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.

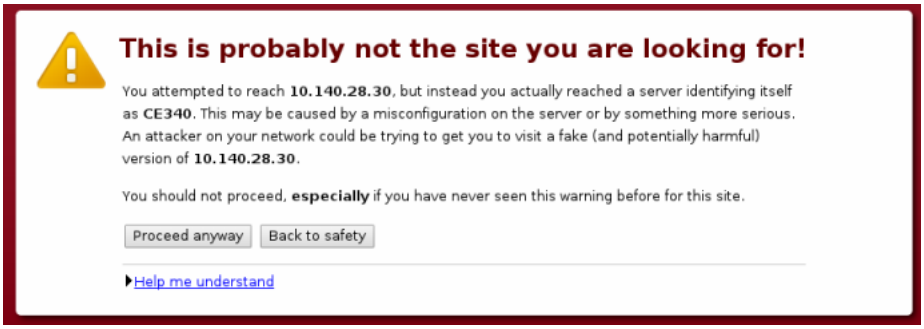
To configure a Cisco Edge 340 Series device using the web-based GUI, follow the steps described in these sections:

Logging In to the Web GUI

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

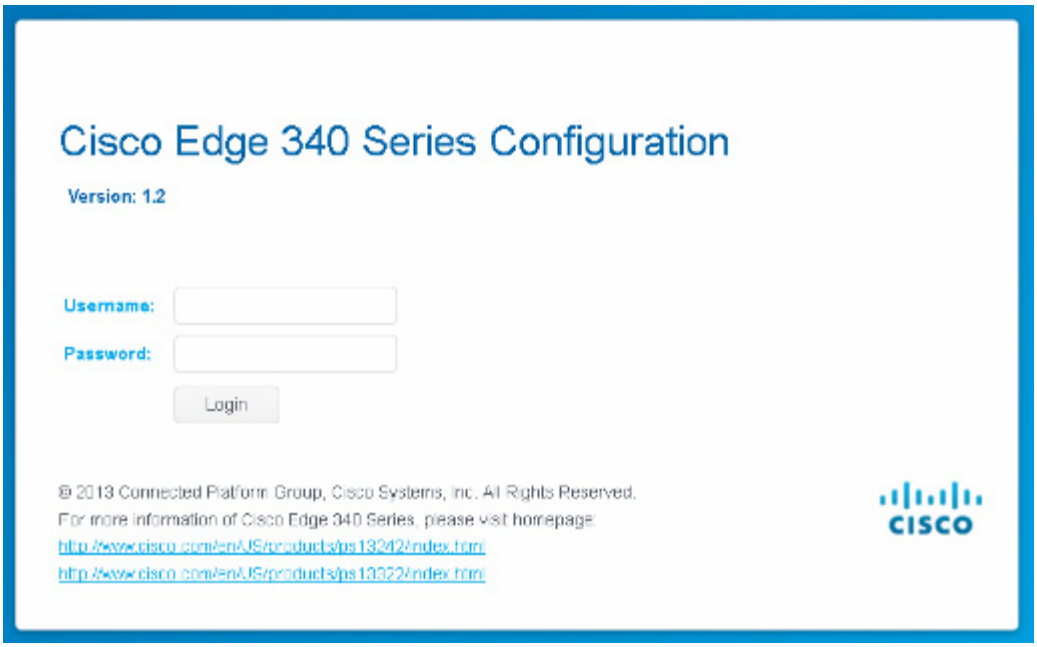


- Click **Preference** on desktop and log in by entering the username and password of system account (Figure 2-2). The default username is **admin**, and the default password of the admin account is **aDMIN123#**.

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.

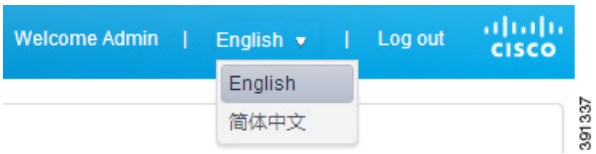
Figure 2-2 Log in Page



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



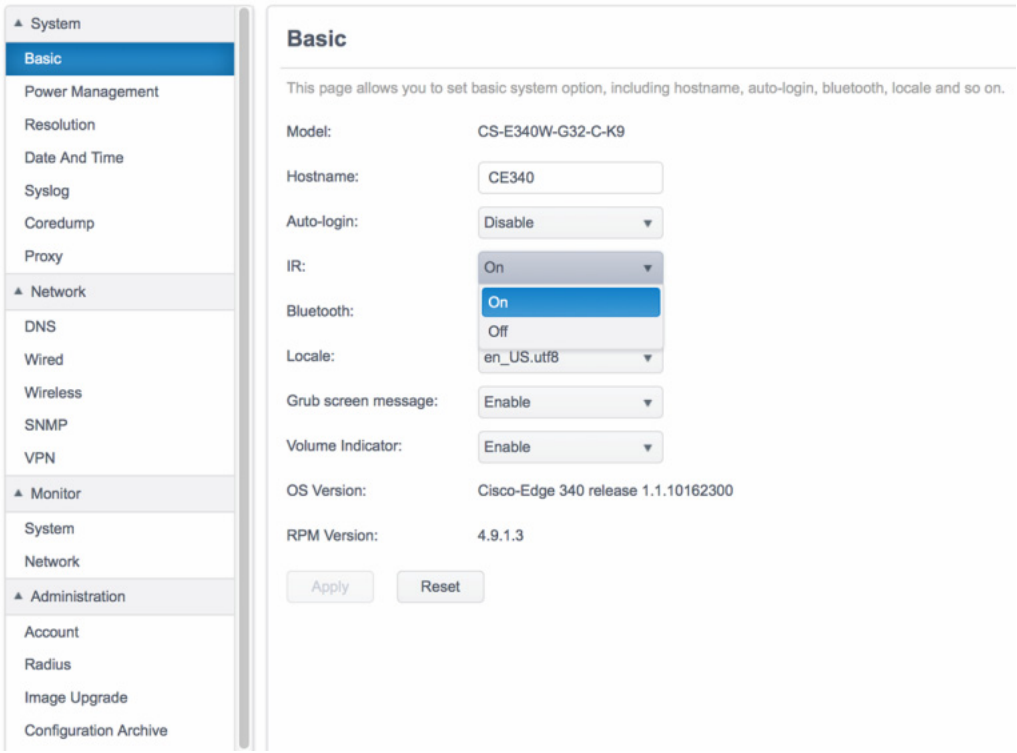
System Configuration

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



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

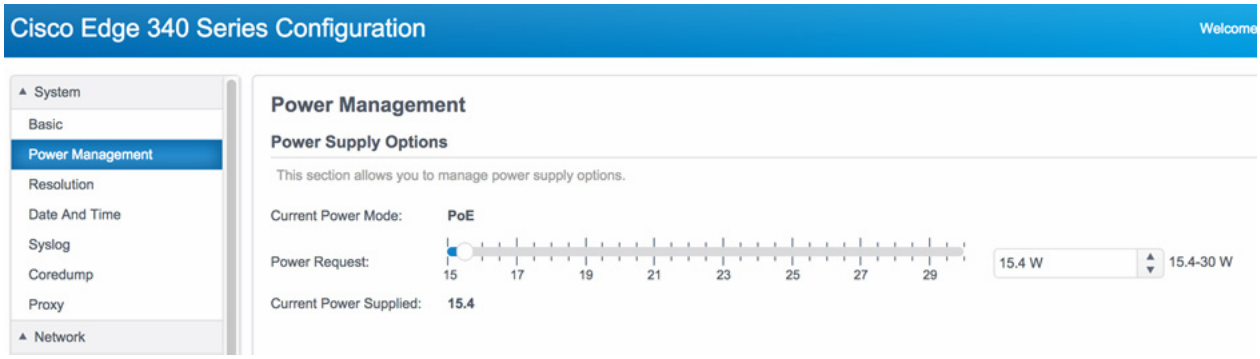
In the PoE Mode, you can request more power supply.

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

Step 1 Click **Power Management** under System in the left pane.

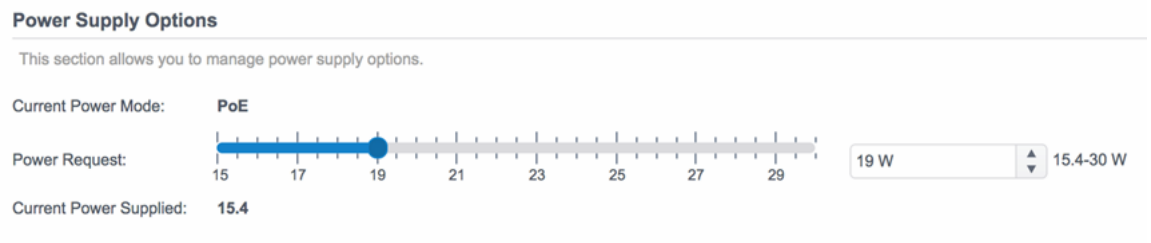
Step 2 Check whether the Current Power Mode is PoE, as shown in Figure 2-5. You can also get the current power in the Current Power Supplied field.

Figure 2-5 Power Management Tab



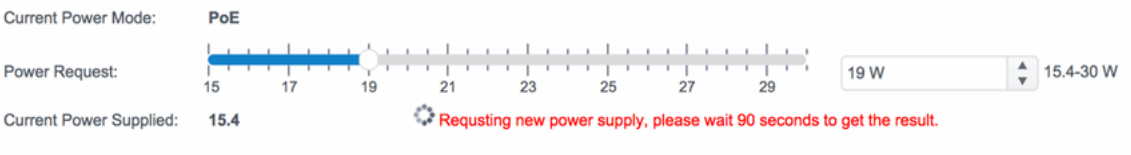
Step 3 Drag the slide bar in the Power Request field, or input new power value in the input box at the end of the Power Request field. For example, in Figure 2-6, the power is upgraded from 15.4 W to 19 W.

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.

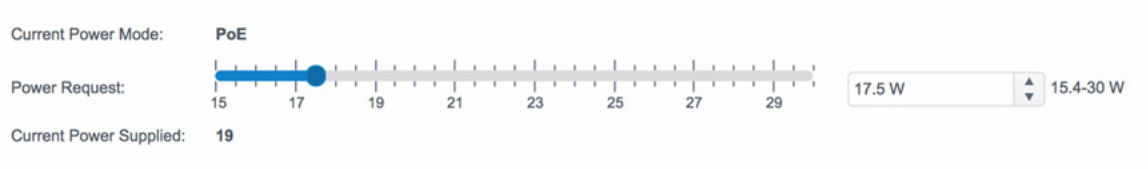
Follow these steps to request downgrading the power supply in the PoE mode:

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.

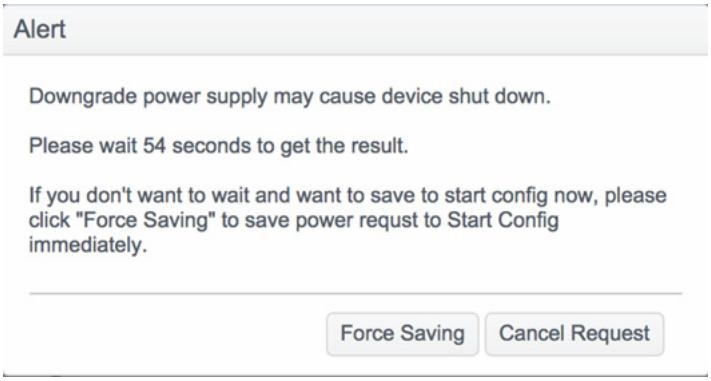
Step 3 Drag the slide bar in Power Request, or input new power value in the input box at the end of the Power Request item. For example, in Figure 2-9, the power is downgraded from 19 W to 17.5 W.

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

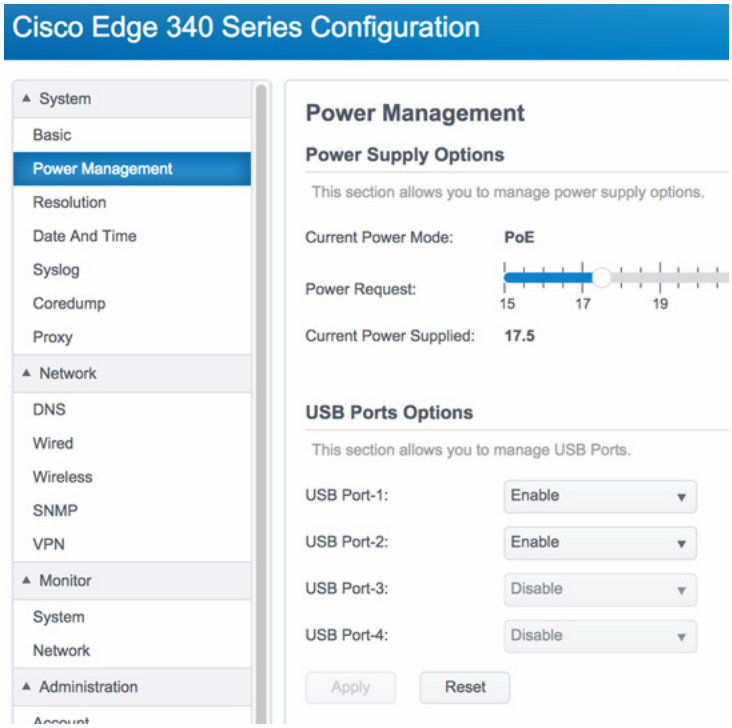
Configuring the USB Ports

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

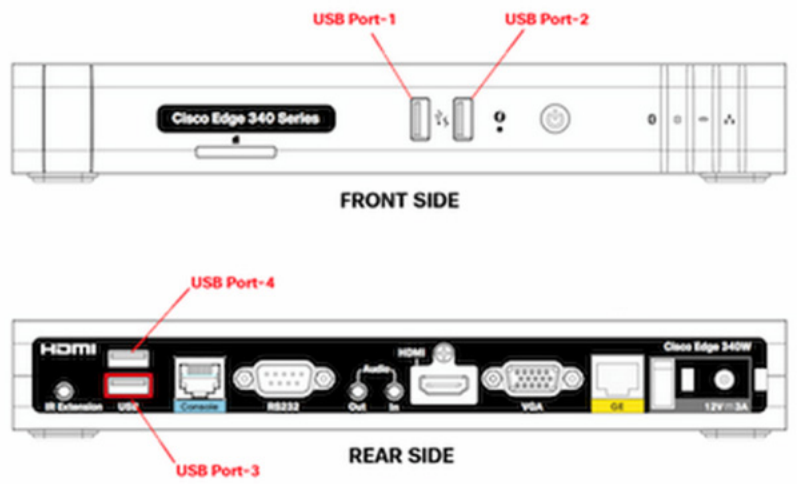


Step 2 Choose **Enable** or **Disable** from the drop-down list for each USB port.

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

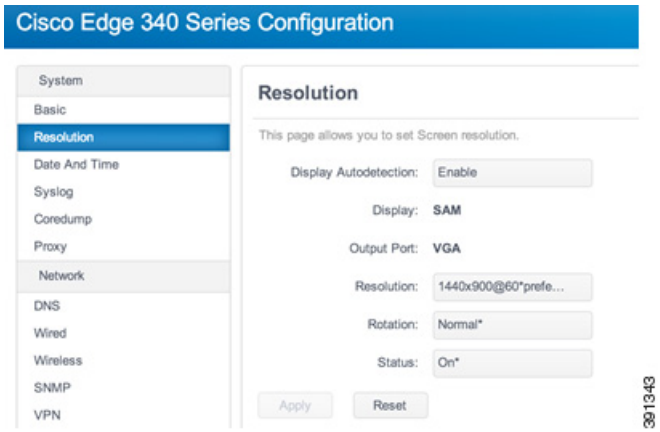
Follow these steps to configure the resolution information of single monitor when auto detection is enabled:

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

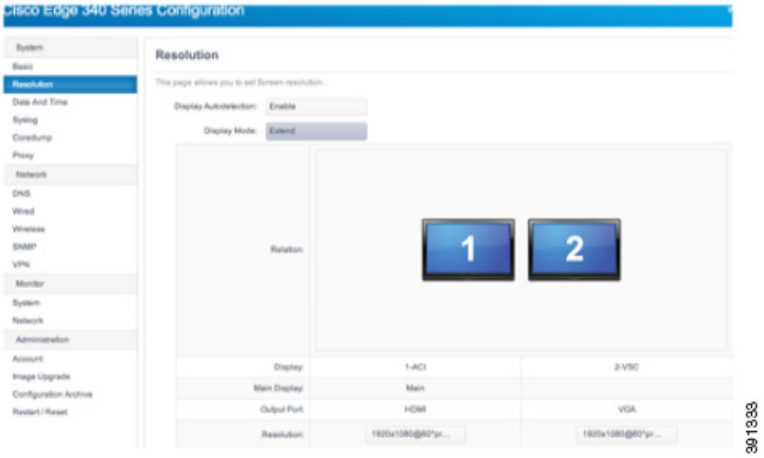
Follow these steps to configure the resolution information of dual monitors when auto detection is enabled:

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

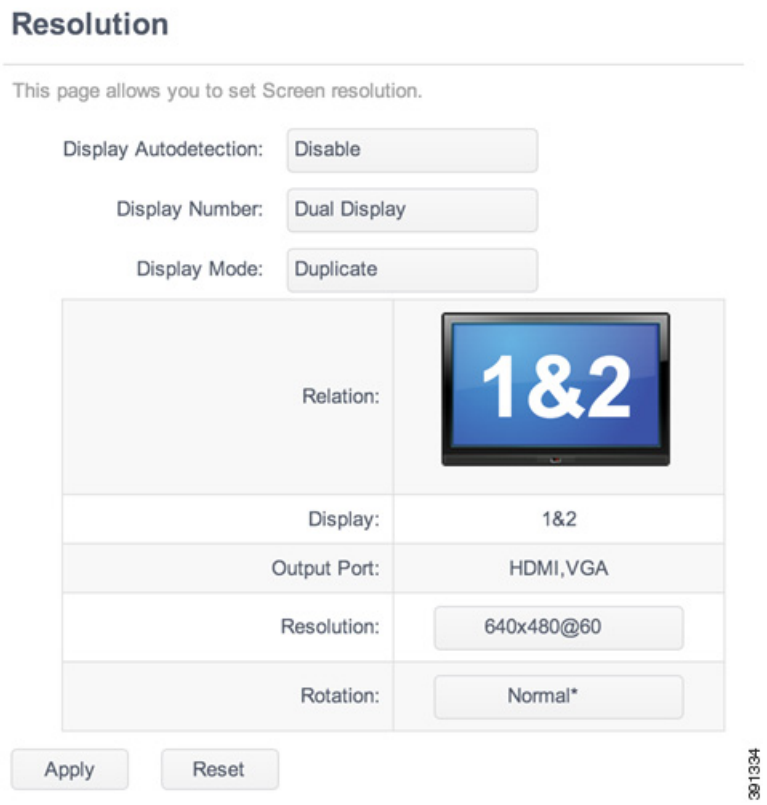
When auto detection is disabled, all modes (single, duplicate, and extend) can be configured no matter whether the monitors are connected or not. The resolution list is retrieved from the file /usr/etc/.force_resolution_list.txt. There are four modes that you can choose with the options Display Number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



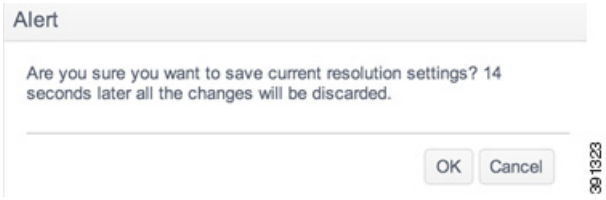
Step 3 You can view or configure the following information of the monitors:

- 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

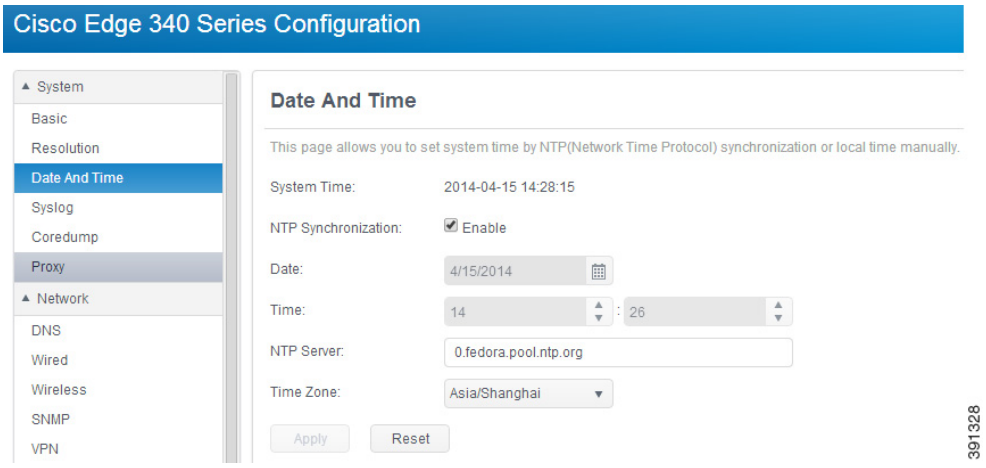
You can configure system date and time, NTP servers and time zone information in the **Date and Time** tab.

Configuring System Time Manually

Follow these steps to configure system time manually:

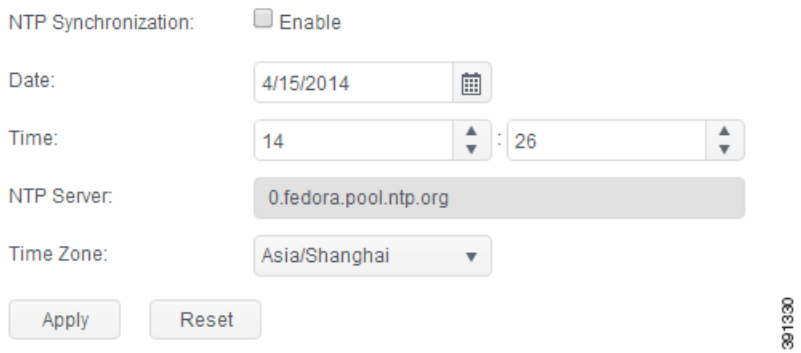
Step 1 Click **Date and Time** under System in the left pane. The Date and Time tab is displayed, as shown in Figure 2-18.

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



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.

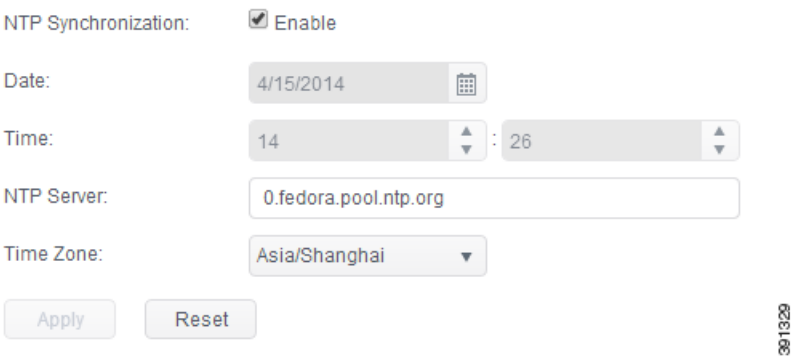
Configuring System Time by Auto-Sync With NTP Servers

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



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.

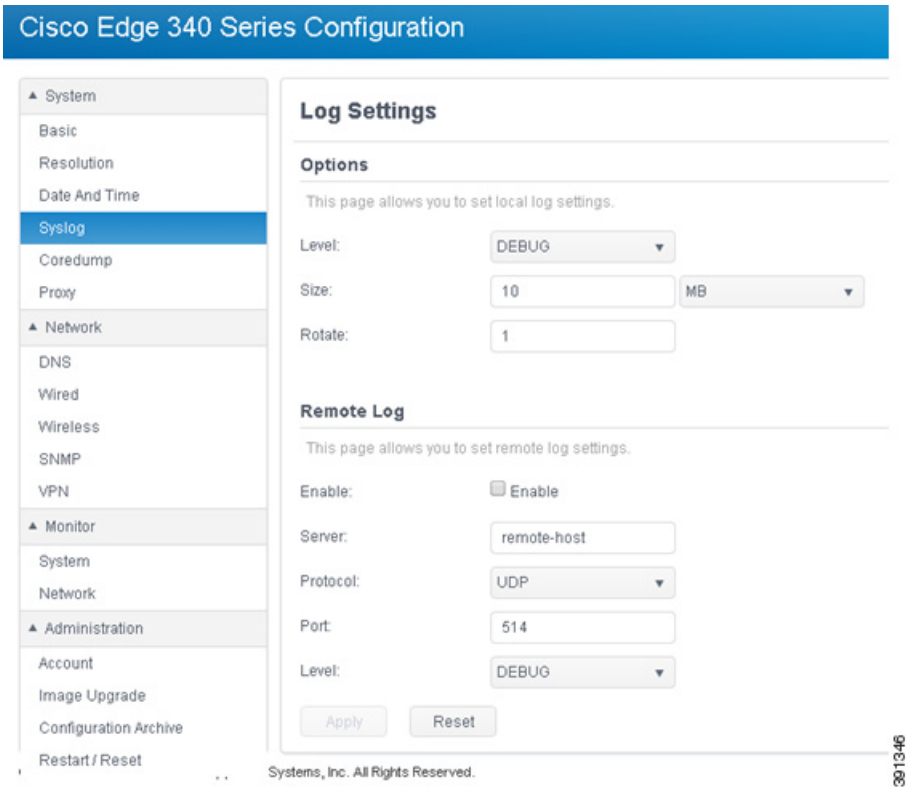
Step 4 Choose a time zone from the Time Zone drop-down list.

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



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

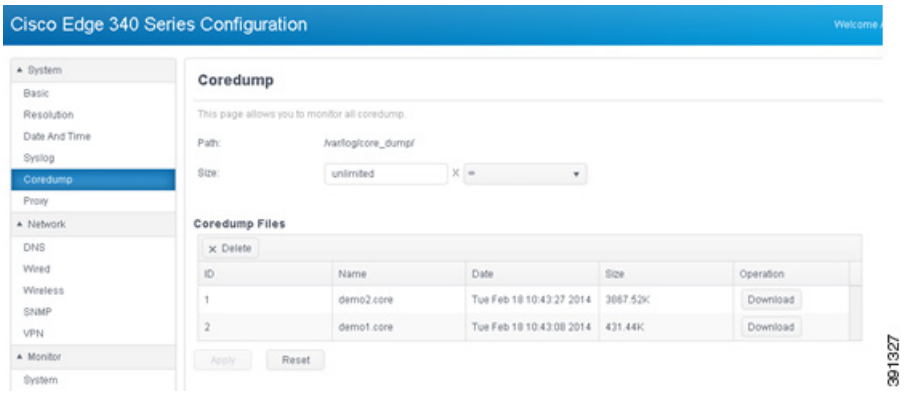
Note These options are listed in the order from low to high priority. When you specify a priority, the one you choose and all the others that are higher than the one you choose are selected too.

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 filed is left empty, the HTTP Proxy setting will be cleared. If the proxy requires authentication, the IP address or hostname filed 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 filed is left empty, the HTTPs proxy setting will be cleared. If the proxy requires authentication, the IP address or hostname filed 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 filed is left empty, the FTP proxy setting will be cleared. If the proxy requires authentication, the IP address/hostname filed 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.

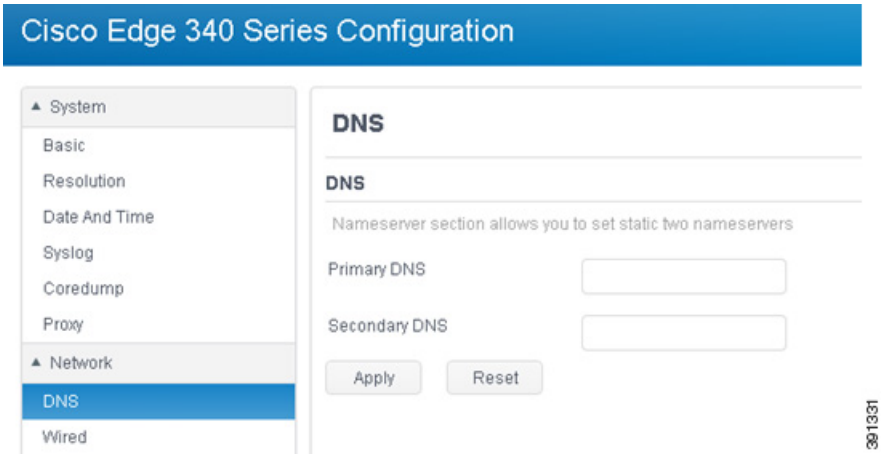
Configuring DNS

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.

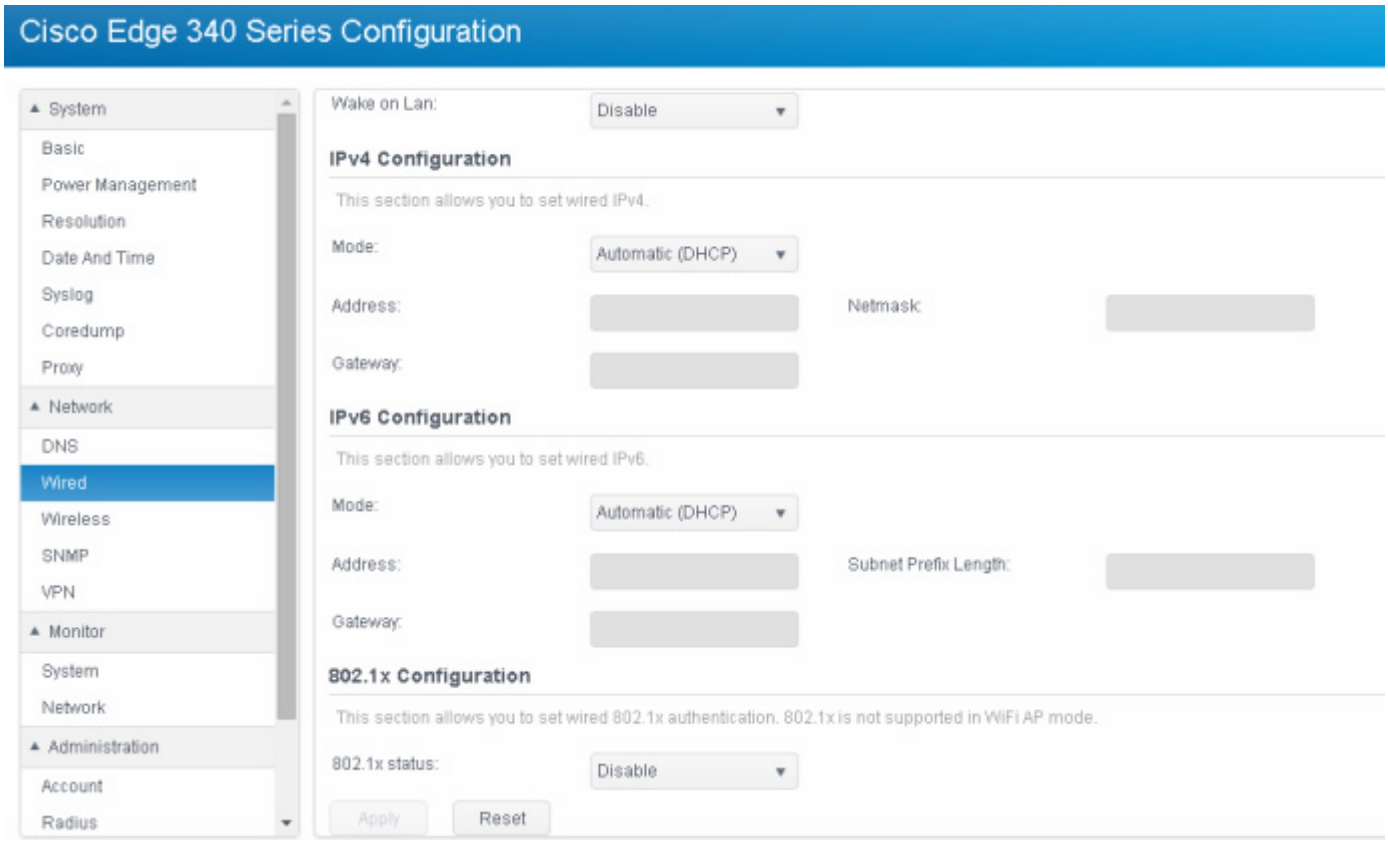
Note When the Primary DNS field is empty, the Secondary DNS must be Empty too.

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



Follow these steps to configure wired link and address settings.

Step 1 (Optional) Configure wired link settings.

a. Choose a link negotiation mode from the Mode drop-down list. Valid options are:

- Auto—Auto negotiation on speed an duplex.
- Manual—Manually set speed and duplex.

b. If you choose Manual mode, choose speed and duplex mode from the Speed and Duplex drop-down list.

c. 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.

a. 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.

b. 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:

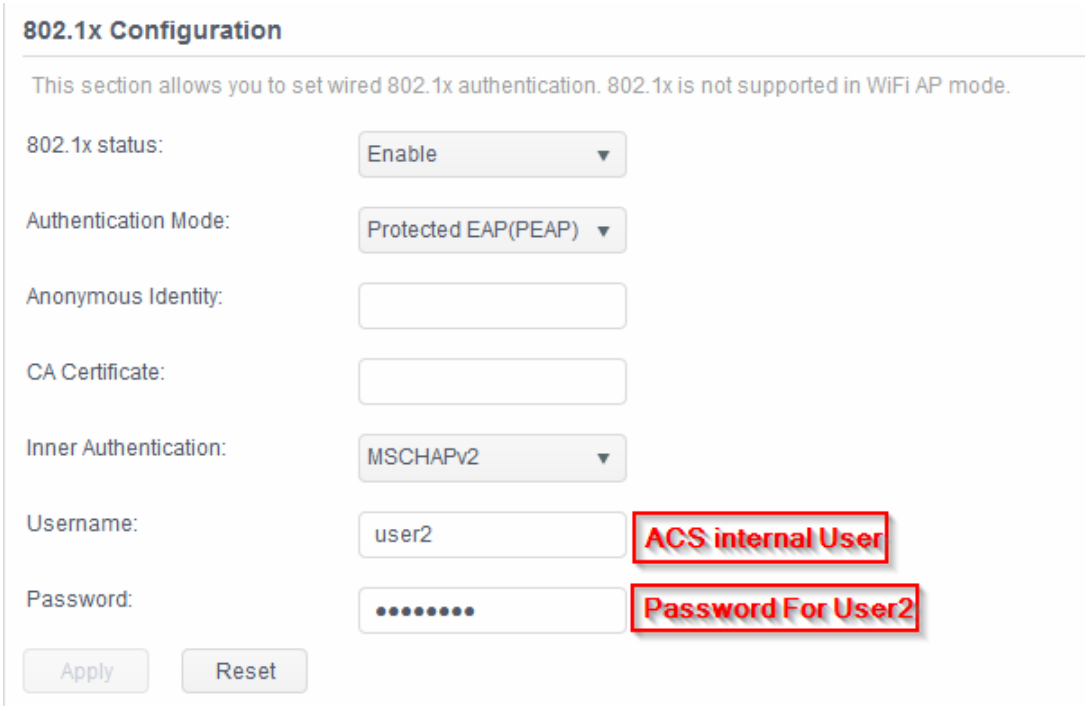
- Automatic (DHCP)—Use DHCP to get IPv6 information and DNS information.
- Manual—Manually set IPv6 information. The Address and Netmask fields are mandatory. The gateway and IP address must be in the same network.

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



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 f**rom 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
```

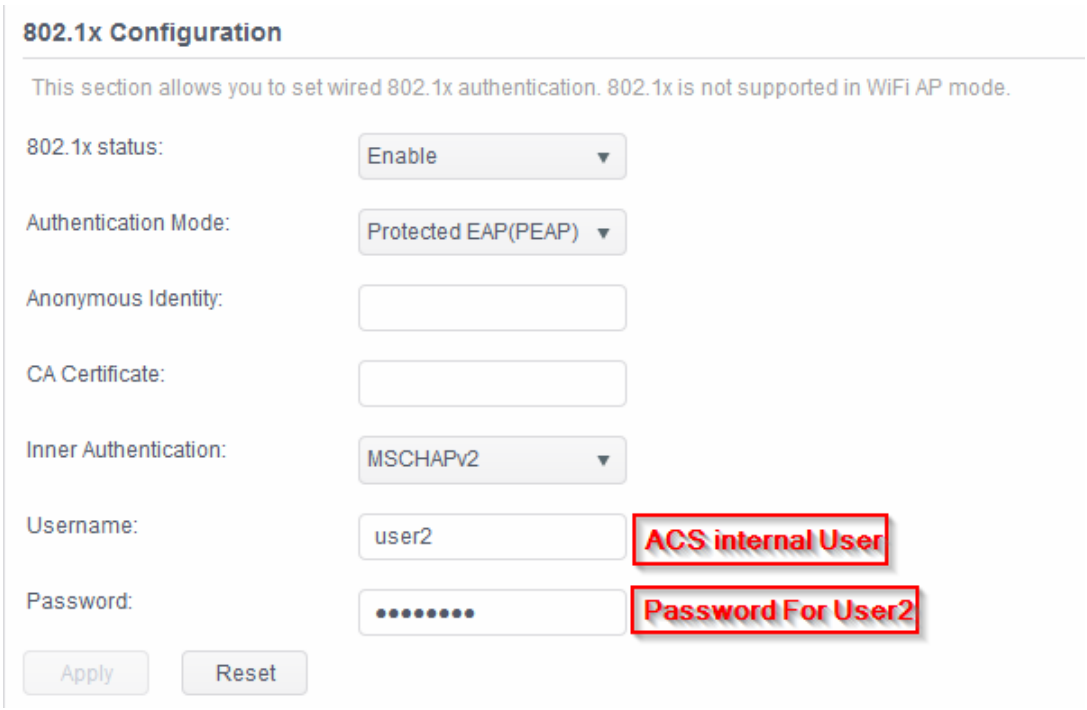
Use the following steps to configure the CE340:

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



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

Figure 2-28 Inner Authentication Setting

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

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

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.

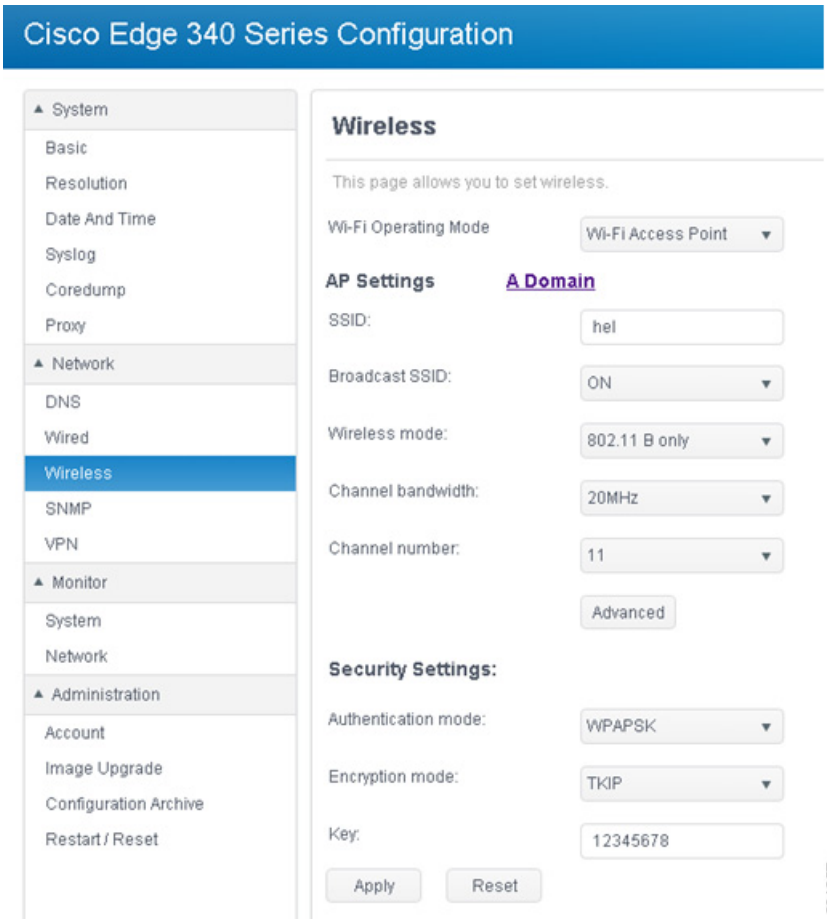
To select a desired wireless mode, click **Wireless** in the left pane and configure the settings for each mode.

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/WPAP2PSK/WPAPASKWPA2PSK length: 8–63
- WPA/WPA2/WPAWPA2 length: 0–64

d. Radius Server IP—Radius Server IP address.

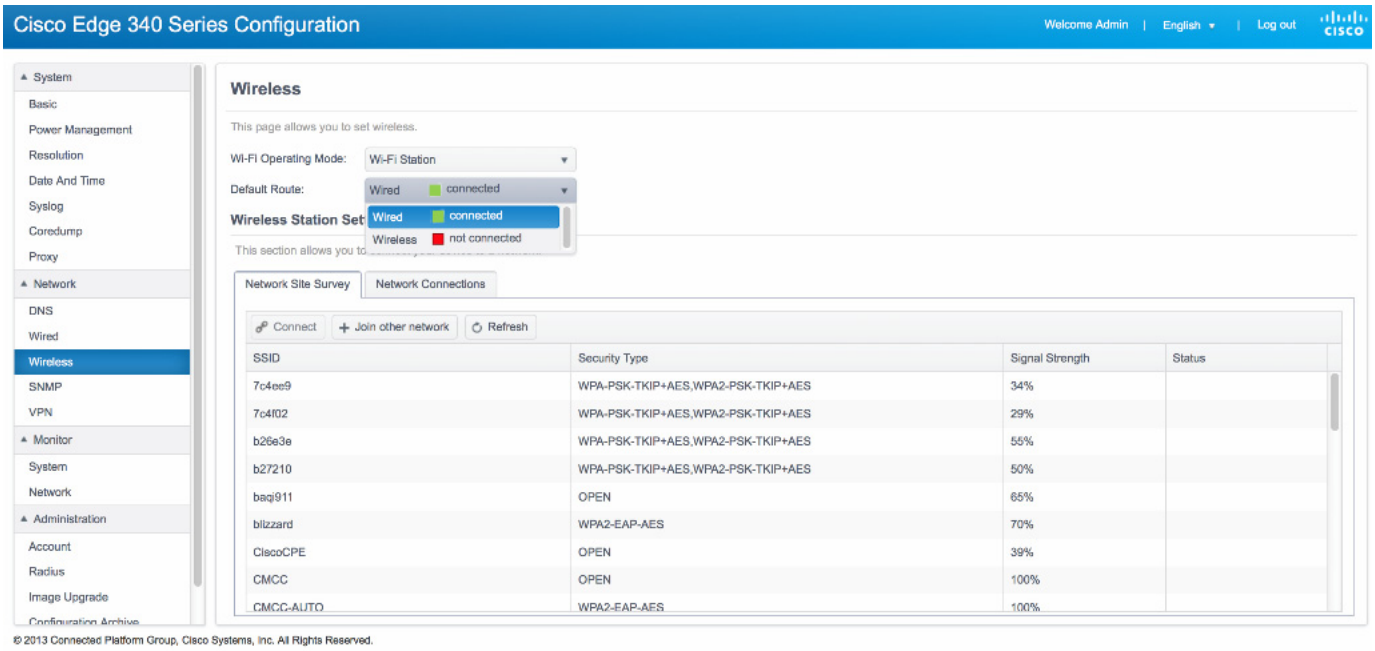
e. Radius Server Port—Default value is 1812.

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



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

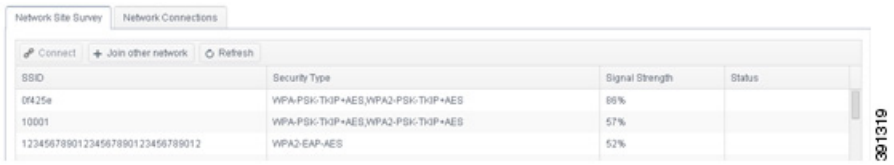
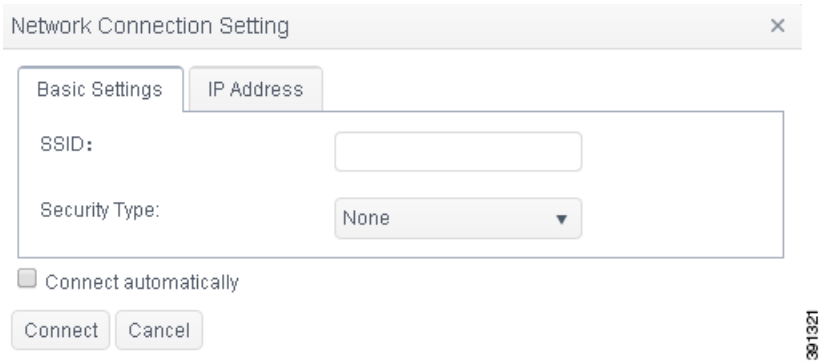


Figure 2-34 Network Connections Tab

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:

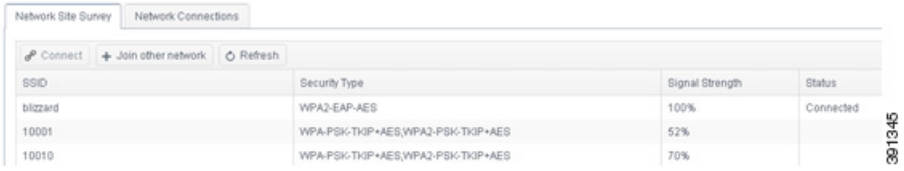
Step 1 Select a wireless network in the Network Site Survey tab or select a network connection in the Network Connections tab.

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



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

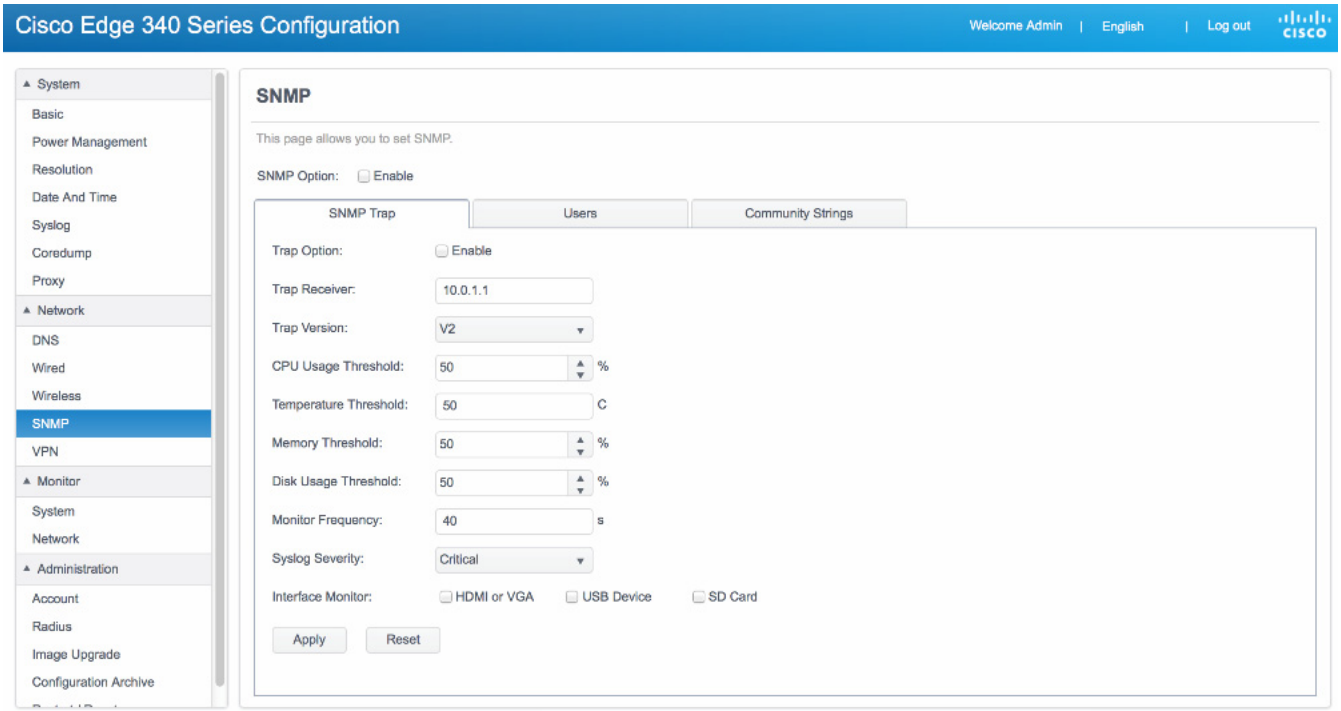
To disable the wireless function, choose **Wi-Fi off** from the **Wi-Fi Operating Mode** drop-down list in the Wireless tab.

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



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.

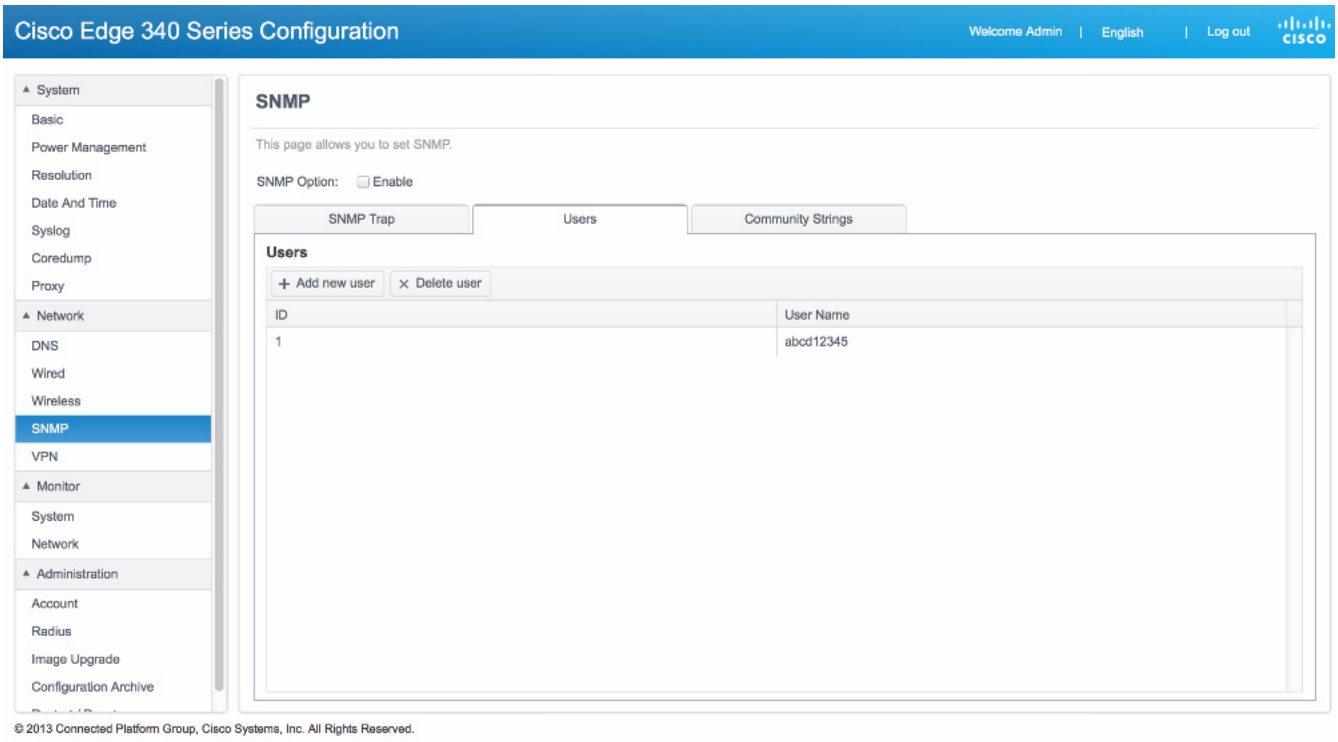
Note The SNMP trap configuration change will cause SNMP service to restart for changes to take effect.

Adding an SNMP User

To add an SNMP user, follow these steps:

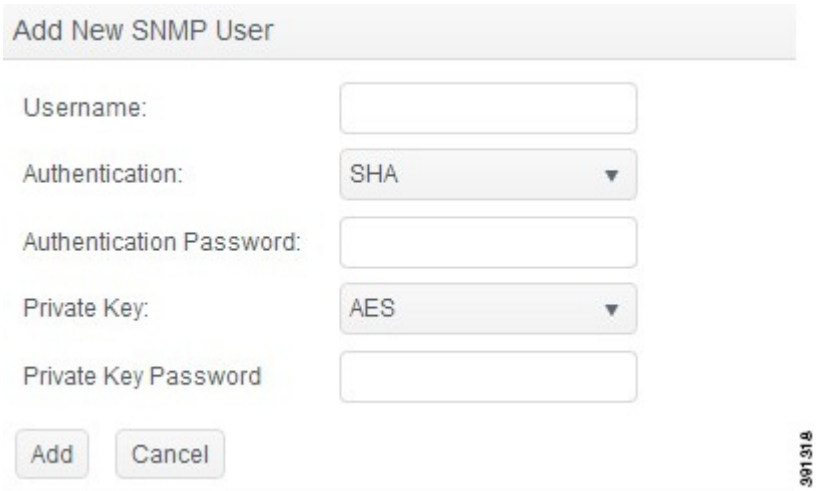
Step 1 Click the Users tab in Figure 2-37 and then click **Add new user**, as shown in Figure 2-38.

Figure 2-38 Configuring SNMP Users



Step 2 The Add snmp user screen is displayed, as shown in Figure 2-39.

Figure 2-39 Adding SNMP User



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.

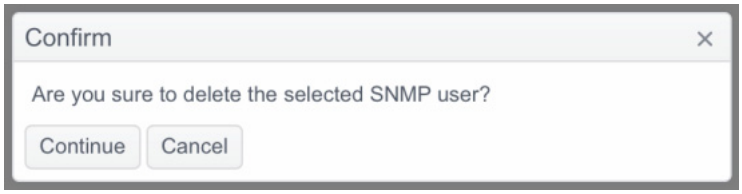
Delete an SNMP User

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 dispayed, 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.

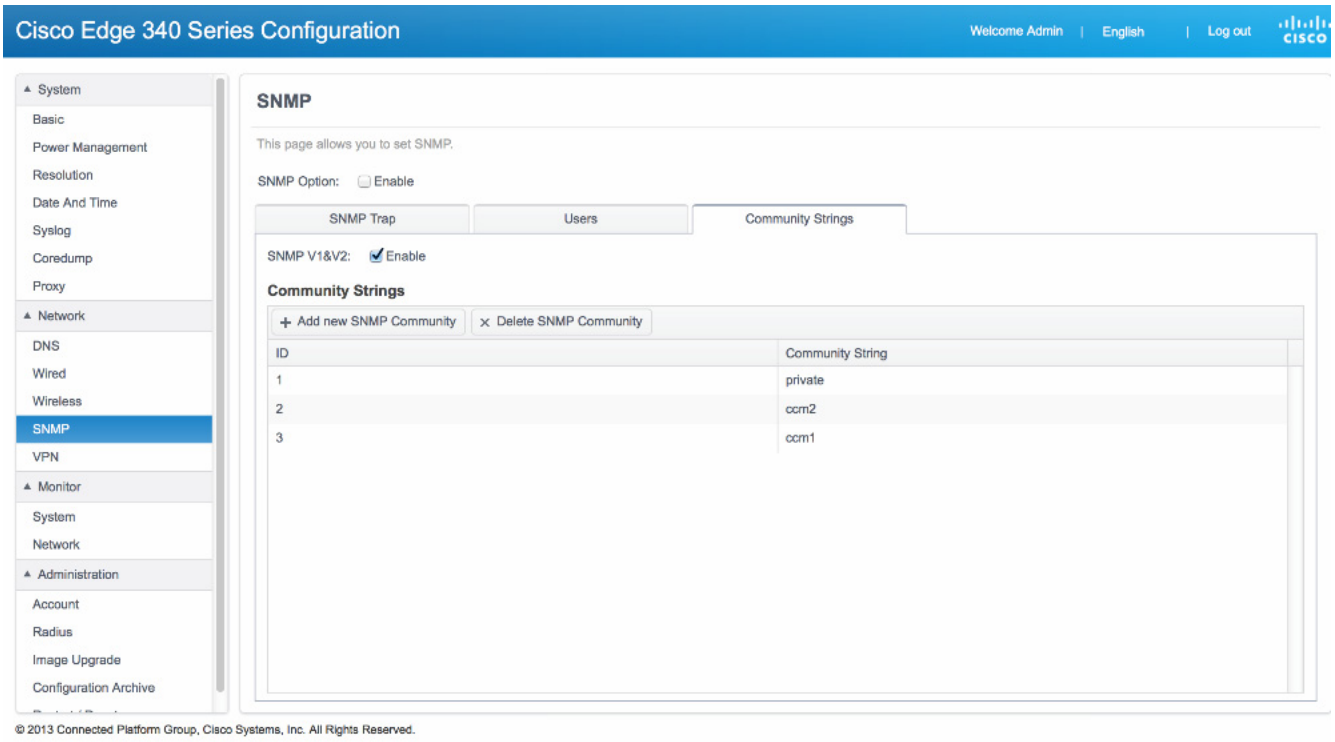
Changing User Password

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



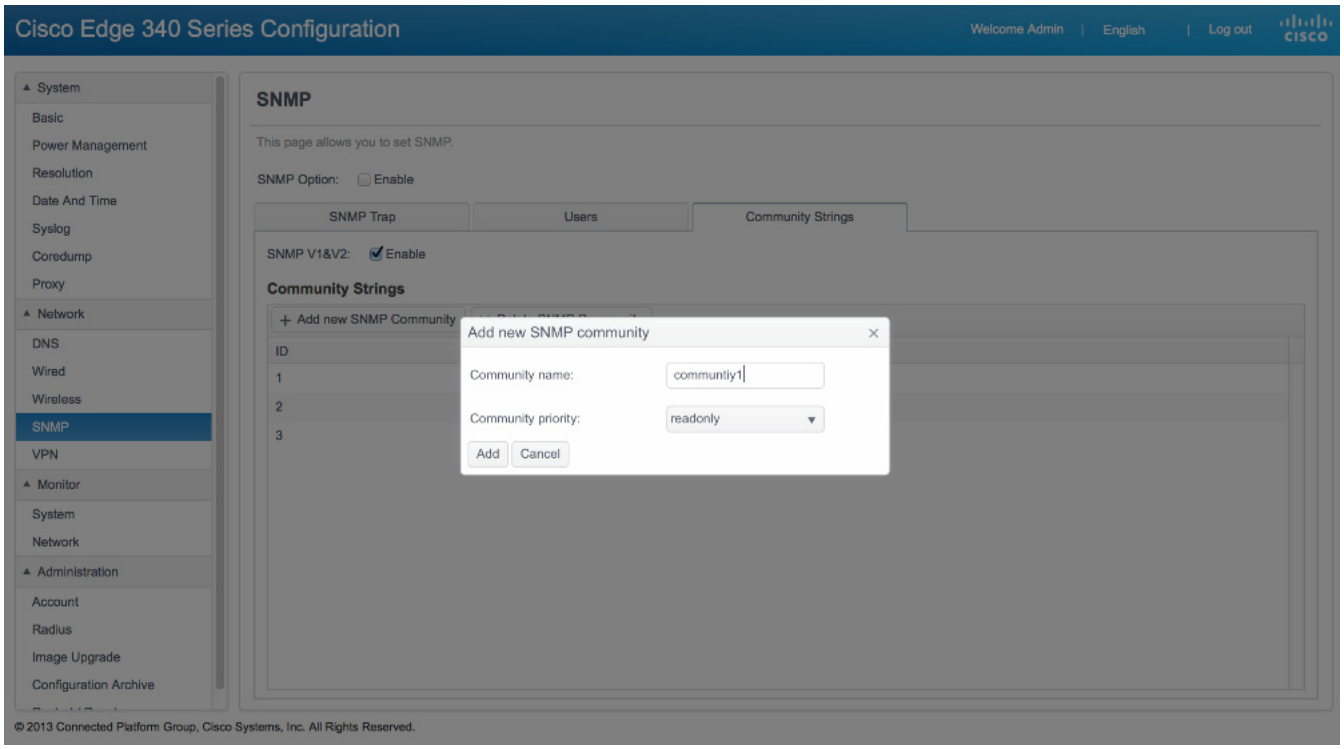
Adding Community Strings

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.

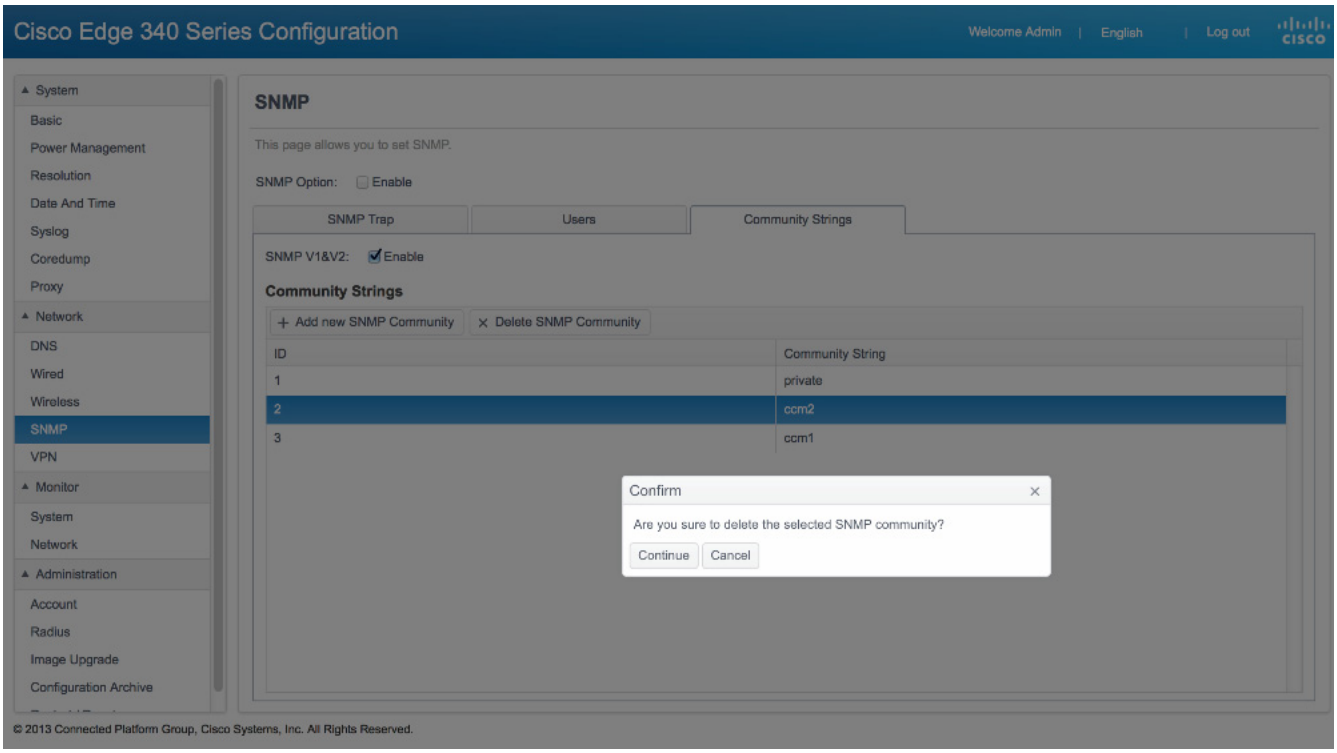
Deleting an SNMP Community String

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



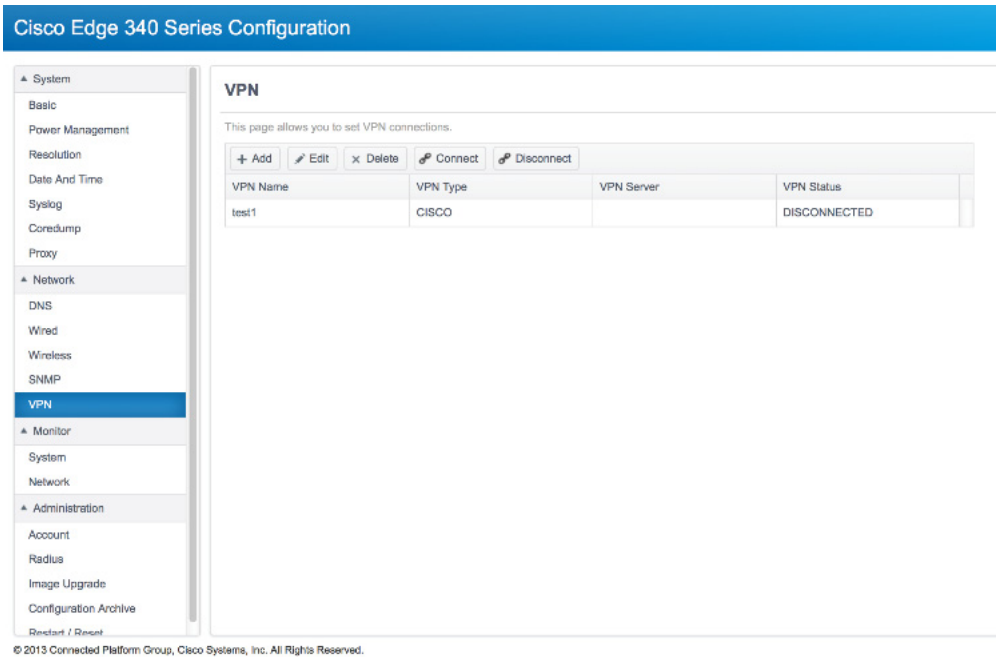
Configuring VPN

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



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

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.

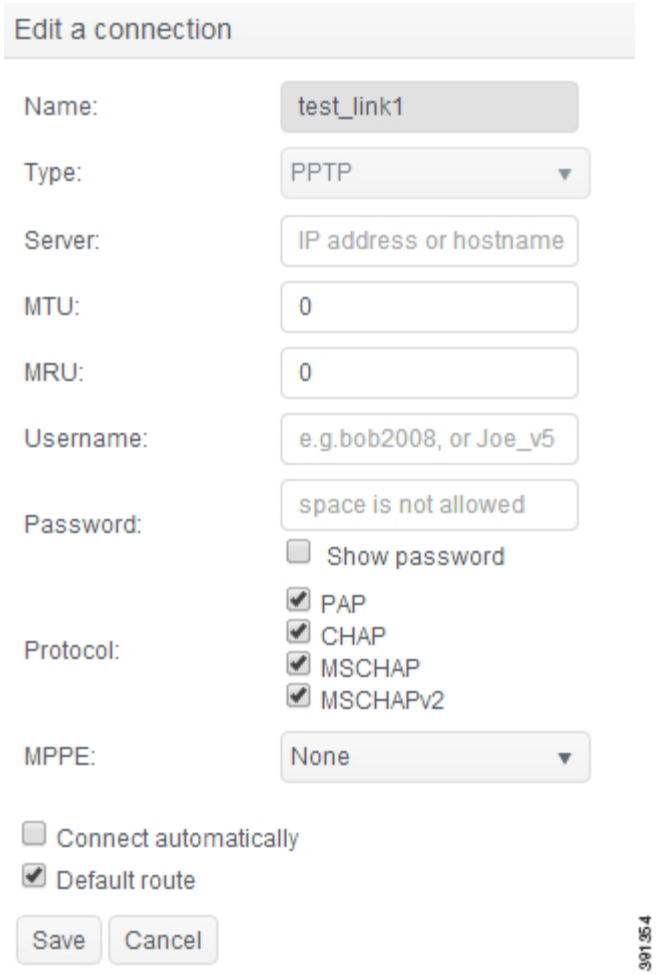
Editing a VPN connection of PPTP Type

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



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.

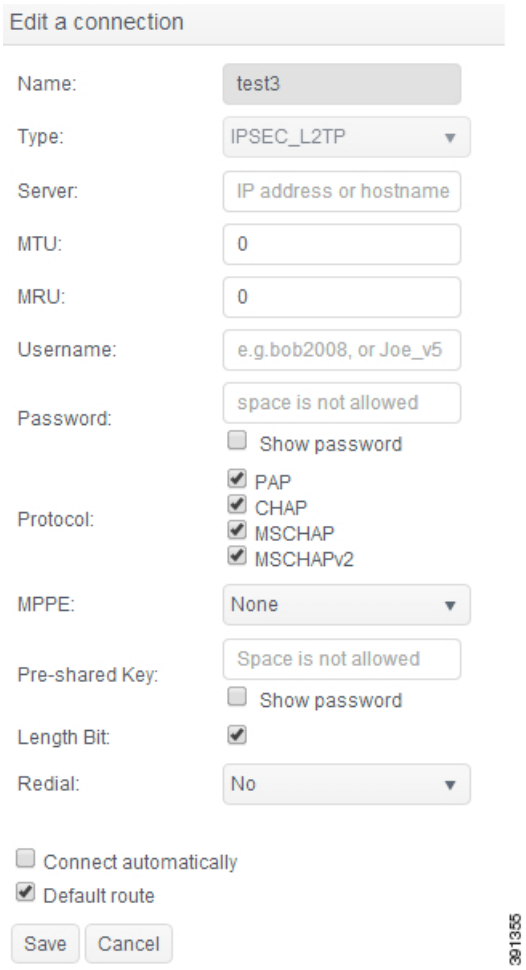
Editing a VPN connection of IPSEC/L2TP/PSK Type

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



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

- 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.

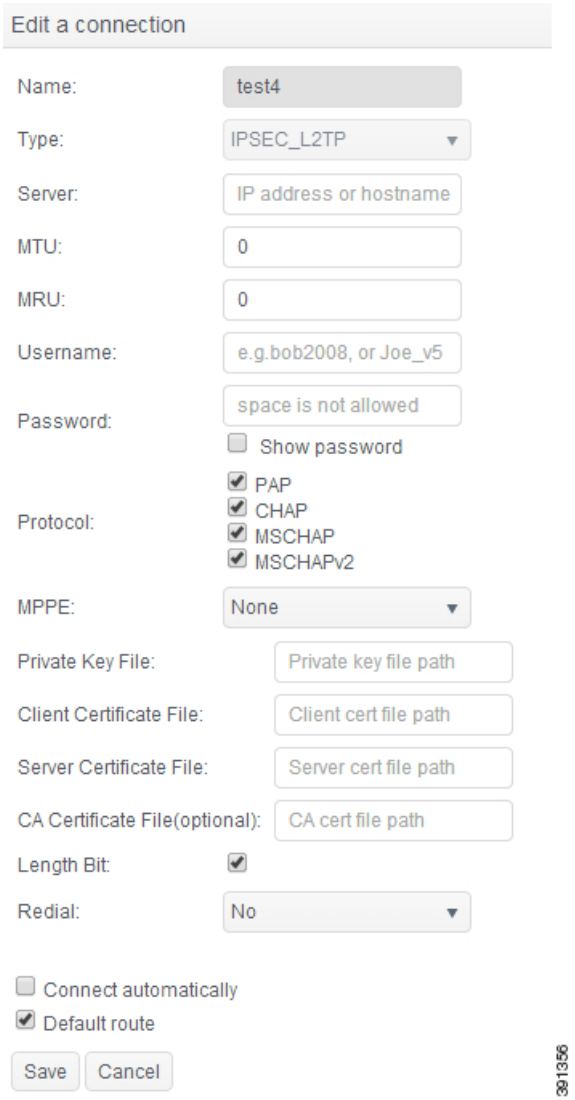
Editing a VPN connection of IPSEC/L2TP/RSA Type

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



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.

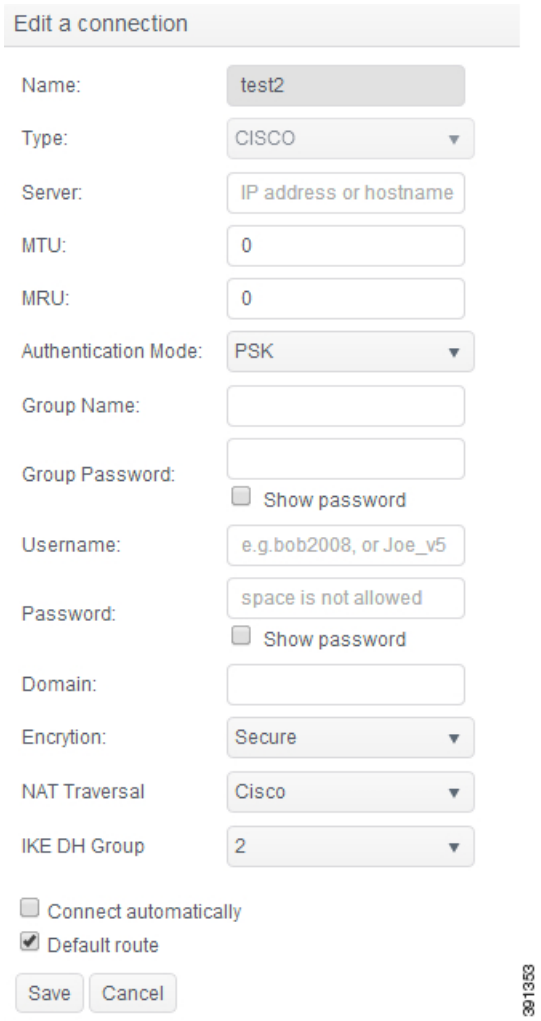
Editing a VPN connection of CISCO Type

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



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.

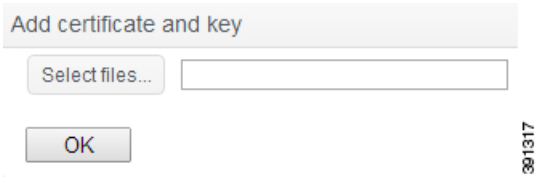
Step 5 (Optional) Enter the value of the MTU and the MRU.

Step 6 Select PSK or Hybrid from the Authentication Mode drop-down list.

a. If you choose PSK, enter the group password.

b. 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.

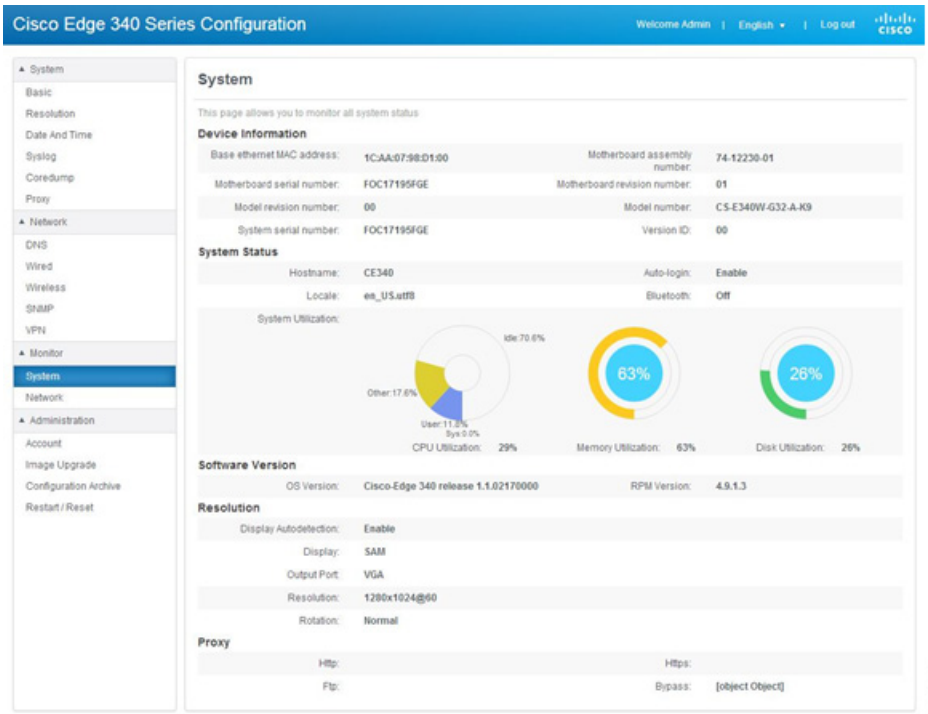
Monitoring the System

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.

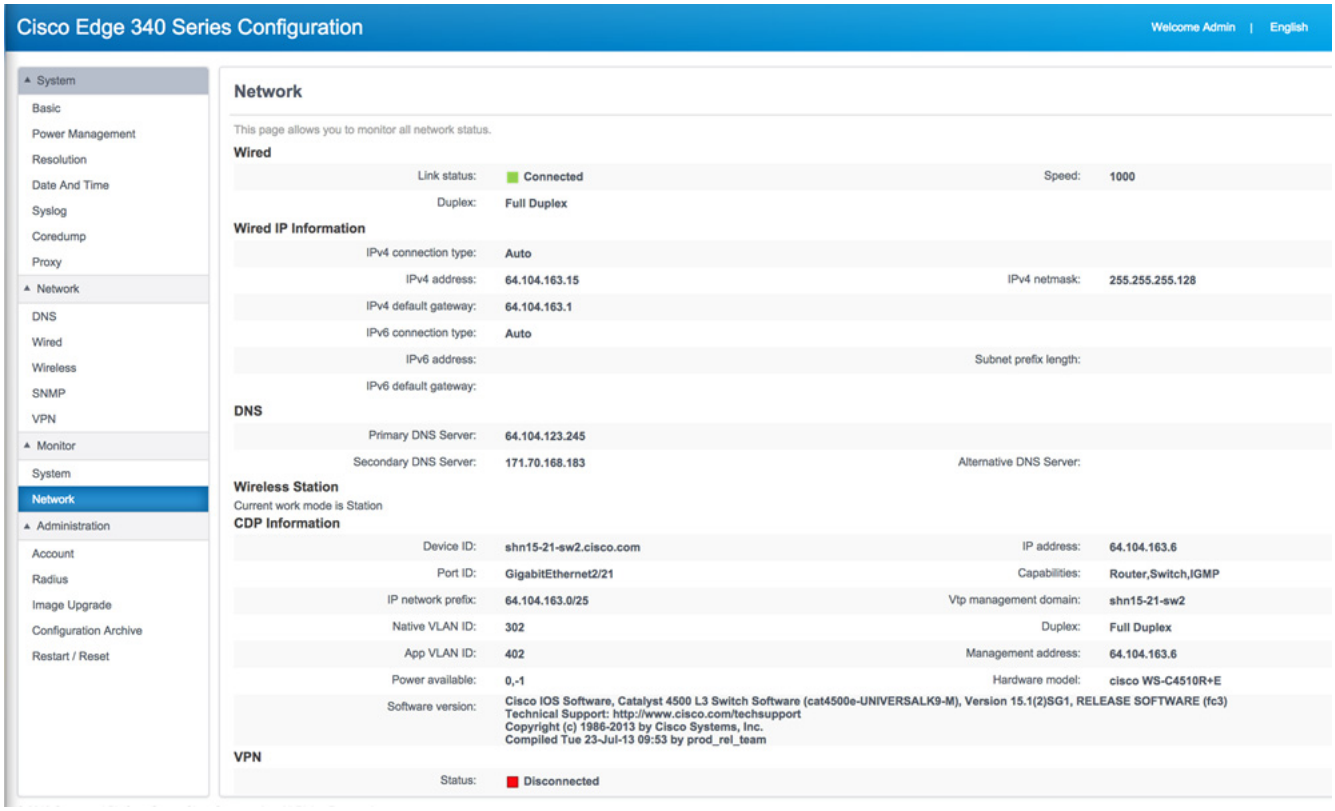
Figure 2-52 System Information



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 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:

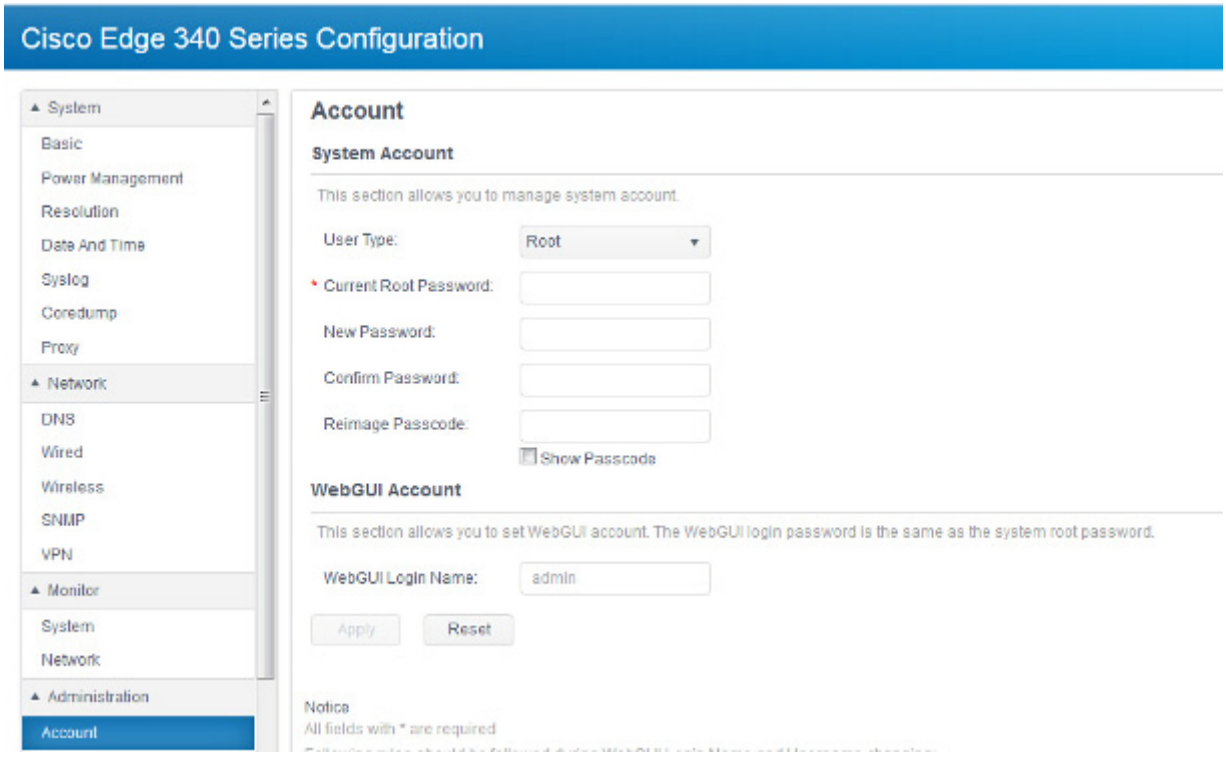
- Configuring System Account Information, page 2-47
- Configuring System Account Reimage Passcode, page 2-48
- Configuring Web GUI Account Information, page 2-48

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



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.

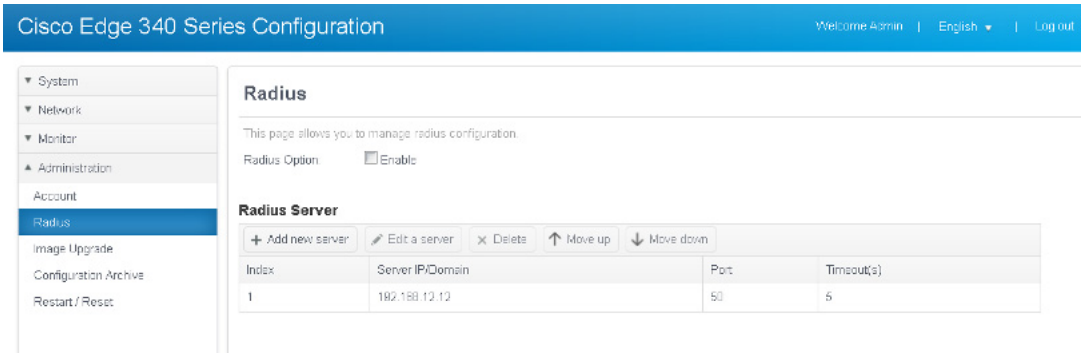
Note Follow these rules when you change the Web GUI login name:
The Web GUI login name should start with alphabet, digit, '.' or '_'.
Other letters in the Web GUI login name could be alphabet, digit, '_', '.' or '-'.
The Web GUI login name should be less than 32 letters.

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



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

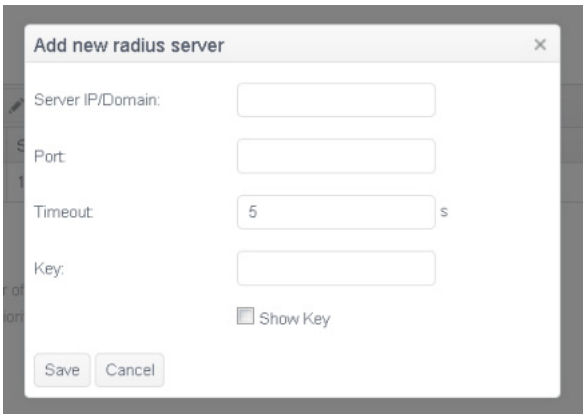
Adding Radius Server

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.

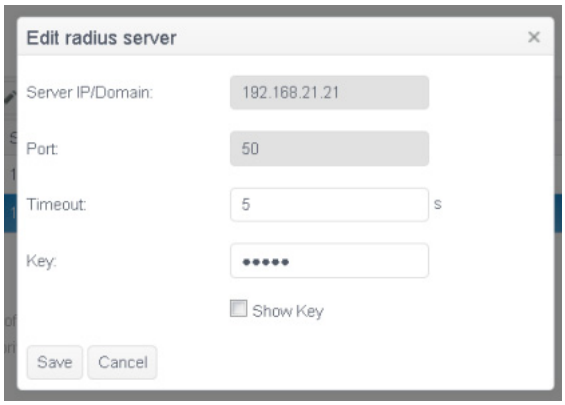
Editing Radius Server

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.

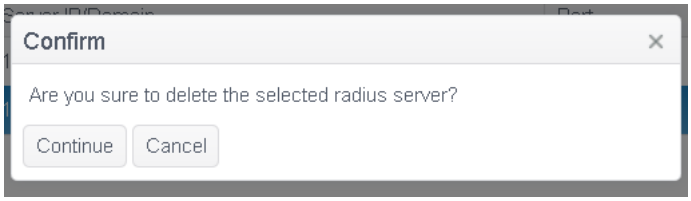
Deleting Radius Server

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:

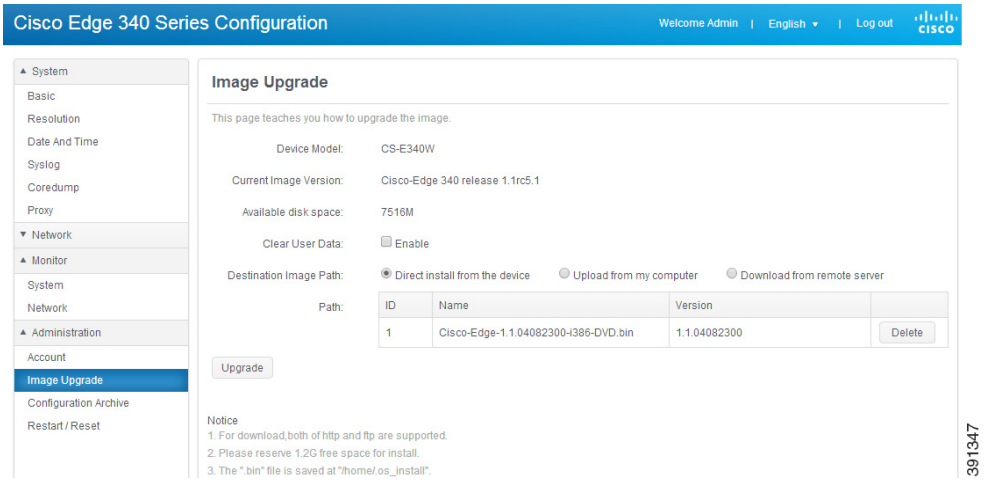
Step 1 Select the radius server that you want to change priority in Figure 2-55.

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

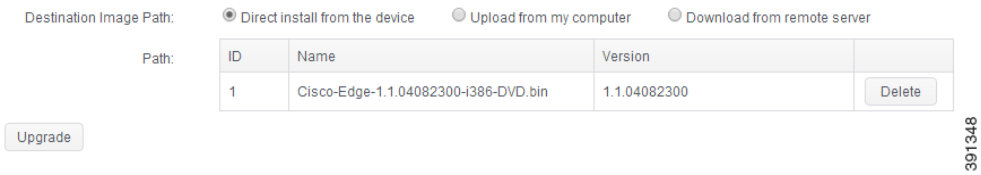
Upgrade From the Device Locally

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

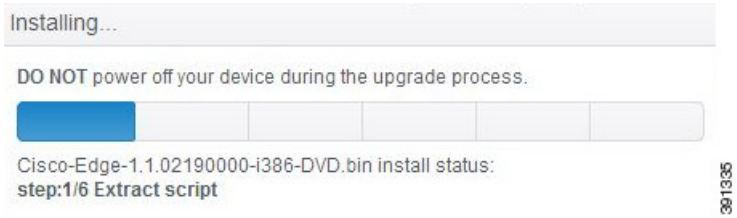


Step 3 In the Path section, click a row to select the image from the table. If there is no image file on the device, upload or download one. The image files on the device can be removed by clicking **Delete** from the table.

Step 4 Click **Upgrade**. In the popup window, click **Continue** to install the selected image.

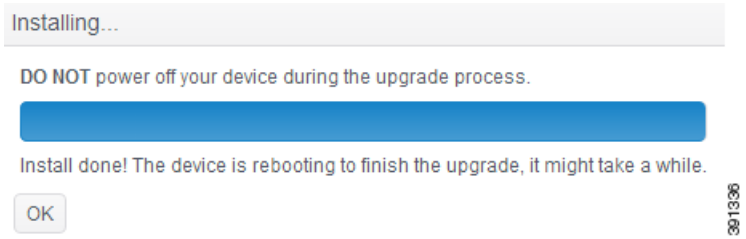
Step 5 If no error happens in the installation preparing stage, a window as shown in Figure 2-62 will show up to demonstrate the installation progress; otherwise, related error message will be printed under the progress bar.

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.

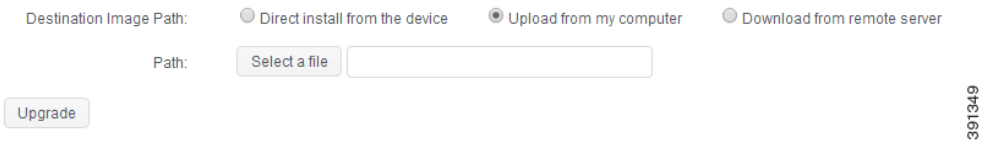
Upgrade by Uploading the Image File From My Computer

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.

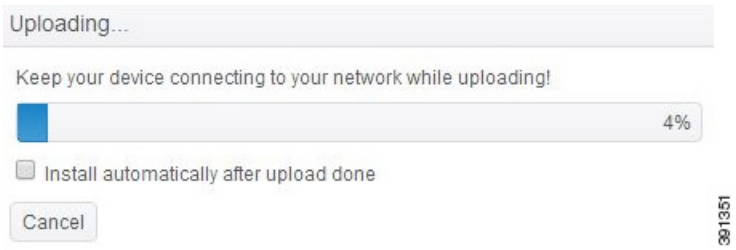
Figure 2-64 Image Upgrade by Uploading the Image From My Computer



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.

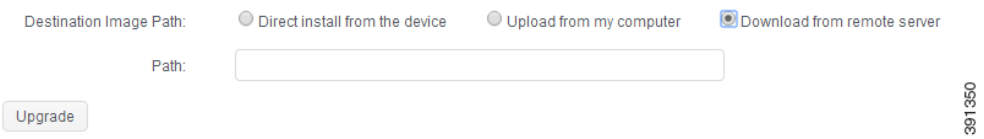
Upgrade by Downloading the Image File From a Remote Server

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.

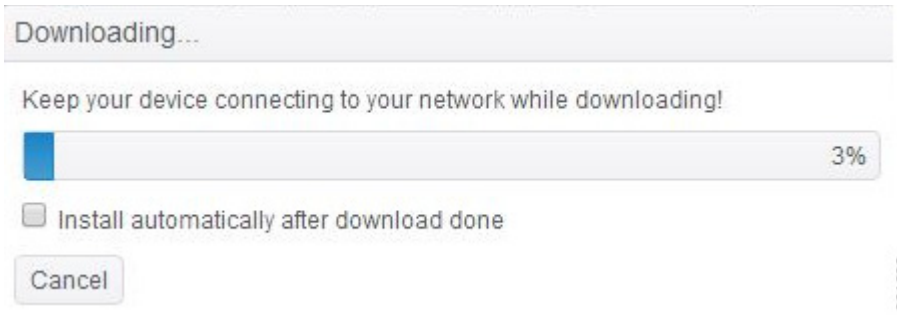
Figure 2-66 Image Upgrade by Downloading the Image From a Remote Server



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

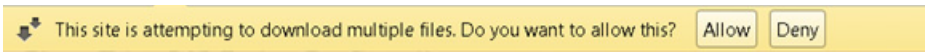
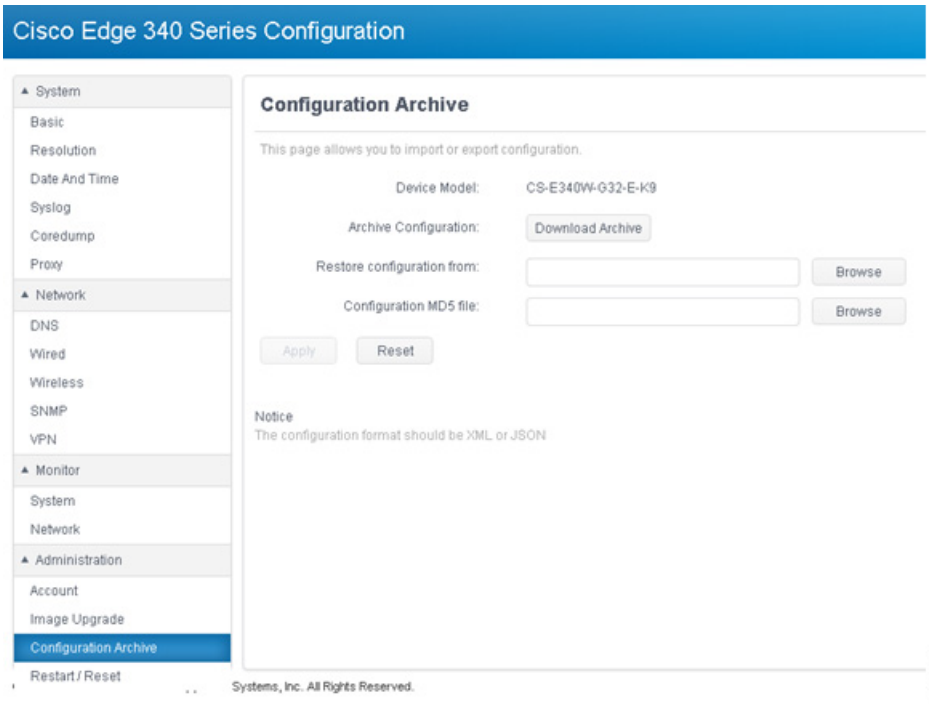


Figure 2-69 Configuration Archive Information



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.**

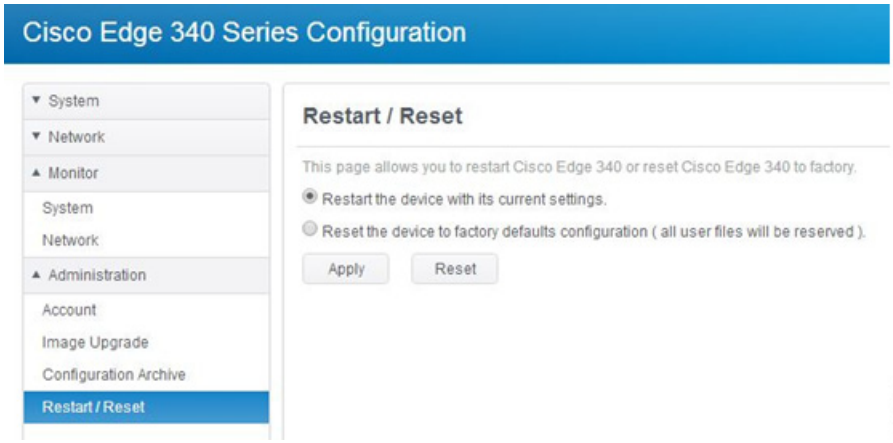
Step 7 Reboot the Cisco Edge 340 Series device.

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.