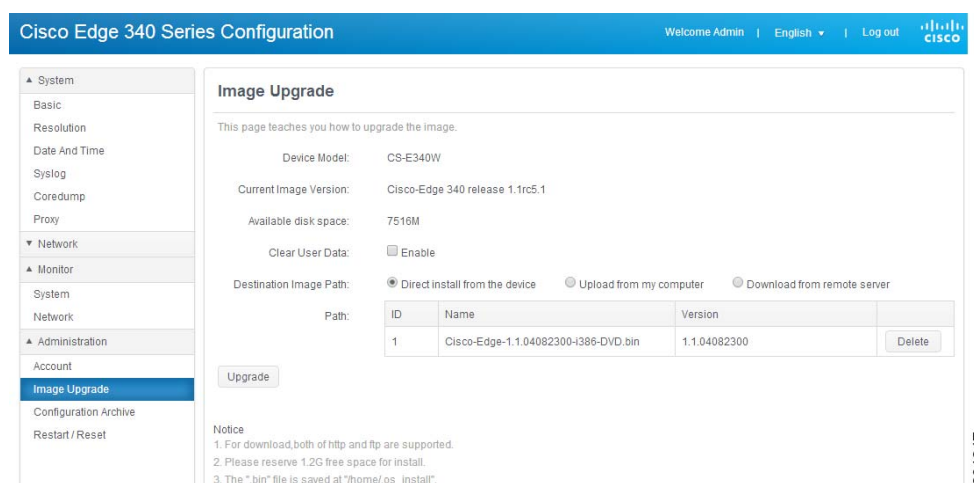
Radius servers displayed in the server list in [Figure 2-55](#) are sorted by priorities in descending order. Follow these steps to change the priority of the a radius server:

- Step 1** Select the radius server that you want to change priority in [Figure 2-55](#).
- Step 2** Click **Move up** or **Move down** to change the priority.

Configuring Image Upgrade

Click **Image Upgrade** under Administration in the left pane to upgrade image version of the Cisco Edge 340 Series device. This page also shows the model number, current image version, and available disk space on the device. You can choose whether to clear user data under /home directory or not, as shown in [Figure 2-60](#).

Figure 2-60 Image Upgrade



There are three ways to perform the image upgrade:

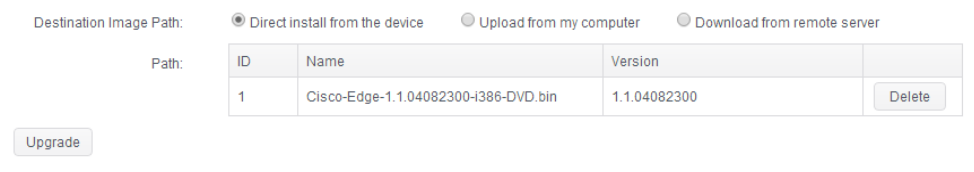
- [Upgrade From the Device Locally](#)
- [Upgrade by Uploading the Image File From My Computer](#)
- [Upgrade by Downloading the Image File From a Remote Server](#)

Upgrade From the Device Locally

Follow these steps to perform image upgrade from the device locally:

- Step 1** Click **Image Upgrade** under Administration in the left pane.
- Step 2** Choose **Direct install from the device** in the Destination Image Path section, as shown in [Figure 2-61](#).

Figure 2-61 Image Upgrade From Device



- Step 3** In the Path section, click a row to select the image from the table. If there is no image file on the device, upload or download one. The image files on the device can be removed by clicking **Delete** from the table.
- Step 4** Click **Upgrade**. In the popup window, click **Continue** to install the selected image.

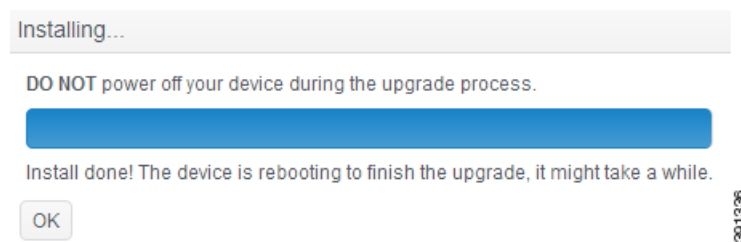
- Step 5** If no error happens in the installation preparing stage, a window as shown in [Figure 2-62](#) will show up to demonstrate the installation progress; otherwise, related error message will be printed under the progress bar.

Figure 2-62 Image Upgrade Progress



- Step 6** If the installation is successful, a window as shown in [Figure 2-63](#) is displayed.

Figure 2-63 Image Upgrade Successful



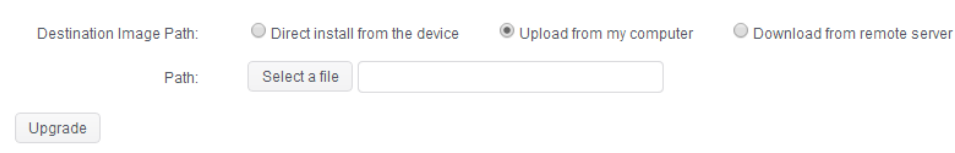
After that, the device will reboot to finish the whole upgrade progress.

Upgrade by Uploading the Image File From My Computer

Follow these steps to perform image upgrade by uploading the image file from my computer:

- Step 1** Click **Image Upgrade** under Administration in the left pane.
- Step 2** Choose **Upload from my computer** in the Destination Image Path section, as shown in [Figure 2-64](#).

Figure 2-64 Image Upgrade by Uploading the Image From My Computer



- Step 3** Click **Select a file** to select an image file from my computer. Make sure that the file is properly named in the form of *Cisco-Edge-xxx-i386-DVD.bin*, and is a valid image file.
- Step 4** Click **Upgrade**. If the file name is valid, a window as shown in [Figure 2-65](#) will display, to demonstrate the upload progress. Select or unselect the checkbox to decide whether or not to install after upload is finished.

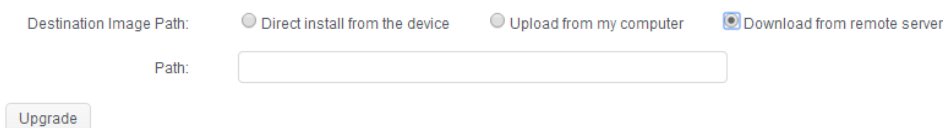
Figure 2-65 Uploading Image Progress

- Step 5** When the image upload is completed, if you do not choose to install automatically, a confirmation window will display. Click **Continue** to install the uploaded image.
- Step 6** If no error happens in the installation preparing stage, a window as shown in [Figure 2-62](#) will show up to demonstrate the installation progress; otherwise, related error message will be printed under the progress bar.
- Step 7** If the installation is successful, a window as shown in [Figure 2-63](#) is displayed. In the meantime, the device will reboot to finish the whole upgrade progress.

Upgrade by Downloading the Image File From a Remote Server

Follow these steps to perform image upgrade by downloading the image file from a remote server:

- Step 1** Click **Image Upgrade** under Administration in the left pane.
- Step 2** Choose **Download from remote server** in the Destination Image Path section, as shown in [Figure 2-66](#).

Figure 2-66 Image Upgrade by Downloading the Image From a Remote Server

- Step 3** Enter the address of an image file on remote server in the Path field. Make sure that the file is properly named in the form of *Cisco-Edge-xxx-i386-DVD.bin*.
- Step 4** Click **Upgrade**. If the file address is valid, a window as shown in [Figure 2-67](#) will display, to demonstrate the download progress. Select or unselect the checkbox to decide whether or not to install after download is finished.

Figure 2-67 Downloading Image Progress

- Step 5** When the image download is complete, if you do not choose to install automatically, a confirmation window will display. Click **Continue** to install the downloaded image.
- Step 6** If no error happens in the installation preparing stage, a window as shown in [Figure 2-62](#) will show up to demonstrate the installation progress; otherwise, related error message will be printed under the progress bar.
- Step 7** If the installation is successful, a window as shown in [Figure 2-63](#) is displayed. In the meantime, the device will reboot to finish the whole upgrade progress.

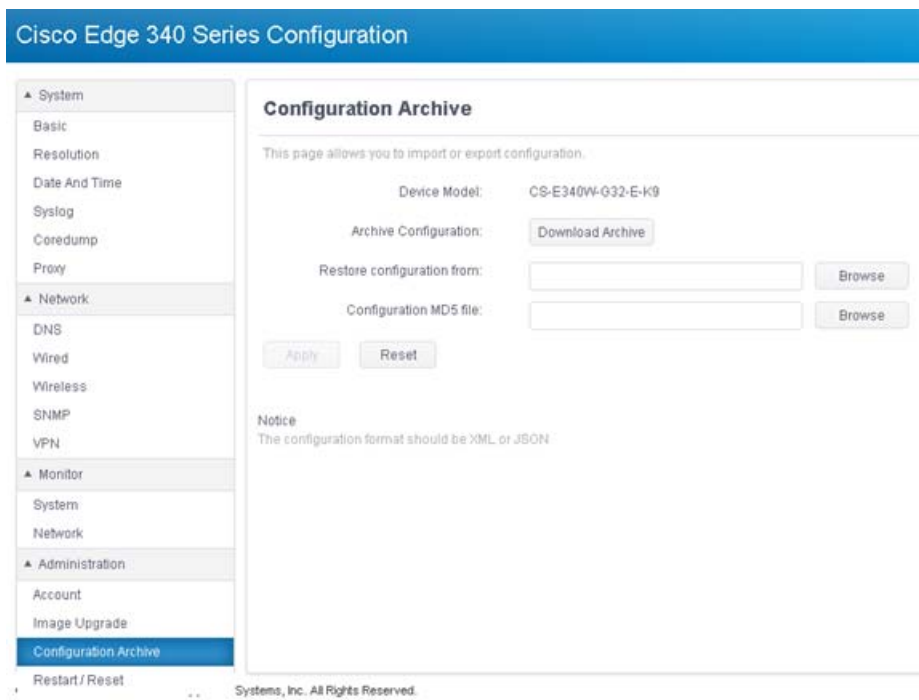
Configuration Archive

Using the Configuration Archive pane, you can download the configuration file to a local directory by clicking the **Download Archive** button, as shown in [Figure 2-69](#). Two files will be downloaded. One is the configuration file named `CE340_Cfg_XXXXXX.xml`, the other is MD5 checksum of the configuration file, named as `CE340_Cfg_XXXXXXXX.xml.md5`.

The browser may warn that multiple files are downloaded, click the **allow** button to allow this action, as shown in [Figure 2-68](#).

Figure 2-68 Popup Windows of Allowing Multiple Downloads

Figure 2-69 Configuration Archive Information



To copy the configuration file from one Cisco Edge 340 Series device to another Cisco Edge 340 Series device, follow these steps:

- Step 1** Click the **Download Archive** button to download the configuration file from the original Cisco Edge 340 Series device. Two files will be downloaded. One is XML file, the other is MD5 file.
- Step 2** Save the configuration file to another Cisco Edge 340 Series device by copying the configuration file locally or remotely.
- Step 3** Open the web GUI from the second Cisco Edge 340 Series device, and click **Configuration Archive** under Administration in the left pane.
- Step 4** Click the **Browse** button next to the Restore configuration from field to select the configuration file with suffix .XML that you have saved in [Step 2](#). The file name is displayed in the text field to the left of the Browse button.
- Step 5** Click **Browse** button next to the Configuration MD5 file field to select the MD5 checksum file with suffix .md5 that you have saved in [Step 2](#). The file name is displayed in the text field to the left of the Browse button.
- Step 6** Click **Apply**.
- Step 7** Reboot the Cisco Edge 340 Series device.

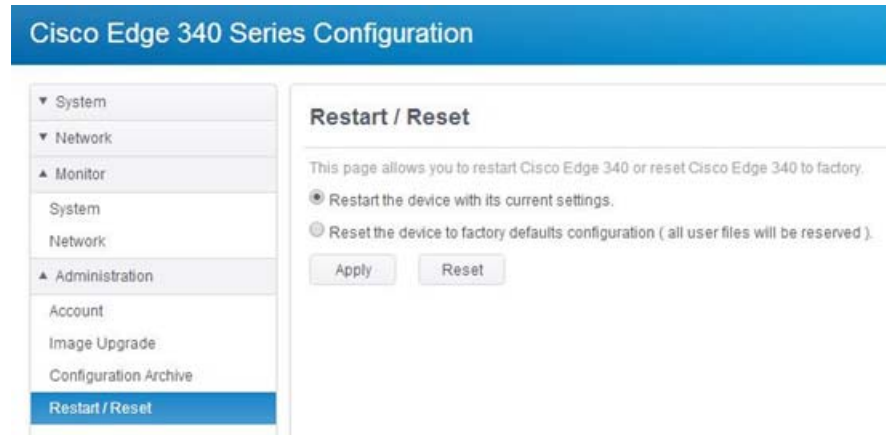
**Note**

Configurations can only be restored to the devices of the same model. For example, configurations from a non-wifi model cannot be applied to a wifi model.

Restart or Reset

Using the Restart/Reset pane, you can restart the Cisco Edge 340 Series device with its current settings, or reset the Cisco Edge 340 Series device to factory defaults, and then reboot.

Figure 2-70 Restart/Reset Information



Follow these steps to restart or reset the device:

-
- Step 1** Click **Restart/Reset** under Administration in the left pane. The Restart/Reset pane is displayed, as shown in [Figure 2-70](#).
 - Step 2** Choose the restart or reset option.
 - Step 3** Click **Apply** to apply the change or **Reset** to restore to the previous value.
-



Configuring Local CLI - CLISH

This chapter contains the following sections:

- [Configuration Guidelines](#)
- [Command Reference](#)

Configuration Guidelines

You can configure the Cisco Edge 340 Series in CLISH, which is used for the local CLI configuration. The CLI uses only those commands that are specific to the Cisco Edge 340 Series. Although the syntax is similar to the Cisco IOS CLI, these commands are *incompatible* with Cisco IOS commands.

You can use CLISH in two modes:

- User mode—When you log in to the Cisco Edge 340 Series as an ordinary user, you enter the user mode. To enter the privileged mode, enter the **enable** command and then enter the password of the root user.
- Global (privileged) mode—When you log in to the Cisco Edge 340 Series as root user, you enter the global mode directly and do not have to enter the **enable** command.

Use the CLI to configure these device settings:

- Basic device settings—Hostname, MAC address, bluetooth settings, password, Network Time Protocol (NTP) server, and device language
- Ethernet interface settings—Status, speed, and quality of service (QoS)
- Wireless interface settings—Status, radio, wireless mode, channel, wireless separation, transmission power, Wi-Fi Multimedia (WMM), and advanced wireless settings
- Service Set Identifier (SSID) security settings—Broadcast, authentication, and encryption

Follow these configuration guidelines when using CLISH:

- Enter **ssh username@ip-address** or **ssh root@ip-address** in the command prompt in your PC, and enter the password in the welcome screen. Enter the **mgcmd** command to start the CLISH process.
- If you log in as an ordinary user, enter the **enable** command and the password of the root user to switch to the global mode.
- Start a Cisco Edge configuration with the **configure terminal** global command. End the Cisco Edge configuration file with the **exit** global command.

**Note**

If you log in to the Cisco Edge 340 Series as ordinary user, and you want to enter CLISH as the root user, use the Linux command **su -**, where **-** means to switch ordinary user to root user, and use the environment variables of root. If more than 10 minutes passed by without any activity after you enter the privileged mode, you will exit the privileged mode automatically. Notice the prompt **>** and **#**; **>** means user mode, and **#** means privileged mode.

- From the system configuration mode, you can enter these configuration modes:
 - Ethernet configuration mode

Use the **interface** system configuration command to enter this mode. Use the **exit** global configuration command to return to the system configuration mode.
 - WiFi AP interface configuration mode

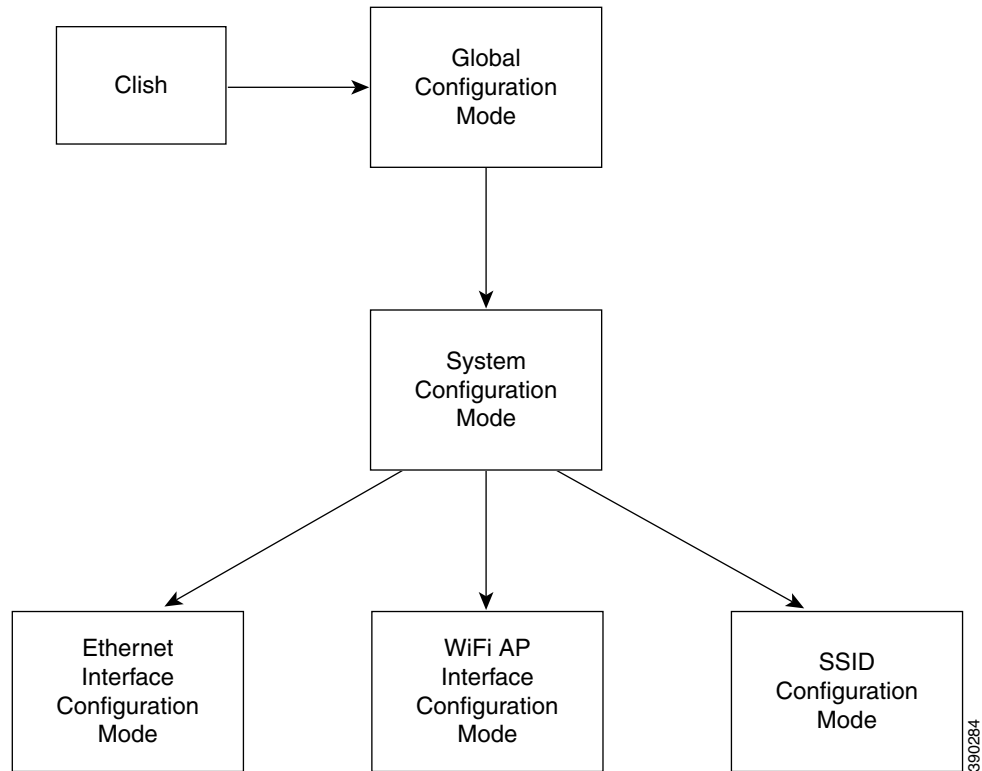
Use the **interface** system configuration command to enter this mode. We recommend that before you configure any wireless settings, you use the **wireless-mode** WiFi configuration command to set the 802.11 wireless mode. Use the **exit** global configuration command to return to the system configuration mode.
 - SSID configuration mode

Use the **ssid** system configuration command to enter this mode. Use the **exit** global configuration command to return to the system configuration mode.
- All commands must be entered in lowercase letters. Arguments can include uppercase letters.
- If there is a configuration conflict, the most recent configuration takes precedence. In this example, the SSID is not broadcast:

```
ssid NEWAP1
    broadcast ssid on
    broadcast ssid off
exit
```

Figure 3-1 shows the logic sequence of the CLISH functional structure.

Figure 3-1 Logic Sequence of the CLISH Functional Structure



Command Reference

This sections contains the commands of the following modes:

- [User Configuration Mode Commands](#)
- [Global Configuration Mode Commands](#)
- [System Configuration Mode Commands](#)
- [Ethernet Interface Configuration Mode Commands](#)
- [WiFi AP Interface Configuration Mode Commands](#)
- [SSID Configuration Mode](#)
- [show Commands](#)


Note

Syntax description, command default, command mode, usage guidelines, and examples are provided *only* for commands that are not self-explanatory.

User Configuration Mode Commands

This section contains user configuration mode commands. [Table 3-1](#) describes the functions these commands perform.

Table 3-1 **User Configuration Mode Commands**

Command	Function
enable	Enters the global configuration mode.
exit	Exits from the CLI.
help	Shows the descriptions of the interactive help system.
ping	Diagnoses basic network connectivity, and verifies if the remote device is reachable.
show	Shows running system information.
traceroute	Prints the route packets trace to the network host.

enable

To enter the global configuration mode, use the **enable** command in the user configuration mode.

enable

Command Modes User configuration

Usage Guidelines Use the **enable** command and enter the password of the **root** user to switch to the global configuration mode.

exit

To exit the configuration mode that you are in, use the **exit** command in any configuration mode.

exit

Command Modes

User configuration
Global configuration
System configuration
Ethernet interface configuration
WiFi AP interface configuration
SSID configuration

Usage Guidelines

Use **exit** to leave a configuration mode and return to the previous configuration mode.

help

To display a brief description of the help system, use the **help** command in the user configuration mode.

help

Command Modes

User configuration
Global configuration

Usage Guidelines

The **help** command displays a list of available commands, along with a brief description of each. To display additional details for a specific command, enter the command name followed by the **-?** option.

ping

To diagnose basic network connectivity on a Cisco Edge 340 Series device, use the **ping** command in the user configuration mode or the global configuration mode.

```
ping {[ip | ipv6 | arp] hostname | ip_address}
```

Syntax Description

ip	Sends Internet Control Message Protocol (ICMP) IPv4 messages to network hosts (default).
ipv6	Sends ICMP IPv6 messages to network hosts.
arp	Sends ARP requests to neighbor hosts.
<i>hostname</i>	Hostname to ping.
<i>ip_address</i>	IP address to ping.

Command Modes

User configuration
Global configuration

Usage Guidelines

The **ping** command sends an echo request packet to an address then waits for a reply. Ping output can help you evaluate path-to-host reliability, delays over the path, and whether the host can be reached or is functioning.

traceroute

To discover the routes that packets will pass through when traveling to their destination address, use the **traceroute** command in the user configuration mode or the global configuration mode.

```
traceroute [protocol] destination [ [resolve] source ip_address | interface interface_name]
```

Syntax Description

<i>protocol</i>	(Optional) Protocol; either IP or IPv6. When not specified, the protocol argument is based on an examination of the destination format by the software. The default protocol is IP.
<i>destination</i>	The destination address or hostname of the route that you want to trace.
resolve	Resolves the hostname.
source <i>ip_address</i>	Specifies the source IP address.
interface <i>interface_name</i>	Specifies the source interface.

Command Modes

User configuration
Global configuration

Usage Guidelines

The **traceroute** command works by taking advantage of the error messages generated by devices when a datagram exceeds its hop limit value.

The **traceroute** command first sends probe datagrams with a hop limit of 1. Including a hop limit of 1 with a probe datagram causes the neighboring devices to discard the probe datagram and send back an error message. The **traceroute** command sends several probes with increasing hop limits and displays the round-trip time for each.

The **traceroute** command sends out one probe at a time. Each outgoing packet might result in one or more error messages. A `time-exceeded` error message indicates that an intermediate device has seen and discarded the probe. A `destination unreachable` error message indicates that the destination node has received and discarded the probe because the hop limit of the packet has reached a value of 0. If the timer goes off before a response comes in, the **traceroute** command prints an asterisk (*).

The **traceroute** command is terminated when the destination responds, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, simultaneously press and release the **Ctrl**, **Shift**, and **6** keys, and then press the **X** key.

Global Configuration Mode Commands

This section contains global configuration mode commands. [Table 3-2](#) describes the functions these commands perform.

Table 3-2 Global Configuration Mode Commands

Command	Function
configure terminal	Starts the Cisco Edge configuration file, and enters the global configuration mode.
copy running-config startup-config	Saves the running configuration as the startup configuration file.
exit	Exits the global configuration mode.
export	Exports the running-config or startup-config to a destination path.
help	Shows the descriptions of the interactive help system.
import	Imports a configuration file to running-config or startup-config.
ping	Diagnoses the basic network connectivity, and verifies if the remote device is reachable.
reboot	Halts and performs a cold restart.
restore	Restores the default factory configuration.
show	Shows running system information.
tracert	Prints the route packets trace to the network host.

configure terminal

To enter the global configuration mode, use the **configure terminal** in the global configuration mode.

configure terminal

Command Modes Global configuration

copy running-config startup-config

To save the running configuration as the startup configuration file, use the **copy running-config startup-config** command in the global configuration mode.

copy running-config startup-config

Command Modes

Global configuration

export

To export a configuration file to the USB storage or a local directory, use the **export-config** command in the global configuration mode.

export startup-config to *destination*

Syntax Description

destination

Destination that you want to export the configuration file to. The destination can be either a USB or a local directory.

Command Modes

Global configuration

Usage Guidelines

You can export a configuration file to either a USB or a local directory. If you choose to export a configuration file to the USB, the configuration is automatically detected, mounted, and exported to the USB.

import

To import a configuration file from a USB or a local directory, use the **import-config** command in the global configuration mode.

import startup-config from *source*

Syntax Description

<i>source</i>	Location of the configuration file that you want to import. The source can be either a USB or a local directory.
---------------	--

Command Modes

Global configuration

Usage Guidelines

You can import a configuration file from either a USB or a local directory. If you choose to import a configuration file from a USB, the configuration is automatically detected, mounted, and imported from the USB.

reboot

To halt and perform a cold restart, use the **reboot** command in the global configuration mode.

reboot

Command Modes

Global configuration

restore

To restore default factory configuration, use the **restore** command in the global configuration mode.

restore factory-default

Command Modes

Global configuration mode

show

To display running system information, use the **show** command in the global configuration mode.

show

Command Modes

User configuration

Global configuration

System Configuration Mode Commands

This section contains system configuration mode commands. [Table 3-3](#) describes the functions these commands perform.

Table 3-3 System Configuration Mode Commands

Command	Function
auto-login	Enables or disables auto login to the system.
bluetooth	Enables or disables bluetooth on the device.
clock	Configures the time zone.
display	Configures the relation between HDMI and VGA when two monitors are connected.
do	Executes user EXEC or privileged EXEC commands from the global configuration mode or other configuration modes or submodes.
exit	Exits the system configuration mode.
hdmi	Configures HDMI resolution and rotation.
hostname	Configures the hostname of the device.
interface	Enters the Ethernet interface configuration mode to configure the Gigabit Ethernet interface, or enters the WiFi AP interface configuration mode to configure the wireless interface.
language support	Configures the language of the device.
log	Configures the log size.
monitor	Enables or disables HDMI or VGA.
ntp	Configures the NTP server that is used by the device.
proxy-server	Configures the proxy server.
ssh	Configures the SSH users.
ssid	Configures the SSID name and enters the SSID configuration mode to configure the security settings for the access point.
vga	Configures VGA resolution and rotation.
wifi-mode	Sets the WiFi mode.

auto-login

To configure the auto login of the system, use the **auto-login** command in the system configuration mode.

```
auto-login {enable | disable}
```

Syntax Description

enable	Enables auto login to the system.
disable	Disables auto login to the system.

Command Default

Auto login is disabled.

Command Modes

System configuration

bluetooth

To enable or disable bluetooth on the Cisco Edge 340 Series device, use the **bluetooth** command in the system configuration mode.

bluetooth {on | off}

Command Default Bluetooth is on.

Command Modes System configuration

clock

To set the time zone for display purposes, use the **clock** command in the system configuration mode.

clock *timezone* *timezone*

Syntax Description	<i>timezone</i>	Continent or ocean. Valid values are Africa , America , Antarctica , Arctic , Asia , Atlantic , Australia , Europe , Indian , Mideast , and Pacific .
---------------------------	-----------------	--

Command Modes	System configuration
----------------------	----------------------

display

To configure the relation between two monitors, use the **display** command in the system configuration mode.

```
display type {hdmi | vga} relation type {hdmi | vga}
```

Syntax Description	type	Selects monitor type, either HDMI or VGA .
	relation <i>type</i>	Configures relation between the two monitors. Valid values are same-as , right , left , below , and above .

Command Modes	System configuration
---------------	----------------------

do

To execute user configuration or global configuration commands in the global configuration mode or other configuration modes, use the **do** command in any configuration mode.

do *command*

Syntax Description	<i>command</i> User configuration or global configuration command to be executed.
Command Default	A user configuration or global configuration command is not executed from a configuration mode.
Command Modes	All configuration modes.
Usage Guidelines	Use this command to execute user configuration or global configuration commands (such as show , copy , and export) while configuring your routing device. After the command is executed, the system will return to the configuration mode that you were using.

hdmi

To configure high-definition multimedia (HDMI) resolution or rotation, use the **hdmi** command in the system configuration mode.

```
hdmi { resolution resolution_value | rotation rotation_value }
```

Syntax Description

<i>resolution_value</i>	Resolution that you want to set, in the form <i>xx@yy</i> .
<i>rotation_value</i>	Rotation that you want to set. Valid values are normal , right , inverted , and left .

Command Modes

System configuration

hostname

To configure the hostname of the Cisco Edge 340 Series device, use the **hostname** command in the system configuration mode.

hostname *name*

Syntax Description

name Name that you assign to the device.

Command Modes

System configuration

Usage Guidelines

Changing the hostname requires a reboot.

interface

To enter the Ethernet interface configuration mode to configure the Gigabit Ethernet interface, or to enter WiFi AP interface configuration mode to configure the wireless interface, use the **interface** command in the system configuration mode.

```
interface { ethernet ge | wireless bvi1 }
```

Syntax Description

ethernet ge	Configures the Gigabit Ethernet interface.
wireless bvi1	Configures the wireless interface.

Command Modes

System configuration

Usage Guidelines

Use the **interface** command to enter the Ethernet interface configuration mode or the WiFi AP interface configuration mode.

Related Commands

Use the **exit** command to leave the Ethernet interface configuration mode or the WiFi AP interface configuration mode.

[Table 3-4 on page 3-37](#) lists the Ethernet interface configuration mode commands.

[Table 3-5 on page 3-44](#) lists the WiFi AP interface configuration mode commands.

language support

To configure the device language, use the **language support** command in the system configuration mode.

```
language support language_value
```

Syntax Description	<i>language_value</i>	Language for the device. Valid values are zh_CH.utf8 , en_US.utf8 , ko_KR.utf8 , and ja_JP.utf8 .
---------------------------	-----------------------	---

Command Default	The default is English (en_US.utf8).
------------------------	--------------------------------------

Command Modes	System configuration
----------------------	----------------------

Usage Guidelines	Changing the language requires a reboot.
-------------------------	--

log

To set the log size, use the **log command** in the system configuration mode.

log size *value*

Syntax Description

size <i>value</i>	Sets the log size. Default unit is MB. The valid range is from 1 to 10000. Default is 10 MB.
--------------------------	--

Command Modes

System configuration

monitor

To enable or disable the monitor type of HDMI or VGA, use the **monitor** command in the system configuration mode.

```
monitor type {hdmi | vga} {on | off}
```

Syntax Description

type	Sets the monitor type.
hdmi	Sets the monitor type to HDMI.
vga	Sets the monitor type to VGA.
on	Enables the monitor.
off	Disables the monitor.

Command Modes

System configuration

no

no

To remove the configuration for a command or set the command to default, use the **no** command in the system configuration mode.

no

Command Modes

System configuration

ntp

To configure the Network Time Protocol (NTP) server that is used by the Cisco Edge 340 Series device, use the **ntp** command in the system configuration mode.

```
ntp {refresh {on | off} | server ip_address}
```

Syntax Description

refresh	Configures auto sync of the NTP server.
on	Enables auto sync of the NTP server.
off	Disables auto sync of the NTP server.
server ip_address	Configures the IP address of the NTP server

Command Modes

System configuration

proxy-server

To configure the proxy server, use the **proxy-server** command in the system configuration mode.

```
proxy-server server [type] [port port_number]
```

Syntax Description

<i>server</i>	Hostname or IP address of the proxy server.
<i>type</i>	(optional) Type of proxy server. Valid values are no_for , all , http , ftp , and https .
port <i>port_number</i>	(optional) Specifies the proxy port number. The range is from 0 to 65535.

Command Modes

System configuration

ssh

To configure a Secure Shell (SSH) user, use the **ssh** command in the system configuration mode.

```
ssh {add user | delete user}
```

Syntax Description

add <i>user</i>	Adds an SSH user.
delete <i>user</i>	Deletes an SSH user.

Command Modes

System configuration

ssid

To set the Service Set Identifier (SSID) name and enter the SSID configuration mode to configure the security settings for the access point of the device, use the **ssid** command in the system configuration mode.

```
ssid ssid
```

Syntax Description	<i>ssid</i>	SSID name for the access point. The name can include all the ASCII characters except '\ " ? = , and space.
---------------------------	-------------	--

Command Default	The default SSID name is CISCO_EDGE.
------------------------	--------------------------------------

Command Modes	System configuration
----------------------	----------------------

Related Commands	Use the exit command to leave the SSID configuration mode. Table 3-6 on page 3-75 lists the SSID configuration mode commands.
-------------------------	--

vga

To configure the Video Graphics Array (VGA) resolution or rotation, use the **vga** command in the system configuration mode.

```
vga {resolution resolution | rotation rotation}
```

Syntax Description

<i>resolution</i>	Resolution that you want to set, in the form <i>xx@yy</i> .
<i>rotation</i>	Rotation that you want to set. Valid values are normal , right , inverted , and left .

Command Modes

System configuration

wifi-mode

To set the WiFi mode of the Cisco Edge 340 Series device, use the **wifi-mode** command in the global configuration mode.

wifi-mode {WiFiAP | WiFiSta | NonWiFi}

Syntax Description	WiFiAP	WiFiSta	NonWiFi
	Sets the WiFi mode to access point (AP) after reboot.	Sets the WiFi mode to client after reboot.	Sets the WiFi mode to off.

Command Modes System configuration

Usage Guidelines If you choose the AP mode, the Cisco Edge 340 Series device will work in the AP mode immediately, and only the commands that are specific to the AP mode are visible. If you choose the client mode, the Cisco Edge 340 series device will work in the client mode immediately, and only the commands that are specific to the client mode are visible.

Ethernet Interface Configuration Mode Commands

This section contains Ethernet interface configuration mode commands. [Table 3-4](#) describes the functions these commands perform.

Table 3-4 Ethernet Interface Configuration Mode Commands

Command	Function
do	Executes user configuration or global configuration commands from the global configuration mode or other configuration modes.
duplex	Configures the duplex mode for the Gigabit Ethernet (GE) interface.
exit	Exits the Ethernet interface configuration mode.
ip address	Configures the IP address of an interface.
ip default-gateway	Configures the default gateway.
ipv6 address	Configures the IPv6 address of an interface.
ipv6 default-gateway	Configures the IPv6 default gateway.
speed	Configures the speed for the GE interface.

duplex

To configure the duplex mode for the Gigabit Ethernet (GE) interface, use the **duplex** command in the Ethernet interface configuration mode.

duplex {auto | half | full}

Syntax Description

auto	Configures automatic duplex mode sensing.
half	Configures half-duplex mode.
full	Configures full-duplex mode.

Defaults

The default is automatic duplex mode sensing.

ip address

To set the IP address for an interface, use the **ip address** command in the Ethernet interface configuration mode.

```
ip address {dhcp | ip_address}
```

Syntax Description	<i>dhcp</i>	IP address negotiated through the Dynamic Host Configuration Protocol (DHCP).
	<i>ip_address</i>	IP address of the interface.

Command Default The default is dhcp.

ipv6 address

To set the IPv6 address for an interface, use the **ipv6 address** command in the Ethernet interface configuration mode.

```
ipv6 address { dhcp | ipv6_address }
```

Syntax Description

<i>dhcp</i>	IPv6 address negotiated through DHCP.
<i>ipv6_address</i>	IPv6 address of the interface.

Command Default

The default is dhcp.

ip default-gateway

To specify the default gateway for the Cisco Edge 340 Series device, use the **ip default-gateway** command in the Ethernet interface configuration mode.

```
ip default-gateway ip_address
```

Syntax Description	<i>ip_address</i>	IP address of the default gateway.
--------------------	-------------------	------------------------------------

ipv6 default-gateway

To specify the IPv6 default gateway for the Cisco Edge 340 Series device, use the **ipv6 default-gateway** command in the Ethernet interface configuration mode.

```
ipv6 default-gateway ipv6_address
```

Syntax Description	<i>ip_address</i>	IPv6 address of the default gateway.
--------------------	-------------------	--------------------------------------

speed

To configure the speed for an interface, use the **speed** command in the Ethernet configuration mode.

```
speed {auto | 10 | 100 | 1000}
```

Syntax Description		
	auto	Configures automatic speed sensing.
	10	Configures 10 Mbps speed.
	100	Configures 100 Mbps speed.
	1000	Configures 1000 Mbps speed and full-duplex mode.

Command Default The default is auto.

WiFi AP Interface Configuration Mode Commands

This section contains WiFi AP interface configuration mode commands. [Table 3-5](#) describes the functions these commands perform.

Table 3-5 *WiFi AP Interface Configuration Mode Commands*

Command	Function
aggregation-msdu	Enables or disables aggregation MAC Service Data Unit (MSDU).
ap-isolation	Configures wireless separation for clients that are connected to the same SSID.
apsd	Configures Wi-Fi Multimedia (WMM) power save mode for an access point.
auto-block	Enables or disables auto block.
ba-decline	Enables or disables to decline a ba request.
beacon-interval	Configures the beacon interval for an access point.
bg-protection	Configures the CTS-to-self protection for an access point.
channel bandwidth	Configures the channel width when the access point functions in the 802.11n mode or the 802.11n mixed mode.
channel number	Configures the channel number (which sets the frequency) for an access point.
data-beacon-rate	Configures the Delivery Traffic Indication Message (DTIM) interval for an access point.
do	Executes user configuration or global configuration commands from the global configuration mode or other configuration modes.
exit	Exits the WiFi AP interface configuration mode.
extension channel	Configures the control-side band that is used for the extension or secondary channel when the access point functions in the 802.11n mode or the 802.11n mixed mode.
frag-threshold	Configures the frag threshold.
guard-interval	Configures the period between packets when an access point functions in the 802.11n mode or the 802.11n mixed mode.
igmp-snoop	Enables or disables Internet Group Management Protocol (IGMP) snooping.
mcs	Configures the high throughput Modulation and Coding Schemes (MCS) rate when the access point functions in 802.11n mode or 802.11n mixed mode.
multicast-mcs	Configures the high throughput MCS rate on multicast frames.
multicast-phy-mode	Configures PHY mode on multicast frames.
operating-mode	Configures greenfield or mixed mode when the access point functions in the 802.11n mode.
packet aggregation	Configures Aggregate MAC Service Data Unit (A-MSDU) packet aggregation when an access point functions in the 802.11n mode or the 802.11n mixed mode.

Table 3-5 *WiFi AP Interface Configuration Mode Commands (continued)*

Command	Function
rdg	Configures the Reverse Direction Grant (RDG) when an access point functions in the 802.11n mode or the 802.11n mixed mode.
rts-threshold	Sets the RTS threshold.
short-slot	Configures the short-slot time when the access point functions in the 802.11g mode or the 802.11g mixed mode.
stbc	Configures the space time block coding (STBC).
transmit burst	Configures the transmit burst (Tx burst) for an access point.
transmit preamble	Configures the preamble for an access point.
transmit power	Configures the power at which an access point radio transmits its wireless signal.
wireless-mode	Configures the 802.11 wireless mode for an access point.
wmm	Configures Wi-Fi Multimedia (WMM) for an access point.

aggregation-msdu

To enable or disable MAC Service Data Unit (MSDU) aggregation, use the **aggregation-msdu** command in the WiFi AP interface configuration mode.

aggregation-msdu {on | off}

Syntax Description

on	Enables aggregation MSDU.
off	Disables aggregation MSDU.

Command Modes

WiFi AP interface configuration

ap-isolation

To configure wireless separation for clients that are connected to the same Service Set Identifier (SSID), use the **ap-isolation** command in the WiFi AP interface configuration mode.

ap-isolation { on | off }

Syntax Description	on	off
	Enables wireless separation. Wireless clients that are connected to the same SSID are prevented from communicating with each other.	Disables wireless separation. Wireless clients that are connected to the same SSID can communicate with each other.

Command Default Wireless separation is disabled.

Related Commands WiFi AP interface configuration

apsd

To configure Wi-Fi Multimedia (WMM) power save mode for an access point, use the **apsd** command in the WiFi AP interface configuration mode.

apsd { **on** | **off** }

Syntax Description

on	Enables WMM power save mode.
off	Disables WMM power save mode.

Command Default

WMM power save mode is disabled.

Command Modes

WiFi AP interface configuration

Usage Guidelines

You can configure the **apsd** command only when the WMM is enabled.

Related Commands

Use the [wmm](#) command to enable WMM.

auto-block

To configure auto block, use the **auto-block** command in the WiFi AP interface configuration mode.

auto-block {on | off}

Syntax Description	on	Enables auto block.
	off	Disables auto block.

Related Commands WiFi AP interface configuration

ba-decline

To enable or disable the task of declining a BA request, use the **ba-decline** command in the WiFi AP interface configuration mode.

ba-decline {on | off}

Syntax Description

on	Enables the task of declining a BA request.
off	Disables the task of declining a BA request.

Command Modes

WiFi AP interface configuration

beacon-interval

To configure the beacon interval for an access point, use the **beacon-interval** command in the WiFi AP interface configuration mode.

beacon-interval *interval*

Syntax Description	<i>interval</i>	Period that you want to configure the beacon interval with. The range is between 20 and 1000 milliseconds. The default is 100 milliseconds.
---------------------------	-----------------	---

Command Default The default period is 100 milliseconds.

Command Modes WiFi AP interface configuration

Usage Guidelines The default setting should work well for most networks.

Configure a long interval to:

- Increase an access point's throughput performance.
- Decrease the discovery time for clients and decrease the roaming efficiency.
- Decrease the power consumption of clients.

Configure a short interval to:

- Minimize the discovery time for clients and improve the roaming efficiency
- Decrease an access point's throughput performance.
- Increase the power consumption of clients.

bg-protection

To configure CTS-to-self protection for an access point, use the **bg-protection** command in the WiFi AP interface configuration mode.

bg-protection { **auto** | **on** | **off** }



Note

This command applies to the 802.11b/g mixed mode, 802.11n/g mixed mode, and 802.11b/g/n mixed mode.

Syntax Description

auto	Configures automatic selection of CTS-to-self protection.
on	Enables CTS-to-self protection.
off	Disables CTS-to-self protection.

Command Default

The default is automatic selection of CTS-to-self protection.

Command Modes

WiFi AP interface configuration

Usage Guidelines

CTS-to-self protection minimizes collisions among clients in a mixed mode environment, but reduces throughput performance.

channel bandwidth

To configure the channel width in a scenario there an access point functions in the 802.11n mode, use the **channel bandwidth** command in the WiFi AP interface configuration mode.

```
channel bandwidth { 20 | 20/40 }
```



Note

This command applies to the 802.11n mode or the 802.11n mixed mode.

Syntax Description

20	Configures a 20-MHz channel width.
20/40	Configures automatic selection of a 20-MHz or a 40-MHz channel width.

Command Default

The default is automatic selection of a 20-MHz or a 40-MHz channel width.

Command Modes

WiFi AP interface configuration

Usage Guidelines

The default setting should work well for most networks.

A 40-MHz channel provides a higher throughput performance for 802.11n clients.

802.11b and 802.11g clients can function only with a 20-MHz channel.

Related Commands

The setting of the **channel bandwidth** command affects the options for the **mcs** command.

channel number

To configure a channel number, which sets the frequency for an access point, use the **channel number** command in the WiFi AP interface configuration mode.

channel number { *auto* | *number* }

Syntax Description	auto	Configures automatic selection of a channel number.
	<i>number</i>	Channel number. The default is auto.

Command Default The default value is auto.

Command Modes WiFi AP interface configuration

Usage Guidelines We recommend that you either use the default channel number or the automatic selection of the channel number and only change the channel number if you experience interference in the network.

data-beacon-rate

To configure the Delivery Traffic Indication Message (DTIM) interval for an access point, use the **data-beacon-rate** command in the WiFi AP interface configuration.

data-beacon-rate *rate*

Syntax Description	<i>rate</i> The range is between 1 and 255 milliseconds. The default is 1 millisecond.
Command Default	The default rate is 1 millisecond.
Command Modes	WiFi AP interface configuration
Usage Guidelines	<p>The DTIM interval is a multiple of the beacon interval. Before you change the DTIM interval, consider the types of clients in the network: laptops might function better with a short interval, but mobile phones might function better with a long interval.</p> <p>A long interval allows clients to save power, but may delay multicast and broadcast traffic.</p> <p>A short interval decreases the delivery time of multicast and broadcast traffic, but may increase power consumption by clients.</p>
Related Commands	The setting of the beacon-interval command affects the data-beacon-rate command.

extension channel

To configure the control sideband that is used for the extension or secondary channel when an access point functions in the 802.11n mode, use the **extension channel** command in the WiFi AP interface configuration mode.

extension channel {upper | lower}



Note

This command applies to the 802.11n mode or the 802.11n mixed mode.

Syntax Description

upper	Configures the upper extension channel.
lower	Configures the lower extension channel.

Command Default

The lower extension channel is configured.

Command Modes

WiFi AP interface configuration

Usage Guidelines

This command takes effect only when you configure a 40-MHz channel width.

When the main channel number is in the lower range (for example, in the 1 to 4 range), use the upper extension channel.

When the main channel number is in the upper range (for example, in the 10 to 13 range), use the lower extension channel.

When the main channel number is in the middle range (for example, in the 5 to 9 range), use either the upper extension channel or the lower extension channel.

Related Commands

Use the [channel bandwidth](#) command to configure the channel width.

Use the [channel number](#) command to configure the main channel number.

frag-threshold

To configure the Frag threshold, use the **frag-threshold** command in the WiFi AP interface configuration mode.

frag-threshold *value*

Syntax Description

value Configures the Frag threshold value. The range is from 256 to 2346.

Command Modes

WiFi AP interface configuration

guard-interval

To configure the guard interval period between packets when the access point functions in the 802.11n mode, use the **guard-interval** command in the WiFi AP interface configuration mode.

```
guard-interval {400 | 800}
```



Note

This command applies to the 802.11n mode or the 802.11n mixed mode.

Syntax Description

400	Configures a short guard interval of 400 nanoseconds (ns).
800	Configures a long guard interval of 800 ns.

Command Default

The default is 400 ns.

Command Modes

WiFi AP interface configuration

Usage Guidelines

Use a 400-ns interval to increase the throughput performance for 802.11n clients, but may result in some packet errors and multipath interference.

Use an 800-ns interval to minimize packet errors and multipath interference, but decrease the throughput performance for 802.11n clients.

Related Commands

The setting of the **guard-interval** command affects the options for the **mcs** command.

igmp-snoop

To enable or disable Internet Group Management Protocol (IGMP) snooping on a wireless interface, use the **igmp-snoop** command in the WiFi AP interface configuration mode.

igmp-snoop { on | off }

Syntax Description	on	IGMP snooping is on.
	off	IGMP snooping is off.

Command Default IGMP snooping is off.

Command Modes WiFi AP interface configuration

mcs

To configure the high throughput Modulation and Coding Scheme (MCS) rate when an access point functions in the 802.11n mode, use the **mcs** command in the WiFi AP interface configuration mode.

mcs *index_number*



Note

This command applies to the 802.11n mode or the 802.11n mixed mode.

Syntax Description

index_number The range is from 0 to 15, and 33 (automatic selection).

Command Default

The default is 33 (automatic rate configuration).

Command Modes

WiFi AP interface configuration

Usage Guidelines

This table shows the MCS index numbers with their potential data rates in Mbps based on MCS, guard interval, and channel width.

Index Number	Guard Interval of 800 nanoseconds		Guard Interval of 400 nanoseconds	
	20-MHz Channel Width	40-MHz Channel Width	20-MHz Channel Width	40-MHz Channel Width
0	6.5	13.5	7 2/9	15
1	13	27	14 4/9	30
2	19.5	40.5	21 2/3	45
3	26	54	28 8/9	60
4	39	81	43 1/3	90
5	52	109	57 5/9	120
6	58.5	121.5	65	135
11	52	108	57 7/9	120
12	78	162	86 2/3	180
13	104	216	115 5/9	240
14	117	243	130	270
15	130	270	144 4/9	300
33	Configures automatic selection of the MCS index number.			

We recommend that you use automatic selection of the MCS index number. Change the MCS index to a fixed number only if the Received Signal Strength Indication (RSSI) for the clients in the network can support the selected MCS index number.

Related Commands

The setting of the **channel bandwidth** command affects the options for the **mcs** command.

The setting of the **guard-interval** command affects the options for the **mcs** command.

multicast-mcs

To configure the high throughput Modulation and Coding Scheme (MCS) rate on multicast frames when an access point functions in the 802.11n mode, use the **multicast-mcs** command in the WiFi AP interface configuration mode.

multicast-mcs *index_number*



Note

This command applies to the 802.11n mode or the 802.11n mixed mode.

Syntax Description

index_number The range is from 0 to 15.

Command Default

The default is 2.

Usage Guidelines

This table shows the MCS index numbers with their potential data rates in Mbps based on MCS, guard interval, and channel width.

Index Number	Guard Interval of 800 ns		Guard Interval of 400 ns	
	20-MHz Channel Width	40-MHz Channel Width	20-MHz Channel Width	40-MHz Channel Width
0	6.5	13.5	7 2/9	15
1	13	27	14 4/9	30
2	19.5	40.5	21 2/3	45
3	26	54	28 8/9	60
4	39	81	43 1/3	90
5	52	109	57 5/9	120
6	58.5	121.5	65	135
7	65	135	72 2/9	152.5
8	13	27	14 4/9	30
9	26	54	28 8/9	60
10	39	81	43 1/3	90
11	52	108	57 7/9	120
12	78	162	86 2/3	180
13	104	216	115 5/9	240
14	117	243	130	270
15	130	270	144 4/9	300

multicast-phy-mode

To configure the PHY mode on multicast frames when an access point functions in the 802.11n mode, use the **multicast-phy-mode** command in the WiFi AP interface configuration mode.

multicast-phy-mode {0 | 1 | 2 | 3}

Syntax Description		
	0	Specifies that the mode is disabled.
	1	Specifies Complementary Code Keying (CCK) (802.11b).
	2	Specifies Orthogonal Frequency Division Multiplexing (OFDM) (802.11g). This is the default.
	3	Specifies HTMIX (802.11b/g/n).

Command Default The default is 2.

Command Modes WiFi AP interface configuration

operating-mode

To configure greenfield mode or the mixed mode when an access point functions in the 802.11n mode, use the **operating-mode** command in the WiFi AP interface configuration mode.

operating-mode {greenfield | mixed}



Note

This command applies to the 802.11n mode.

Syntax Description

greenfield	Configures the greenfield mode, which improves 802.11n throughput performance, but prevents 802.11b and 802.11g clients present in the coverage area from recognizing the 802.11n traffic.
mixed	Configures the mixed mode, which allows the 802.11b and 802.11g clients in the coverage area to recognize the 802.11n traffic. This is the default.

Command Default

The default is **mixed**.

Command Modes

WiFi AP interface configuration

Usage Guidelines

Use the greenfield mode if there are only 802.11n clients in the coverage area. If you use the greenfield mode when 802.11b, 802.11g, and 802.11n clients coexist in the same coverage area, packet collisions might occur.

Use the mixed mode when 802.11b, 802.11g, and 802.11n clients coexist in the same coverage area.

packet aggregation

To configure Aggregate MAC Service Data Unit (A-MSDU) packet aggregation when an access point functions in the 802.11n mode, use the **packet aggregation** command in the WiFi AP interface configuration mode.

packet aggregation { on | off }



Note

This command applies to the 802.11n mode or the 802.11n mixed mode.

Syntax Description

on	Enables packet aggregation.
off	Disables packet aggregation.

Command Default

Packet aggregation is off.

Command Modes

WiFi AP interface configuration

Usage Guidelines

Enable packet aggregation if network traffic consists primarily of data.

Disable packet aggregation if network traffic consists primarily of voice, video, or other multimedia traffic.

rdg

To configure the Reverse Direction Grant (RDG) when an access point functions in the 802.11n mode, use the **rdg** command in the WiFi AP interface configuration mode.

rdg {on | off}



Note

This command applies to the 802.11n mode or the 802.11n mixed mode.

Syntax Description

on	Enables RDG.
off	Disables RDG.

Command Default

RDG is disabled.

Command Modes

WiFi AP interface configuration

Usage Guidelines

When RDG is enabled, a transmitter that has reserved the channel transmission opportunity allows the receiver to send packets in the reserved direction. When RDG is disabled, packets can be transmitted only in one direction during the channel transmission opportunity reservation.

Enable RDG for better throughput performance of 802.11n traffic.

rts-threshold

To configure the Request to Send (RTS) threshold, use the **rts-threshold** command in the WiFi AP interface configuration mode.

rts-threshold *value*

Syntax Description

value Sets the RTS threshold. The range is from 1 to 2347.

Command Modes

WiFi AP interface configuration

short-slot

To configure the short-slot time when the access point functions in the 802.11g mode or the 802.11g mixed mode, use the **short-slot** command in the WiFi AP interface configuration mode.

short-slot { **on** | **off** }



Note

This command applies to the 802.11g mode or the 802.11g mixed mode.

Syntax Description

on	Enables short-slot time.
off	Disables short-slot time.

Command Default

Short-slot time is enabled.

Command Modes

WiFi AP interface configuration

Usage Guidelines

Enable the short-slot time for better throughput performance for 802.11g clients.
If there are mostly 802.11b clients in the network, disable the short-slot time.

stbc

To configure the space time block coding (STBC), use the **stbc** command in the WiFi AP interface configuration mode.

```
stbc {on | off}
```

Syntax Description

on	Enables STBC.
off	Disables STBC.

Related Commands

WiFi AP interface configuration

transmit burst

To configure the transmit burst (Tx burst) for an access point, use the **transmit burst** command in the WiFi AP interface configuration mode.

transmit burst {on | off}

Syntax Description	on	Enables Tx burst.
	off	Disables Tx burst.

Command Default Tx burst is enabled.

Command Modes WiFi AP interface configuration

Usage Guidelines Leave Tx burst on for better throughput performance.
Disable Tx burst if you notice wireless interference in the network.

transmit preamble

To configure the preamble for an access point, use the **transmit preamble** command in the WiFi AP interface configuration mode.

transmit preamble {long | short | auto}

Syntax Description

long	Configures a long preamble.
short	Configures a short preamble.
auto	Configures automatic preamble selection.

Command Default

The default is a long preamble.

Command Modes

WiFi AP interface configuration

Usage Guidelines

Use the long preamble setting for compatibility with legacy 802.11 systems operating at 1 and 2 Mb/s. Configure a short preamble setting to improve throughput performance.

transmit power

To configure the power at which an access point radio transmits its wireless signal, use the **transmit power** command in the WiFi AP interface configuration mode.

transmit power *percentage*

Syntax Description	<i>percentage</i> Percentage of transmit power. The range is from 1 to 100.
Command Default	The default is 100 percent.
Command Modes	WiFi AP interface configuration
Usage Guidelines	<p>For transmission of the wireless signal over a long distance, use the 100 percent setting.</p> <p>For transmission of the wireless signal over a short distance, for example, when all the clients are in a small room, lower the percentage.</p>

wireless-mode

To configure the 802.11 wireless mode for an access point, use the **wireless-mode** command in the WiFi AP interface configuration mode.

wireless-mode {0 | 1 | 2 | 4 | 6 | 7 | 8 | 9 | 11}

Syntax Description	0	Configures the 802.11b/g mixed mode.
	1	Configures the 802.11b mode.
	2	Configures the 802.11a mode for 5GHz only.
	4	Configures the 802.11g mode.
	6	Configures the 802.11n mode for 2GHz only.
	7	Configures the 802.11n/g mixed mode.
	8	Configures the 802.11a/n mixed mode for 5GHz only.
	9	Configures the 802.11b/g/n mixed mode.
	11	Configures the 802.11n mode for 5GHz only.

Command Default The default is the 802.11b/g/n mixed mode.

Command Modes WiFi AP interface configuration

Usage Guidelines

802.11b/g mixed mode—Select this mode if you have devices in the network that support 802.11b and 802.11g.

802.11b mode—Select this mode if all the devices in the wireless network only support 802.11b.

802.11a mode for 5GHz only—Select this mode if all the devices in the wireless network only support 802.11a in the 5GHz band.

802.11g mode—Select this mode if all the devices in the wireless network only support 802.11g.

802.11n mode for 2GHz only—Select this mode if all the devices in the wireless network only support 802.11n in the 2GHz band.

802.11b/g/n mixed mode—Select this mode if you have devices in the network that support 802.11b, 802.11g, and 802.11n.

802.11b/g mixed mode—Select this mode if you have devices in the network that support 802.11b and 802.11g.

wmm

To configure Wi-Fi Multimedia (WMM) for an access point, use the **wmm** command in the WiFi AP interface configuration mode.

```
wmm { on | off }
```

Syntax Description	on	Enables WMM.
	off	Disables WMM.

Command Default WMM is disabled.

Command Modes WiFi AP interface configuration

Usage Guidelines WMM provides QoS for wireless traffic. If there is a lot of mixed media traffic (voice, video, data), enable WMM.

Related Commands Use the [apsd](#) command to configure WMM power save mode.

SSID Configuration Mode

This section contains Service Set Identifier (SSID) configuration mode commands. [Table 3-6](#) describes the functions these commands perform.

Table 3-6 SSID Configuration Commands

Command	Function
broadcast ssid	Enables or disables broadcast of the Service Set Identifier (SSID) name.
do	Executes THE user EXEC or privileged EXEC commands from global configuration mode or other configuration modes or submodes.
encryption mode (open, shared, or WEP configuration)	Configures open, shared, Wi-Fi Protected Access (WPA), WPA1WPA2, WPA2, WPA2PSK, WPAPSK, and WPAPSKWPA2PSK authentication and associated encryption for the access point.
encryption mode (WPA configuration)	
exit	Exits the SSID configuration mode.
no	Removes the configuration for a command or sets the command to default.
radius-server	Configures the name of a RADIUS server.



Note

Configuration for SSID will take effect after exiting the SSID configuring mode.

broadcast ssid

To enable or disable broadcast of the SSID name, use the **broadcast ssid** command in the SSID configuration mode.

broadcast ssid {on | off}

Syntax Description

on	Enables broadcast of the SSID name.
off	Disables broadcast of the SSID name.

Command Default

The SSID is broadcast.

Command Modes

SSID configuration

Usage Guidelines

Disable broadcast of the SSID for enhanced security. Only wireless clients who know the SSID can connect to the access point.

Enable broadcast of the SSID for wider availability and easier access.

encryption mode (open, shared, or WEP configuration)

To configure open, shared, or Wired Equivalency Privacy (WEP) authentication and associated encryption for an access point, use the **encryption mode** command in the SSID configuration mode.

```
encryption mode {open | shared} type {none | wep {key {1 | 2 | 3 | 4} {hex number | ascii phrase}}}
```

Syntax Description	
open	Configures open access without authentication.
shared	Configures authentication with a shared key.
none	Configures no encryption.
wep	Configures WEP encryption.
key 1	Configures the key number for WEP encryption. (You can use only one of the four keys.)
key 2	
key 3	
key 4	
hex number	Configures either authentication with a hexadecimal key or authentication and encryption with a hexadecimal key: <ul style="list-style-type: none"> When you select the none keyword, configures authentication with a hexadecimal key. When you select the wep keyword, configures authentication and encryption with a hexadecimal key. For <i>number</i> , enter either 10 or 26 hexadecimal digits.
ascii phrase	Configures either authentication with a passphrase or authentication and encryption with a passphrase: <ul style="list-style-type: none"> When you select the none keyword, configures authentication with a passphrase. When you select the wep keyword, configures authentication and encryption with a passphrase. For <i>phrase</i> , enter either 5 or 13 alphanumerical characters. Dash (-) and underscore (_) characters are supported.

Command Default The default is open access and no encryption.

Command Modes SSID configuration

Usage Guidelines For shared access without encryption, the WEP hexadecimal number or passphrase is used only for authentication.

For shared access with WEP encryption, the WEP hexadecimal number or passphrase is used for both authentication and encryption.

Examples

This example shows how to configure shared authentication and WEP encryption, using key 3 and the passphrase 3uifsfis-_0r5:

```
encryption mode shared type wep key 3 ascii 3uifsfis-_0r5
```

encryption mode (WPA configuration)

To configure Wi-Fi Protected Access (WPA) authentication and associated encryption for an access point, use the **encryption mode** command in the SSID configuration mode.

```
encryption mode { wpa2psk | wpa2psk | wpa2pskwpa2psk } type { tkip | aes | tkipaes }
pass-phrase phrase
```

Syntax Description	
wpa2psk	Configures WPA with preshared key (PSK) authentication.
wpa2psk	Configures WPA2 with PSK authentication.
wpa2pskwpa2psk	Configures combined WPA and WPA2 with PSK authentication.
tkip	Configures Temporal Key Integrity Protocol (TKIP) encryption.
aes	Configures Advanced Encryption Standard (AES) encryption.
tkipaes	Configures combined TKIP and AES encryption.
pass-phrase <i>phrase</i>	Configures a passphrase (password). For <i>phrase</i> , enter at least 8 and a maximum of 63 alphanumerical characters. Dash (-) and underscore(_) characters are supported.

Command Default The default is open access and no encryption.

Command Modes SSID configuration

Examples This example shows how to configure combined WPA and WPA2 authentication with combined TKIP and AES encryption, using the passphrase safE478_Ty33Yep-:

```
encryption mode wpa2pskwpa2psk type tkipaes pass-phrase safE478_Ty33Yep-
```

encryption mode (802.1x)

To configure Wi-Fi Protected Access (WPA) authentication and associated encryption for an access point, use the **encryption mode** command in the SSID configuration mode.

```
encryption mode {wpa | wpa2 | wpa1wpa2} type {tkip | aes | tkipaes}
```



Note

The encryption mode (802.1x) should be used in combination with RADIUS server.

Syntax Description

wpa	Configures WPA with 802.1x authentication.
wpa2	Configures WPA2 with 802.1x authentication.
wpa1wpa2	Configures combined WPA and WPA2 with 802.1x authentication.
tkip	Configures Temporal Key Integrity Protocol (TKIP) encryption.
aes	Configures Advanced Encryption Standard (AES) encryption.
tkipaes	Configures combined TKIP and AES encryption.

Command Default

The default mode is wpa2psk access, tkipaes encryption, and the password is Cisco123.

Command Modes

SSID configuration

Examples

This example shows how to configure combined WPA and WPA2 authentication with combined TKIP and AES encryption, using the 802.1x authentication method:

```
encryption mode wpa1wpa2 type tkipaes
```


radius-server

To configure the related information of a RADIUS server, use the **radius-server** in the SSID configuration mode.

```
radius-server hostname [auth-port port_number] [key secret]
```

Syntax Description		
	<i>hostname</i>	Hostname or IP address of the RADIUS server.
	auth-port	Specifies the authentication port number of the RADIUS server.
	<i>port_number</i>	Authentication port number of the RADIUS server. The range is from 0 to 65535. The default is 1812.
	key	Specifies the password of the authentication service on the RADIUS server.
	<i>secret</i>	Password of the authentication service on the RADIUS server.

Command Default

The default value for *port_number* is 1812.
The default value for *secret* is NULL.

Command Modes

SSID configuration

Examples

This example shows how to configure the related information of a RADIUS server:

```
radius-server 192.168.1.1 auth-port 1812 key pass1234
```

show Commands

User Configuration Mode

Use the following **show** commands in the user configuration mode to display the configuration on a Cisco Edge 340 Series device:

- **show cpu**—Displays CPU information.
- **show mac**—Displays MAC address.
- **show memory**—Displays memory usage information.
- **show mount**—Displays mount information.
- **show os-build-time**—Displays release build time.
- **show os-version**—Displays release version.
- **show os-install-time**—Displays release installed time.
- **show storage**—Displays storage information.

Global Configuration Mode

Use the following **show** commands in the global configuration mode to display the configuration on a Cisco Edge 340 Series device:

- **show all-running-config**—Displays all information about the running configuration.
- **show all-startup-config**—Displays all information about the startup configuration.
- **show running-config**—Displays the configuration saved in the RAM.
- **show startup-config**—Displays the configuration saved in the database.
- **show bluetooth**—Displays bluetooth information.
- **show hdmi dev-name**—Displays the device name of the connected HDMI monitor.
- **show hdmi current-resolution**—Displays the current resolution of the connected HDMI monitor.
- **show hdmi support-resolution**—Displays the connected HDMI monitor support resolution.
- **show hostname**—Displays the hostname.
- **show ip interface**—Displays the status of interfaces configured for IP.
- **show log-size**—Displays the log size.
- **show monitor-full**—Displays all the current monitor information.
- **show ssid**—Displays the AP wireless ssid setting.
- **show wifi-mode**—Displays the WiFi mode.
- **show vga dev-name**—Displays the device name of the connected VGA monitor.
- **show vga current-resolution**—Displays the current resolution of the connected VGA monitor.
- **show vga support-resolution**—Displays the connected VGA monitor support resolution.



Troubleshooting

This appendix provides information about troubleshooting the Cisco Edge 340 Series device with the following issues:

- [Boot and Login, page A-1](#)
- [Reset and Upgrade, page A-2](#)
- [Display Issues, page A-4](#)
- [Network Issues, page A-4](#)
- [Power Issues, page A-5](#)



Note

The end users are not encouraged to perform troubleshooting by themselves.

Boot and Login

This section provides troubleshooting information about boot and login issues.

Forget Root Password

If you forget the root password of a Cisco Edge 340 Series device, follow these steps to reset the password to the factory default:

-
- Step 1** Plug in a USB external storage device to an Linux PC or VM, for example, a Kingston USB disk with the partition of /dev/sdd1.
- Step 2** Execute the following commands to create a USB recovery disk and wait until the process is complete:
- ```
[user@CE340 root]$ su
[user@CE340 ~]# cd /home/user/Downloads/
[user@CE340 Downloads]# chmod 777 Cisco-Edge-1.1-i386-DVD.bin
[user@CE340 Downloads]# ./Cisco-Edge-1.1-i386-DVD.bin -t/dev/sdd1 -w
```
- Step 3** Plug in the USB recovery disk to your device. Press **F12** when you start the Cisco Edge 340 Series device to enter the privileged mode as shown in [Figure A-1](#). Choose your USB device as the boot device, which in this example is KingstonDataTraveler 2.0.1.00.

**Figure A-1** *Select Boot Device*

```

Please select boot device:

SATA PM: SanDisk SSD U100 32G
Generic STORAGE DEVICE 0208
 SYSRecovery
Atheros Boot Agent
UEFI: Built-in EFI Shell
KingstonDataTraveler 2.01.00
Enter Setup

↑ and ↓ to move selection
ENTER to select boot device
ESC to boot using defaults

```

391407

**Note**


---

This operation will wipe all the user data from the device.

---

## System Starts Slowly

If the system takes more than one or two minutes to start, follow these steps:

- 
- Step 1** Plug in the console cable of the Cisco Edge 340 Series device.
  - Step 2** Check the log printed on the terminal to verify if the problem is caused by the insufficient power support from external devices.
  - Step 3** If yes, disconnect the external devices and restart the system. Alternatively, power off the Cisco Edge 340 Series device and restart it.
  - Step 4** If the problem is not caused by external devices, record the system log and contact a Cisco support representative.
- 

## System Locked After Using Wrong Password Five Times

If type the wrong password more than five times when you log in, the system is locked for 15 seconds. After 15 seconds have lapsed, the system is unlocked and you can retype the password.

## Reset and Upgrade

This section provides troubleshooting information about reset and upgrade issues.

## Having Trouble Updating the System

If you have trouble updating the system of a Cisco Edge 340 Series device, perform one of the following actions:

### Able To Log In

If you can log in to the system, use the following command to execute *Cisco-Edge-1.1-i386-DVD.bin* file to update the system automatically:

```
[user@CE340 root]$ su
[user@CE340 ~]# cd /home/user/Downloads/
[user@CE340 Downloads]# chmod 777 Cisco-Edge-1.1-i386-DVD.bin
[user@CE340 Downloads]# ./Cisco-Edge-1.1-i386-DVD.bin
```

### Unable To Log In

If you cannot log in to the system, perform the following steps to recover:

- 
- Step 1** Press **F12** when you start the Cisco Edge 340 Series device to enter the privileged mode.
  - Step 2** Choose **SYSRecovery PMAP** as the boot device in [Figure A-1](#).
  - Step 3** You will see the following options:
    - Install Cisco-Edge in Keep User Data Mode—Reimage your device with /home partition reserved.
    - Install Cisco-Edge in Clean User Data Mode—Reimage your device with /home partition wiped. All the configuration, user application, and data will be wiped out.
  - Step 4** Choose the option that you want to install.
- 

## Creating USB Recovery Disk

Use the procedures in the “[Forget Root Password](#)” section on page A-1 to create a USB recovery disk. However, this is not a recommended method. When you reimage your device using this method, the SYSRecovery function will not refresh with your current installed version of image. The next time you use the functions, they either cannot work or forces your system to roll back to the old version.

There is a work around to solve this problem. After your system is recovered by using the external USB disk, run the following command to reimage the system again with normal process and refresh the system recovery partition:

```
[user@CE340 root]$ su
[user@CE340 ~]# cd /home/user/Downloads/
[user@CE340 Downloads]# chmod 777 Cisco-Edge-1.1-i386-DVD.bin
[user@CE340 Downloads]# ./Cisco-Edge-1.1-i386-DVD.bin
```

## Restore Factory Settings Action Fails in Web GUI

If you fail to restore the factory settings in the Web GUI, try again by clicking **Restart/Reset** in the left pane under the Administration tab.

# Display Issues

This section provides troubleshooting information about display issues.

## No Signal Output

If you do not find signal output after connecting a monitor, and the network status of the Cisco Edge 340 Series device is disconnected, follow these steps:

- 
- Step 1** Check if power is flowing to the monitor.
- Step 2** Check if the VGA or HDMI connector is correctly connected.
- Step 3** If both the power and connection are fine, use the console port to trouble shoot. Log in to the system with root permission. Enter the **DISPLAY:=0.0 xrandr** command to check if the monitor is detected by the Cisco Edge 340 Series device.



---

**Note** If the issue is not resolved, reboot the device.

---

## Screen Blurred After Resolution is Changed

If you find the screen is blurred after changing the resolution, take one of the following actions:

- Check the connection of the Cisco Edge 340 Series device and the monitor, and restart the system.
- Change the current resolution to a new value in the web GUI.

## Network Issues

This section provides troubleshooting information about network issues.

### Connection Status Not Refreshed in the WiFi Station Mode

In the WiFi station mode, if you find that the connection status is not refreshed to be connected after connecting to an AP, click the **Refresh** button in the web GUI. If the issue still exists, click the **Wireless** option on the left navigation pane to refresh the screen.

### Wake On LAN Not Effective

If the Wake on LAN is not effective, take one of the following actions:

- Verify that the Wake on LAN function is enabled on the Cisco Edge 340 Series device.
- Verify that the remote devices and the Cisco Edge 340 Series device are in the same broadcast domain.

## DNS Not Parsed

Cisco Edge 340 Series supports up to three DNS servers. If the top three DNS servers cannot be parsed, other DNS servers can not be used although they are valid.

If the DNS cannot be parsed, edit the `resolve.config` file by entering the `#vi /etc/resolve.config` command to replace the top three DNS servers with the other valid servers.

## Third-Party Device Cannot be Connected

If a third-party device that is in the station mode cannot connect to the Cisco Edge 340 Series device that is in the AP mode, take one of the following actions:

- Verify if the encryption and authentication mechanism between the third-party device and Cisco Edge 340 Series are matched.
- Verify if the network card in the third-party device supports 5G. The network cannot be connected unless this item is matched.

## Unstable Connection Due to Multiple SSIDs

In the Wi-Fi station mode, when a Cisco Edge 340 series device connects to an AP (for example, a Cisco Aironet series AP) with multiple hidden SSIDs on a single BSSID, the connection will be unstable and even failed. In this case, you are recommended to enable multiple BSSIDs on the AP.

## Wait Before Reconnecting

When you need to switch to another subnet, wait 5 to 8 seconds before you re-establish the network connectivity.

For more information, see <https://bugs.launchpad.net/ubuntu/+source/network-manager/+bug/894082>.

## Power Issues

This section provides troubleshooting information about power issues.

### Power Shortage of Peripheral Equipment

If the peripheral equipment is suffering from a power shortage and the Cisco Edge 340 Series device is powered by Power Over Ethernet (PoE), verify if the device is powered by PoE 802.3AF. If yes, change it to the 802.3AT mode, because the power supported by 802.3AT is more stable than the power supported by 802.3AF.

## USB Ports on the Rear Panel Not Working

If only the two USB ports on the front panel are working, and the USB ports on the rear panel have no power, verify if the Cisco Edge 340 Series device is powered by PoE. To enable the USB ports on the rear panel, use external power supply.





# SNMP Information

Cisco Edge 340 Series supports Simple Network Management Protocol (SNMP), so that you can monitor hundreds of Cisco Edge 340 Series devices in the same time.

This appendix provides information about the SNMP information with Cisco Edge 340 Series in the following sections:

- [Compatibility, page B-1](#)
- [Supported MIB Information, page B-1](#)

## Compatibility

Cisco Edge 340 Series supports only SNMP v3. The SNMPv3 authentication is performed by using a users authKey to sign the message being sent. The authProtocol must be SHA, and the private key must be AES. Both authKeys and privKeys are generated from a passphrase that must be at least 8 characters in length.

## Supported MIB Information

[Table B-1](#) provides the MIB information that the Cisco Edge 340 Series supports using SNMP:

**Table B-1** Supported MIB Information

| Information         | Oid                     | Name                                                                                                                                                                                                       |
|---------------------|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CPU usage           | .1.3.6.1.4.1.2021.10    | UCD-SNMP-MIB::laTable<br>Load-1 (1 minute load): .1.3.6.1.4.1.2021.10.1.3.1<br>Load-5 (5 minute load): .1.3.6.1.4.1.2021.10.1.3.2<br>Load-15 (15 minutes load): .1.3.6.1.4.1.2021.10.1.3.3                 |
|                     | .1.3.6.1.4.1.2021.11    | UCD-SNMP-MIB::systemStats<br>Percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0<br>Percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0<br>Percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0 |
| Version information | .1.3.6.1.4.1.9.1.1095.4 | —                                                                                                                                                                                                          |
| Disk Utilization    | .1.3.6.1.4.1.2021.9     | UCD-SNMP-MIB::dskTable                                                                                                                                                                                     |
| Hostname            | .1.3.6.1.2.1.1.5        | SNMPv2-MIB::sysName                                                                                                                                                                                        |

**Table B-1** Supported MIB Information

| Information                        | Oid                          | Name                                                 |
|------------------------------------|------------------------------|------------------------------------------------------|
| Interface status and configuration | .1.3.6.1.2.1.2.2             | IF-MIB::ifTable                                      |
| IP Address                         | .1.3.6.1.2.1.4.20            | IP-MIB::ipAddrTable                                  |
| Wi-Fi AP                           | .1.3.6.1.4.1.9.1.1095.2.1    | CISCO-CE340-MIB:wifiAPMib                            |
| Wi-Fi Client                       | .1.3.6.1.4.1.9.1.1095.2.2    | CISCO-CE340-MIB:wifiClientMib                        |
| Wi-Fi                              | .1.3.6.1.4.1.9.9.272.1.1.1.6 | CISCO-DOT11-IF-MIB::cd11IfAuxSsidTable               |
|                                    | .1.3.6.1.4.1.9.9.272.1.1.2.5 | CISCO-DOT11-IF-MIB::cd11IfPhyDsssTable               |
|                                    | .1.3.6.1.4.1.9.9.413.1.1.1   | CISCO-DOT11-SSID-SECURITY-MIB::cdot11SecAuxSsidTable |
| USB Devices Name and status        | .1.3.6.1.4.1.9.1.1095.1      | CISCO-CE340-MIB:usbMib                               |
| USB Devices Name and status        | .1.3.6.1.3.103.1.3           | USB-MIB::usbDeviceTable                              |
| NTP server IP address              | .1.3.6.1.4.1.9.1.1095.5      | CISCO-CE340-MIB:ntpMib                               |
| DHCP server IP address             | .1.3.6.1.4.1.9.1.1095.3      | CISCO-CE340-MIB:dhcpMib                              |



# Configuring SCEP and Obtaining and Enrolling the Certificate

Cisco Edge 340 Series supports Simple Certificate Enrollment Protocol (SCEP) since software Release 1.2 patch 12.

## Components Used

The information in this document is based on these software and hardware versions:

- Windows 2008 server
- Server with a Certificate Authority (CA) available
- Cisco Edge 340



### Note

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any commands.



### Note

For more information on the SCEP server configuration, see <http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-nds-in-active-directory-certificate-services-ad-cs.aspx>

To configure SCEP and obtain and enroll the certificate, follow these steps:

**Step 1** Establish a secure shell (SSH) connection with the CE340.

**Step 2** Apply the SCEP patch image.

For detailed information about applying the patch 1.2.0.12, see the release notes for patch 12.

**Step 3** Create a text file with SCEP server information as following:

```
[root@340 home]# cat api.txt
{
 "module": "http",
 "managed": "true",
 "url": "http://<SCEP_Server_IP>/CertSrv/mscep/mscep.dll",
 "challenge_password": "",
 "params": {
 "keysize": 2048,
```

```

 "subject":
 "/C=IN/ST=Bangalore/O=Example/CN=test.example.com/emailAddress=admin@example.com"
 }
}

```

| Parameter          | Description                                                                                                                           |                                                                                                                                                                            |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| module             | Specifies the module to be enabled. Currently, the only supported value is web server: http.                                          |                                                                                                                                                                            |
| managed            | Specifies whether or not need SCEP manage.                                                                                            |                                                                                                                                                                            |
| url                | Specifies CA server URL.<br>For example: http://10.75.212.202/CertSrv/mscep/mscep.dll”                                                |                                                                                                                                                                            |
| challenge_password | (Optional) The value of this field depends on the server settings.<br>For example, if EnforcePassword=0, this field need to be empty. |                                                                                                                                                                            |
| params             | CSR and private key related parameters.                                                                                               |                                                                                                                                                                            |
|                    | Parameter                                                                                                                             | Description                                                                                                                                                                |
|                    | keysize                                                                                                                               | The value is 2048, 4096, or 8192.                                                                                                                                          |
|                    | subject                                                                                                                               | Certificate subject. For example,<br><br>/C=<Country Name>/ST=<State>/L=<Locality Name>/O=<Organization Name>/CN=<Common Name><br><br>Supported subjects are as following: |
|                    | Subject Key Name                                                                                                                      | Description                                                                                                                                                                |
|                    | C                                                                                                                                     | Country name                                                                                                                                                               |
|                    | ST                                                                                                                                    | State                                                                                                                                                                      |
|                    | L                                                                                                                                     | Locality name                                                                                                                                                              |
|                    | O                                                                                                                                     | Organization name                                                                                                                                                          |
| CN                 | Common name                                                                                                                           |                                                                                                                                                                            |
| OU                 | Organization unit                                                                                                                     |                                                                                                                                                                            |
| emailAddress       | Email address                                                                                                                         |                                                                                                                                                                            |

| Return Value | Description |
|--------------|-------------|
| “”           | Success.    |
| Others       | Exceptions. |

**Step 4** Set SCEP server information.

```

curl -X PUT -u root:ADMIN123# -H "Content-Type:application/json" -d @api.txt
http://127.0.0.1/api/v3/system/scep

```

**Step 5** Call get\_ca.

```

curl -X PUT -u root:ADMIN123# -H "Content-Type:application/json" -d
'{"method": "getca", "module": "http"}' http://127.0.0.1/api/v3/system/scep/command

```

**Step 6** Call enroll.

```
curl -X PUT -u root:ADMIN123# -H "Content-Type:application/json" -d
'{"method": "enroll", "module": "http"}' http://127.0.0.1/api/v3/system/scep/command
```

**Step 7** Certificate will be saved.

```
pwd
/usr/local/share/cpgmt-service/scep/keystore/http
ls cert/
server.crt
```

**Step 8** Check the certificate in CE340.

```
openssl x509 -in /usr/local/share/cpgmt-service/scep/keystore/http/cert/server.crt -text
```

**Step 9** Restart the nginx server or reboot the device.

```
service nginx restart
```

**Step 10** Certificate can be checked in the CE340 browser as well as in the NDES server issued certificates.

**Table C-1 Supported Methods and SCEP Server**

|         | NDES (Windows 2008) | NDES (Windows 2003) |
|---------|---------------------|---------------------|
| getca   | Supported           | Supported           |
| enroll  | Supported           | Supported           |
| getcert | Supported           | Supported           |
| getcrl  | Not supported       | Supported           |





## Importing the SHA2 Certificate

This appendix describes importing the SHA2 certificate to the Cisco Edge 340 Series. The details of creating, getting, or generating the certificate are not provided in this document.

There are two ways to import the SHA2 certificate in CE340:

- [Certificate API, page D-1](#)
- [SCEP API, page D-3](#)

## Certificate API

The Cisco Edge 340 Series support certificate generated from Non-SCEP server as well.

Certificate API user should have key file of certificate with it.



### Note

Make sure to provide hostname of CE340 in Common Name Field while creating or getting certificate.

Following are the steps to insert certificate using Certificate API:

**Step 1** To generate the Key and CSR from the CE340 CLI:

```
i. # openssl genrsa -out key_name.key 2048
```

### Example

```
[root@CE340 home]# openssl genrsa -out 340.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
[root@CE340 home]# pwd
/home
[root@CE340 home]# ls
340.key api.txt lost+found ssid.txt user
[root@CE340 home]#
```

```
ii. # openssl req -out sha256.csr -key key_name.key -new -sha256
```

**Example**

```
[root@CE340 home]# openssl req -out sha256.csr -key 340.key -new -sha256
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [XX]:
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:340.com
Email Address []:email.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:xxxx
[root@CE340 home]#
[root@CE340 home]#
[root@CE340 home]#
[root@CE340 home]# ls
340.key api.txt lost+found sha256.csr ssid.txt user
[root@CE340 home]#
```

**Step 2** Generate the certificate from the CA server using CE340 CSR.

**Step 3** To load the certificate from the local storage, use the following command:

```
curl -k -X PUT -u root:ADMIN123# https://127.0.0.1/api/v3/import/certificate/nginx
--form key=@<path to certificate key file> --form crt=@<path to crt file>
```

**Example**

```
curl -k -X PUT -u root:ADMIN123# https://127.0.0.1/api/v3/import/certificate/nginx --form
key=@/home/tmp/server.key --form crt=@/home/tmp/server.crt
```

Upon success the # prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the # prompt will be shown.

**Step 4** To load the certificate from a remote server, use the following command:

```
curl -k -X PUT -u root:ADMIN123# https://127.0.0.1/api/v3/import/certificate/nginx
--form key=<link location of remote server key file> --form crt=<link location of remote
server crt file>
```

**Example**

```
curl -k -X PUT -u root:ADMIN123# https://127.0.0.1/api/v3/import/certificate/nginx --form
key=http://10.107.3.155:8080/server.key --form crt=http://10.107.3.155:8080/server.crt
```

Upon success the # prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the # prompt will be shown.



**Step 5** To verify that the newly loaded certificate is inserted, use the following command:

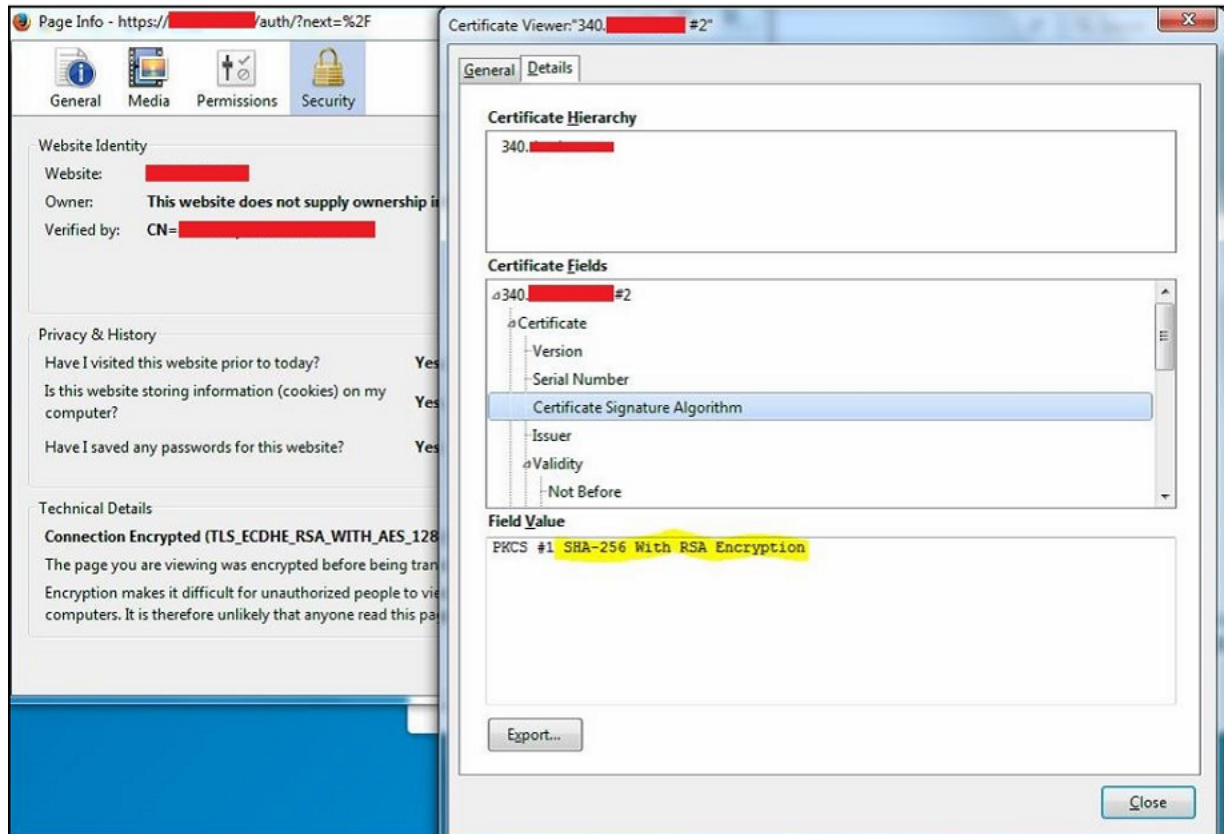
```
curl -k -X GET -u root:ADMIN123# https://127.0.0.1/api/v3/import/certificate/nginx
```

This command will display the newly inserted certificate. Upon success the # prompt will be shown on the screen after the above command is executed.

**Step 6** After loading the new certificate, restart the nginx server by executing the following command:

```
service nginx restart
```

**Step 7** Check the certificate in GUI as following:



## SCEP API

Follow these steps to get certificate from the NDES server:

**Step 1** Upgrade or reimage the device with the new 1.2.0.19 patch.

**Step 2** Connect to the CE340 via SSH.

**Step 3** Create a file named as `api.txt` by using the text editor present in CE340.

Following is a sample file. Please change the values in **bold** and *italic* according to your requirement.

**Note**

Make sure to provide hostname of CE340 in Common Name Field while creating or getting certificate.

```
{
 "module": "http",
 "managed": "true",
 "url": "http://<SCEP-Server-ip>/CertSrv/mscep/mscep.dll",
 "challenge_password": "<SamplePassword>",
 "params": {
 "keysize": 2048,
 "subject":
 "/C=<country-name>/ST=<state-name>/O=<organization-name>/CN=<device-hostname>/emailAddress
 =email@yourcompnay.domain"
 }
}
```

**Step 4** Execute the following command at the same location where `api.txt` was created to configure the SCEP server information:

```
curl -X PUT -u root:ADMIN123# -H "Content-Type:application/json" -d @api.txt
http://127.0.0.1/api/v3/system/scep
```

Upon success the `#` prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the `#` prompt will be shown.

**Step 5** Verify that the certificate request file and private key are generated:

```
openssl req -in /usr/local/share/cpgmt-service/scep/keystore/http/csr/server.csr -noout
- text
```

```
[root@test-340 ~]# openssl req -in /usr/local/share/cpgmt-service/scep/keystore/http/csr/server.csr -noout -text
Certificate Request:
Data:
 Version: 0 (0x0)
 Subject: C=IN, ST=KA, O=, CN=340. .com/emailAddress= .com
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:c8:a0:85:ea:23:9e:7e:29:ae:5b:47:8e:40:ed:
 6d:84:d0:c0:5a:ae:c6:0a:fa:71:fd:63:79:27:12:
 0e:d6:de:22:87:ad:67:96:8e:01:1a:80:f1:b9:c3:
```

**Step 6** Call `get_ca`:

```
curl -X PUT -u root:ADMIN123# -H "Content-Type:application/json" -d
'{"method": "getca", "module": "http"}' http://127.0.0.1/api/v3/system/scep/command
```

Upon success the `#` prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the `#` prompt will be shown.

**Step 7** Call `enroll`:

```
curl -X PUT -u root:ADMIN123# -H "Content-Type:application/json" -d
'{"method": "enroll", "module": "http"}' http://127.0.0.1/api/v3/system/scep/command
```

Upon success the `#` prompt will be shown on the screen after the above command is executed.

Upon failure the generic failure message will be shown on the screen and then the `#` prompt will be shown.

**Step 8** Make sure the certificate is generated and saved locally on CE340:

```
ls /usr/local/share/cpgmt-service/scep/keystore/http/cert server.crt
```

**Step 9** Make sure that relevant or valid details are present in the certificate:

```
openssl x509 -in /usr/local/share/cpgmtservice/scep/keystore/http/cert/server.crt -text
```

```
[root@test-340 cert]# openssl x509 -in /usr/local/share/cpgmt-service/scep/keystore/http/cert/server.crt -text
Certificate:
 Data:
 Version: 3 (0x2)
 Serial Number:
 13:b7:23:c8:00:01:00:00:00:0e
 Signature Algorithm: sha1WithRSAEncryption
 Issuer: DC=com, DC=, DC=, CN=-CA
 Validity
 Not Before: May 28 12:19:09 2015 GMT
 Not After : May 27 12:19:09 2017 GMT
 Subject: C=IN, ST=KA, O=, CN=340.com/emailAddress=@.com
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:c8:a0:85:ea:23:9e:7e:29:ae:5b:47:8e:40:ed:
```

**Step 10** Restart the nginx server or reboot the device. This step will insert the SCEP certificate in CE340.

```
[root@test-340 cert]# service nginx restart
Redirecting to /bin/systemctl restart nginx.service
[root@test-340 cert]#
```

**Step 11** Check the certificate in GUI as well as in NDES server to ensure that the correct certificate is inserted.

