System Configuration

This chapter describes how to configure the global system settings and perform diagnostics. It contains the following topics:

- LAN, on page 1
- Time, on page 7
- Notification, on page 9
- User Accounts, on page 13
- Management, on page 15
- Security, on page 23

LAN

This section describes the process to configure the port, VLAN, LLDP, IPv4, and IPv6 settings on the WAP device.

IPv4 Configuration

Use the **IPv4 Configuration** section to configure the IPv4 address.

Step 1 Select **LAN > IPv4 Configuration**.

Step 2 Configure the following IPv4 settings:

- **Connection Type**—By default, the DHCP client on the WAP device automatically broadcasts the requests for network information. If you want to use a static IP address, you must disable the DHCP client and manually configure the IP address and other network information.

  Choose one of the following options:

  - **DHCP**—The WAP device acquires its IP address from a DHCP server on the LAN.
  - **Static IP**—Manually configure the IPv4 address. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.168.1.100).

- **Static IP Address, Subnet Mask,** and **Default Gateway**—Enter the static IP address, subnet mask and default gateway.

- **Domain Name Servers** — Select one of the following options:
  - **Dynamic** — The WAP device acquires the DNS server addresses from a DHCP server on the LAN.
  - **Manual** — Enter up to two IP addresses in the fields provided.

Step 3 Click **Apply** to save the changes.

DHCP Auto Configuration Settings

- **DHCP Auto Configuration Options**— This option is enabled by default. When AP comes up with factory defaults, it first tries to auto configure using DHCP options.

  During Auto Configuration:

  - AP boots up with only Ethernet interface enabled and WLAN interfaces down.
  - No services are available to User (except User Interfaces).
  - DHCP Auto Configuration Options is disabled automatically after Wait Interval or TFTP upload of Configuration file whichever is earlier.
  - Disabling the DHCP client (i.e., configure use a static IP address) or disabling DHCP Auto Configuration Options immediately aborts Auto configuration.

  DHCP client automatically broadcasts requests for DHCP options 66 and 67. If DHCP and DHCP Auto Configuration Options are enabled, Access Point is Auto configured during next reboot considering the information received from DHCP Server for DHCP requests.

Note Configuration upload operation by User/Cisco overrides the Auto Configuration so that the chosen configuration file is given preference. In any other cases of rebooting the AP such as firmware upgrade or reboot operations, existing Auto Configuration settings will be effective.

- **TFTP Server IPv4 Address/Host Name**—If you configure TFTP server address, it is used in case of failure to retrieve file from other TFTP Servers specified by DHCP server during Auto Configuration. Enter IPv4 address or hostname information. If it happens to be in hostname format DNS server must be available to translate hostname into IP address.

The value is used during the Auto Configuration procedure during next boot-up.

- **Configuration File Name**—If you specify the configuration file name, it is retrieved from TFTP Server during Auto Configuration of AP, in case the boot file name is not received from DHCP server. Absence of this value indicates config.xml to be used. The file must have an xml extension if specified.

The value is used during the Auto Configuration procedure during next boot-up.

- **Wait Interval**—If configured, Access Point comes up with the local configuration and makes enabled services available to the user, after the wait interval. Access point aborts Auto configuration if TFTP transaction is not initiated within this interval specified. The default value is 3 minutes.

The value is used during the Auto Configuration procedure during next boot-up.

- **Status Log**—This field displays reason of Auto Configuration completion or abort.

IPv6 Configuration

Use the **IPv6 Configuration** section to configure the IPv6 address by performing the following steps:

Step 1 Select **LAN > IPv6 Configuration**.

Step 2 Configure the following parameters:

- **IPv6 Connection Type** — Select one of the following options:
  - **DHCPv6** — The IPv6 address is assigned by a DHCPv6 server.
  - **Static IPv6** — Manually configure the IPv6 address. The IPv6 address should be in a form similar to xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8:CAD5:7D91).
- **IPv6 Administrative Mode** — Check **Enable** to enable IPv6 administrative mode.
- **IPv6 Auto Configuration Administrative Mode** — Check **Enable** to enable the IPv6 automatic address configuration.

  When the IPv6 automatic address configuration is enabled, the WAP device recognizes its IPv6 addresses and gateway by processing the router advertisements received on the LAN port. The WAP device can have multiple auto-configured IPv6 addresses.
- **Static IPv6 Address** — Enter the static IPv6 address. The WAP device can have a static IPv6 address even if addresses have already been configured automatically.
- **Static IPv6 Address Prefix Length** — Enter the prefix length of the static address, which is an integer in the range of 0 to 128. The default is 0.
- **Static IPv6 Address Status** — It can be one of the following status:
  - **Operational** — The IP address has been verified as unique and is usable on the LAN interface.
  - **Tentative** — The WAP device automatically initiates a duplicate address detection (DAD) process when a static IP address is assigned. This IPv6 address is tentative as it is being verified on the network and cannot be used to transmit or receive traffic.
  - **Blank (no value)** — No IP address is assigned.
- **IPv6 Autoconfigured Global Addresses** — Lists the IPv6 addresses which have been automatically assigned to the device.
- **IPv6 Link Local Address** — The IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.
- **Default IPv6 Gateway** —The statically configured default IPv6 gateway.
- **IPv6 Domain Name Servers** — Select one of the following options:
  - **Dynamic** — The DNS servers are recognized dynamically through the DHCPv6.

- **Manual** — To manually specify up to two IPv6 DNS servers.

Port Settings

Use the **Port Settings Table** to view and configure the settings for the port that connects the WAP device to a LAN.

Step 1 Select **LAN** > **More** > **Port Settings Table**.

The **Port Settings Table** includes the following status and configurations for the LAN interface:

- **Link Status** — Displays the current port link status.
- **Port Speed** — When in review mode, it lists the current port speed. When in edit mode, and the Auto Negotiation is disabled, select a port speed such as 100 Mbps or 10 Mbps. The 1000 Mbps speed is the only supported when Auto-Negotiation is enabled.
- **Duplex Mode** —When in review mode, it lists the current port duplex mode. When in edit mode, and the Auto Negotiation is disabled, select either **Half** or **Full** duplex mode.
- **Auto Negotiation** — When enabled, the port negotiates with its link partner to set the fastest link speed and duplex mode available. When disabled, you can manually configure the Port Speed and Duplex Mode.
- **Green Ethernet** — Green Ethernet Mode supports both the auto-power-down mode and the EEE (Energy Efficient Ethernet, IEEE 802.3az) mode. The Green Ethernet Mode works only when the auto-negotiation on the port is enabled. The auto-power-down mode reduces the chip power when the signal from a link partner is not present. The WAP device automatically enters into a low-power mode when energy on the line is lost, and it resumes normal operation when energy is detected. The EEE mode supports QUIET times during low link utilization, allowing both sides of a link to disable portions of each PHY's operating circuit and save power.

Step 2 **Jumbo Frames (For WAP361 Only)** — When enabled, the port supports packet length of up to 9720 bytes. Otherwise, the port supports packet length up to 2000 bytes. The Jumbo Frame is supported only when link speed is in 1000 Mbps mode. Since the wireless interface does not support Jumbo Frames, it only works to forward packets between Ethernet (LAN0 to LAN4) ports. For this reason, it is recommended to disable it.

Step 3 **CoS (port VLAN priority, 802.1p Class of Service, For WAP361 Only)**—Assigns the 802.1p class of service (CoS) when the port receives an untagged packet.

Step 4 Click **Apply**.

Spanning Tree Protocol

In the **Spanning Tree Protocol** mode, the **Enable** checkbox is checked by default to enable the STP mode on the Cisco WAP device. When enabled, STP helps prevent switching loops. STP is recommended if you configure the WDS links.

Step 1 Select **LAN** > **Spanning Tree Protocol**.

Step 2 Check the **Enable** checkbox to enable Spanning Tree.

Step 3 Click **Spanning Tree Settings** to configure the spanning tree protocol for each port.

- **Flood BPDU if STP is disabled on port(s)**—Check to flood the BPDU packets received from the port(s) whose STP status is disabled, or uncheck to drop the BPDU packets received from the port(s) whose STP status is disabled.
- **LAN0 ~4/WDS0 ~3**—Check to enable STP on a port, or uncheck to disable STP on a port.

VLANs Setting

Use the VLAN Configuration page to view and configure the VLANs settings.

Step 1 Select **LAN > More > VLANs Setting Table**.

Step 2 Configure these parameters:

- **Untagged VLAN ID** — Specifies a number between 1 and 4094 for the untagged VLAN ID. The default is 1. The traffic on the VLAN that you specify in this field is not be tagged with a VLAN ID when forwarded to the network.
- **Description** — Description of the related VLAN.
- **Management VLAN** — The Management VLAN is the VLAN used to access the WAP device through Telnet or the web GUI. There must be only one VLAN as the management VLAN. If no interface (wired or wireless) is assigned to the Management VLAN, there will be no interface that a user can use to access the configuration utility.
- **VLAN** — Select from the drop-down list (**Untagged or Tagged**) VLAN.

  By default, all traffic on the WAP device uses the VLAN 1, the default untagged VLAN. This means that all traffic is untagged until you disable the untagged VLAN, change the untagged traffic VLAN ID, or change the VLAN ID for a VAP or client using RADIUS.

Step 3 Click **Apply**. The changes are saved to the Startup Configuration.

Neighbor Discover

Bonjour enables the WAP device and its services to be discovered by using multicast DNS (mDNS). Bonjour advertises services to the network and answers queries for the service types that it supports, simplifying network configuration in your environments.

The WAP device advertises these service types:

- **Cisco-specific device description (csco-sb)** — This service enables clients to discover the Cisco WAP devices and other products deployed in your networks.
- **Management user interfaces** — This service identifies the management interfaces available on the WAP device (HTTP and SNMP).

When a Bonjour-enabled WAP device is attached to a network, any Bonjour client can discover and get access to the configuration utility without prior configuration.

A system administrator can use an installed Internet browser plug-in to discover the WAP device. The web-based Configuration Utility shows up as a tab in the browser.

Note The system administrator can view the Bonjour enabled WAP's using the latest Internet Explorer plug-in (Cisco Business Dashboard tool). All WAP devices present in a cluster, are shown under the cluster name after the Bonjour discovery process. The administrator should ensure that the name of the cluster is unique within a network.

Bonjour works in both IPv4 and IPv6.

To enable the WAP device to be discovered through Bonjour, follow these steps:

Step 1 Select **LAN** > **More** > **Neighbor Discover**.

Step 2 Check **Enable** to enable Bonjour. By default, this option is enabled.

Step 3 Click **Apply**. The changes are saved to the Startup Configuration.

LLDP

The Link Layer Discovery Protocol (LLDP) is defined by the IEEE 802.1AB standard and allows the UAP to advertise its system name, system capabilities, and power requirements. This information can help to identify system topology and detect bad configurations on the LAN. The AP also supports the Link Layer Discovery Protocol for the Media Endpoint Devices (LLDP-MED), which standardizes additional information elements that devices can pass to each other to improve network management.

Step 1 To configure the LLDP settings, select **LAN** > **More** > **LLDP**.

Step 2 Configure the following parameters:

- **LLDP Mode** — Check **Enable** to enable the LLDP. Once enabled, the AP transmits LLDP Protocol Data Units to the neighbor devices. By default, this mode is enabled.
- **TX Interval** — The number of seconds between each LLDP message transmissions. The valid range is 5 to 32768 seconds. The default value is 30 seconds.
- **POE Priority** — Select the priority level from the drop-down list (**Critical, High, Low or Unknown**). The PoE priority helps the Power Sourcing Equipment (PSE), determine which powered devices should be given priority in power allocation when the PSE doesn't have enough capacity to supply power to all connected devices.

Step 3 Click **Apply**.

IPv6 Tunnel

The WAP device supports the Intra-Site Automatic Tunnel Addressing Protocol (ISATAP). The ISATAP enables the WAP device to transmit IPv6 packets encapsulated within the IPv4 packets over the LAN. The

protocol enables the WAP device to communicate with remote IPv6-capable hosts even when the LAN that connects them does not support the IPv6.

The WAP device acts as an ISATAP client. An ISATAP-enabled host or router must reside on the LAN. The IP address or host name of the router is configured on the WAP device (by default, it is ISATAP). If configured as a host name, the WAP device communicates with a DNS server to resolve the name into one or more ISATAP router addresses. The WAP device then sends solicit messages to the routers. When an ISATAP-enabled router replies with an advertisement message, the WAP device and the router establish the tunnel. The tunnel interface is assigned a link-local and a global IPv6 address, which serve as virtual IPv6 interfaces on the IPv4 network.

When IPv6 hosts initiate the communication with the WAP device connected through the ISATAP router, the IPv6 packets are encapsulated into IPv4 packets by the ISATAP router.

1. **ISATAP Status** — Check **Enable** to enable ISATAP on the device. By default, this option is enabled.
2. **ISATAP Capable Host** — Enter the IP address or DNS name of the ISATAP router. The default value is isatap.
3. **ISATAP Query Interval** — Enter how often the WAP device should send queries to the DNS server to attempt to resolve the ISATAP host name into an IP address. The valid range is 120 to 3600 seconds. The default value is 120 seconds.
4. **ISATAP Solicitation Interval** — Enter how often the WAP device should send the router solicitation messages to the ISATAP routers. The WAP device sends the router solicitation messages only when there is no active ISATAP router. The valid range is 120 to 3600 seconds. The default value is 120 seconds.
5. **ISATAP IPv6 Link Local Address**— The IPv6 address used by the local physical link. The link local address is not configurable and is assigned by using the IPv6 Neighbor Discovery process.
6. **ISATAP IPv6 Global Address**— If the WAP device has been assigned one or more IPv6 addresses automatically, the addresses are listed.

Note When the tunnel is established, the ISATAP IPv6 Link Local Address and ISATAP IPv6 Global Address fields appear on the page. These are the virtual IPv6 interface addresses.

7. Click **Apply**.

Time

A system clock provides a network-synchronized time-stamping service for the message logs. The system clock can be configured manually or as a Network Time Protocol (NTP) client that obtains the clock data from a server.

Use the Time Settings page to configure the system time manually or from a preconfigured NTP server. By default, the WAP device is configured to obtain its time from a predefined list of NTP servers.

The current system time appears at the top of the page, along with the **System Clock Source** option.

Automatically Acquiring the Time Settings through NTP

To automatically acquire the time settings from a NTP server, follow these steps:

Step 1 Select **System Configuration** > **Time**.

Step 2 In the **System Clock Source** area, click **Network Time Protocol (NTP)**. By default, the NTP is enabled.

Step 3 Configure the following parameters:

- **NTP Server (1 through 4)** — Specify the IPv4 address, IPv6 address, or host name of a NTP server. A default NTP server is listed from **0.ciscosb.pool.ntp.org** to **3.ciscosb.pool.ntp.org**.

  A host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.

- **Time Zone** — Select the time zone for your location.
- **Adjust for Daylight Saving Time** — Ensure that you have chosen the appropriate time zone before you select this option. Check the checkbox to enable and configure the following fields:
  - **Starts** — Select the week, day, month, and time when the Daylight Savings time starts.
  - **Ends** — Select the week, day, month, and time when the Daylight Savings time ends.
  - **Daylight Saving Offset** — Specify the number of minutes to move the clock forward when Daylight Savings Time begins and backward when it ends.

Step 4 Click **Apply**. The changes are saved to the Startup Configuration.

Manually Configuring the Time Settings

To manually configure the time settings:

Step 1 Select **System Configuration** > **Time**.

Step 2 In the System Clock Source area, choose **Manual**.

Step 3 Click **Sync Time with PC** to clone the system time settings from your local PC.

Step 4 You can also configure the following fields:

- **System Date** — Select the current month, day, and year date from the drop-down lists.
- **System Time** — Select the current hour and minutes in 24-hour clock format.
- **Time Zone** — Select the time zone for your location.
- **Adjust for Daylight Saving Time** — Ensure that you have chosen the appropriate time zone before you select this option. Check the checkbox to enable and configure the following fields:
  - **Starts** — Select the week, day, month, and time when daylight savings time starts.
  - **Ends** — Select the week, day, month, and time when daylight savings time ends.

- **Daylight Saving Offset** — Specify the number of minutes to move the clock forward when daylight savings time begins and backward when it ends.

Step 5 Click **Apply**. The changes are saved to the Startup Configuration.

Note Click **Sync Time with PC**, the system time of the device will be same as the PC.

Notification

This section details the process to enable and configure notifications for the access point.

LED Display

The WAP device has two type of LEDs: System LED and Ethernet LED. Use the LED Display page to configure all LEDs.

To configure the LED Display do the following:

Step 1 Select **Notification > LED Display**.

Step 2 Select **Enable** to enable the LEDs. Select **Disable** to disable the LEDs. Select **Associate Scheduler** and go to Step 3.

Step 3 Select a profile name from the drop-down list for the Associate Scheduler LED Display. By default there is no profile associated to the LEDs. The drop-down selection will show the configured Scheduler Profile Names configured in the **Wireless > Scheduler** page.

When the LED is associated to a Scheduler Profile, this column shows the status depending on the presence or absence of an active profile rule at that time of the day.

Step 4 Click **Apply**.

Log Settings

Use the Log Settings page to enable log messages to be saved in permanent memory. You can also send logs to a remote host.

If the system unexpectedly reboots, the log messages can be useful to diagnose the cause. However, log messages are erased when the system reboots unless you enable persistent logging.

⚠

Caution Enabling persistent logging can wear out the flash (nonvolatile) memory and degrade network performance. Only enable persistent logging to debug a problem. Make sure that you disable persistent logging after you finish debugging the problem.

Configuring the Persistent Log

Step 1 Select **Notification** > **Log Settings**.

Step 2 Configure these parameters:

- **Persistence** — Check **Enable** to save the system logs to the nonvolatile memory so that the logs are kept when the WAP device reboots. You can save up to 1000 log messages. When the limit of 1000 is reached, the oldest log message is overwritten by the newest message. Clear this field to save system logs to volatile memory. Logs in volatile memory are deleted when the system reboots.
- **Severity** — Select the severity from the drop-down list (**Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug**) used to filter the event messages that will be saved in the nonvolatile memory. All other messages will be saved in the volatile memory.
- **Depth** — Enter the maximum number of messages, up to 1000, that can be stored in volatile memory. When the number that you configure in this field is reached, the oldest log event is overwritten by the newest log event.

Step 3 Click **Apply**.

Remote Log Server Table

The kernel log is a comprehensive list of system events (shown in the System Log) and kernel messages.

You cannot view the kernel log messages directly from the configuration utility. You must first set up a remote log server to receive and capture the logs. Then, you can configure the WAP device to log to the remote log server. The WAP device supports up to two remote log servers.

The remote log server collection for the syslog messages provides these features:

- Allows aggregation of syslog messages from multiple APs.
- Stores a longer history of messages than is kept on a single WAP device.
- Triggers scripted management operations and alerts.

To specify a host on your network to serve as a remote log server:

Step 1 Select **Notification** > **Log Settings**.

Step 2 In the **Remote Log Server Table**, configure the following parameters:

- **Server IPv4/IPv6 Address/Name** — Enter the IPv4 or IPv6 address, or the host name of the remote log server.

  A host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.
- **Enable** — Check **Enable** to enable the remote log server. Next, define the log severity and UDP port.
- **Log Severity** — Check the severities that an event must have for it to be sent to remote log server.
- **UDP Port** — Enter the logical port number for the syslog process on the remote host. The range is from 1 to 65535. The default port is 514.

Using the default port is recommended. If you reconfigure the log port, make sure that the port number that you assign to syslog is available for use.

Step 3 Click **Apply**. The changes are saved to the Startup Configuration.

Note If you enable a remote log server, clicking **Apply** activates the remote logging. The WAP device sends its kernel messages in real-time for display to the remote log server monitor, a specified kernel log file, or other storage, depending on your configuration.

If you disabled a remote log server, click **Apply** to disable remote logging.

View System Log

The **View System Log** page displays the list of system events occurring on the device. The log is cleared upon a reboot and can be cleared by an administrator. Up to 1000 events can be shown. Older entries are removed from the list as needed to make room for new events.

To view the system logs, select **Notification > View System Log**.

The following information is displayed:

- **Time Stamp** — The system time when the event occurred.
- **Severity** — The severity level of the event.
- **Service** — The service associated with the event.
- **Description** — A description of the event.

You can filter or rearrange the settings on View System Log.

Click **Refresh** to refresh the screen and show the most current information.

Click **Clear All** to clear all entries from the log.

Click **Download** to download all entries from the log.

Email Alert/ Mail Server/ Message Configuration

The email alert feature supports mail server configuration, message severity configuration, and up to three email addresses to send urgent and non-urgent email alerts. Use the **Email Alert** to send messages to the configured email addresses when particular system events occur.

Tip Do not use your personal email address. This would unnecessarily expose your personal email login credentials. Use a separate email account instead. Also, be aware that many email accounts keep a copy of all sent messages by default. Anyone with access to this email account has access to the sent messages. Review the email settings to ensure that they conform to your privacy policy.

To configure the WAP device to send email alerts, perform the following steps:

Step 1 Select **Notification** > **Email Alert**.

Step 2 In the **Email Alert** area, configure the following parameters:

- **Administrative Mode** — Check **Enable** to enable the email alert feature.
- **From Email Address** — Enter the email address to be displayed as the sender of the email. The address is a 255-character string with only printable characters. No address is configured by default.
- **Log Duration** — Enter the frequency in minutes at which scheduled messages are sent. The range is from 30 to 1440 minutes. The default is 30 minutes.
- **Scheduled Message Severity** — Select the severity from the drop-down list (**Emergency, Alert, Critical, Error, Warning, Notice, Info** or **debug**) that an event must have for it to be sent to the configuration email address at the frequency specified by the Log Duration. The default severity is **Warning**.
- **Urgent Message Severity** — Select the severity from the drop-down list (**Emergency, Alert, Critical, Error, Warning, Notice, Info or debug**) that an event must have for it to be sent to the configured email address immediately. The default severity is **Alert**.

Step 3 In the **Mail Server Configuration** area, configure these parameters:

- **Server IPv4 Address/Name** — Enter the IP address or host name of the outgoing SMTP server. The server address must be a valid IPv4 address or host name. The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10).

  A host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.
- **Data Encryption** — Choose the mode of security from the drop-down list (**Open or TLSv1**) for the outbound email alert. Using the secure TLSv1 protocol can prevent eavesdropping and tampering during the communication across the public network.
- **Port** — Enter the SMTP port number to use for outbound emails. The range is a valid port number from 0 to 65535. The default port is 465.
- **Username** — Enter the user name for the email account that will be used to send these emails. Typically (but not always) the user name is the full email address including the domain (such as Name@example.com). The specified account will be used as the email address of the sender. The user name can contain in the range of 1 to 64 alphanumeric characters that includes "**@**", "**-**", and "**.**" .
- **Password** — Enter the password for the email account that will be used to send these emails. The password can be from 1 to 64 characters.

Step 4 In the **Message Configuration** area, configure the email addresses and subject line:

- **To Email Address 1/2/3** — Enter up to three addresses to receive the email alerts. Each email address must be a valid address.
- **Email Subject** — Enter the text to appear in the email subject line. This can be up to a 255-character alphanumeric string.

Step 5 Click **Apply**.

Email Alert Examples

The following example shows how to fill in the **Mail Server Configuration** parameters:

```
Gmail
Server IPv4 Address/Name = smtp.gmail.com
Data Encryption = TLSv1
Port = 465
Username = Your full email address you can use to login to your email account
associated with the above server
Password = xxxxxxxx is a valid password of your valid email account
To Email Address 1 = myemail@gmail.com

Windows Live Hotmail
Windows Live Hotmail recommends the following settings: Data Encryption: TLSv1
SMTP Server: smtp.live.com
SMTP Port: 587
Username: Your full email address, such as myName@hotmail.com or
myName@myDomain.com
Password: Your Windows Live account password

Yahoo! Mail
Yahoo requires using a paid account for this type of service. Yahoo
recommends the following settings:
Data Encryption: TLSv1
SMTP Server: plus.smtp.mail.yahoo.com
SMTP Port: 465 or 587
Username: Your email address, without the domain name such as myName (without
@yahoo.com)
Password: Your Yahoo account password
```

The following example shows a sample format of a general log email.

```
From: AP-192.168.2.10@mailserver.com
Sent: Wednesday, September 09, 2009 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP

TIME          Priority > Process Id > > > Message
Sep 8 03:48:25 info >> login[1457]> > > root login on ttyp0
Sep 8 03:48:26 info >> mini_http-ssl[1175]>Max concurrent connections of 20
reached
```

User Accounts

One management user is configured on the WAP device by default:

- User Name: **cisco**
- Password: **cisco**

Use the **User Accounts** page to configure up to four additional users and change the user password.

Adding a User

Configure the following settings to add a new user:

Step 1 Select **System Configuration > User Accounts**.

The **User Account Table** shows the currently configured users. The user cisco is preconfigured in the system and has Read/Write privileges.

All other users can have Read Only access, but not Read/Write access.

Step 2 Click ✚ to add a new row.

Step 3 Check the checkbox for a new user and enter a name for the new user.

Step 4 Enter a new password between 0 and 127 characters and confirm the same password in the appropriate fields.

The **Password Strength Meter** field indicates the password strength as follows:

- **Red** — The password fails to meet the minimum complexity requirements.
- **Orange** — The password meets the minimum complexity requirements but the password strength is weak.
- **Green** — The password is strong.

Step 5 Click **Apply**.

Note To delete a user, select the user name and click **Delete**. To edit an existing user, select the user name and click **Edit**, then click **Apply** to save all changes made to the configurations.

Changing a User Password

To change a user password:

Step 1 Select **System Configuration > User Accounts**.

The **User Account Table** shows the currently configured users. The user cisco is preconfigured in the system to have Read/Write privileges. The password for the user cisco can be changed.

Step 2 Select the user to configure and click **Edit**.

Step 3 Enter a new password between 0 and 127 characters and confirm the same password in the appropriate fields.

The **Password Strength Meter** indicates the password strength as follows:

- **Red** — The password fails to meet the minimum complexity requirements.
- **Orange** — The password meets the minimum complexity requirements but the password strength is weak.
- **Green** — The password is strong.

Step 4 Click **Apply**. The changes are saved to the Startup Configuration.

Note If you change your password, you must log in again to the system.

Management

This section describes how to configure the management settings on the WAP device.

Management

Use the **Management** section to configure the information that identifies the WAP device within the network.

To configure the system settings:

Step 1 Select **Management** > **Management** and configure the following parameters:

- **Host Name** — Enter the host name for the WAP device. By default, the name is the fully qualified domain name (FQDN) of the node. The default host name is wap concatenated with the last 6 hexadecimal digits of the MAC address of the WAP device. The host name label can contain only letters, digits, and hyphens. It cannot begin or end with a hyphen. No other symbols, punctuation characters, or blank spaces are permitted. The host name can be 1 to 63 characters long.
- **System Contact** — Enter the contact person for the WAP device. The system contact can be 0 to 255 characters long and can include spaces and special characters.
- **System Location** — Enter the physical location of the WAP device. The system location can be 0 to 255 characters long and can include spaces and special characters.

Step 2 Click **Apply**. The changes are saved to the Startup Configuration.

Connect Session Settings/HTTP/HTTPS Service

Use the **HTTP/HTTPS Service** to enable and configure the web-based management connections. If the HTTPS is used for secure management sessions, you can also use this page to manage the required SSL certificates.

To configure the HTTP and HTTPS services:

Step 1 Select **Management** > **Management**.

Step 2 In the **Connect Session Settings** area, configure the following parameters:

- **Maximum Sessions** — Enter the number of web sessions, including both the HTTP and HTTPS, that can be in use at the same time.

  When a user logs on to the WAP's configuration utility, a session is created. This session is maintained until the user logs off or the session timeout expires. The range is from 1 to 10 sessions. The default is 5. If the maximum number of sessions are reached, the next user who attempts to log on to the configuration utility receives an error message about the session limit.
- **Session Timeout** — Enter the maximum amount of time, in minutes, that an inactive user remains logged on. When the configured timeout is reached, the user is automatically logged off. The range is from 2 to 60 minutes. The default is 10 minutes.

Step 3 In the **HTTP/HTTPS Service** area, configure the following parameters:

- **HTTP Service** — Enable or disable access through HTTP. By default, HTTP access is disabled. If you disable it, any current connections using that protocol are disconnected.
  - **HTTP Port** — Enter the logical port number to use for the HTTP connections, from 1025 to 65535. The default port number for the HTTP connections is the well-known IANA port number 80.
  - **Redirect HTTP to HTTPS** — Redirects management HTTP access attempts on the HTTP port to the HTTPS port. This field is available only when HTTP access is disabled.
- **HTTPS Service** — Enable or disable access through secure HTTP (HTTPS). By default, HTTPS access is enabled. If you disable it, any current connections using that protocol are disconnected.
  - **HTTPS Port** — Enter the logical port number to use for the HTTPS connections, from 1025 to 65535. The default port number for the HTTPS connections is the IANA port number 443.
  - **TLSv1.0, TLSv1.1, SSLv3** — Check or uncheck the checkbox to enable or disable the protocol of the HTTPS Service.
- **Management ACL Mode** — If the Mode is enabled, access through the web and SNMP is restricted to the specified IP hosts. You can configure up to 5 IPv4 and 5 IPv6 addresses under the **Management Access Control**. If this feature is disabled, anyone can access the configuration utility from any network client by supplying the correct user name and password of the WAP device.

Note Verify any IP address that you enter. If you enter an IP address that does not match your administrative computer, you will lose access to the configuration interface. We recommend that you give the administrative computer a static IP address, so the address does not change over time.

Step 4 Click **Apply**.

SSL Certificate File Status

To use the HTTPS services, the WAP device must have a valid SSL certificate. The WAP device can generate a certificate, or you can download it from your network or from a TFTP server.

In the **Generate SSL Certificate** area, click **SSL Settings**, then click **Generate** to generate the certificate for the WAP device. This procedure should be done after the WAP device has acquired an IP address to ensure that the common name for the certificate matches the IP address of the WAP device. Generating a new SSL certificate restarts the secure web server. The secure connection does not work until the new certificate is accepted on the browser.

In the **SSL Certificate File Status** area, you can view the current certificate on the WAP device. The following will be displayed:

- **Certificate File Present**
- **Certificate Expiration Date**
- **Certificate Issuer Common Name**

If a SSL certificate (with a .pem extension) exists on the WAP device, you can download it to your computer as a backup. In the **Transfer SSL Certificate from** (Device to PC) area, select **HTTP/HTTPS** or **TFTP** as the download option and click **Transfer**.

- If you select **HTTP/HTTPS**, confirm the download and then browse to the location to save the file on your network.
- If you select **TFTP**, enter a file name to assign to the download file, and enter the TFTP server IPv4 address where the file will be downloaded.

You can also upload a certificate file (with a .pem extension) from your computer to the WAP device. In the **Transfer SSL Certificate from** (PC to Device) area, select **HTTP/HTTPS** or **TFTP** as the upload option and click **Transfer**.

- For **HTTP/HTTPS**, browse to the network location, select the file, and click **Transfer**.
- For **TFTP**, enter the file name and the TFTP Server IPv4 Address, then click **Transfer**. The filename cannot contain the following characters: spaces, <, >, |, \, : , (,), &, ; , #, ? aszxaa, *, and two or more successive periods.

A confirmation appears when the upload was successful.

SNMP / SNMPv2c Settings

SNMP defines a standard for recording, storing, and sharing information about network devices. SNMP facilitates network management, troubleshooting, and maintenance. The WAP supports SNMP and can function as an SNMP managed device for seamless integration into network management systems.

Use the SNMP/SNMPv2c Settings section to enable SNMP and configure the basic protocol settings.

To configure general SNMP settings:

Step 1 Select **Management> SNMP Settings**.

Step 2 Check **Enable** to enable **SNMP**.

Step 3 Enter the **UDP Port** for the SNMP traffic. The default is 161. However, you can configure it so that the agent listens to the requests on a different port. The valid range is from 1025 to 65535.

Step 4 In the **SNMPv2c Settings** area, configure the SNMPv2c settings:

- **Read-only Community** — Enter a read-only community name for the SNMPv2 access. The valid range is 1 to 256 alphanumeric and special characters.

  The community name acts as a simple authentication feature to restrict the devices on the network that can request data from the SNMP agent. The name functions as a password, and the request is assumed to be authentic if the sender knows the password.

- **Read-write Community** — Enter a read-write community name to be used for SNMP set requests. The valid range is from 1 to 256 alphanumeric and special characters. Setting a community name is similar to setting a password. Only the requests from the machines that identify themselves with this community name are accepted.

- **Management Station** — Determines which stations can access the WAP device through SNMP. Choose one of these options:

  - **All** — All stations can access the WAP device through SNMP.

- **User Defined** — The set of user defined SNMP requests that are permitted.

- **NMS IPv4 Address/Name** — Enter the IPv4 IP address, DNS host name, or subnet of the network management system (NMS).

  A DNS host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.

  As with community names, this setting provides a level of security on the SNMP settings. The SNMP agent only accepts the requests from the IP address, host name, or subnet specified here.

  To specify a subnet, enter one or more subnetwork address ranges in the form address/mask length where the address is an IP address and mask length is the number of mask bits. Both formats address/mask and address/mask length are supported. For example, if you enter a range of 192.168.1.0/24, this specifies a subnetwork with address 192.168.1.0 and a subnet mask of 255.255.255.0.

- **NMS IPv6 Address/Name** — The IPv6 address, DNS host name, or subnet of the devices that can execute, get, and set requests to the managed devices. The IPv6 address should be in a form similar to xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8:CAD5:7D91).

Note A host name can consist of one or more labels, which are sets of up to 63 alphanumeric characters. If a host name includes multiple labels, each is separated by a period (.). The entire series of labels and periods can be up to 253 characters long.

Step 5 In the **SNMPv2c Trap Settings** area, configure the SNMPv2c trap settings:

- **Trap Community** — Enter a global community string associated with SNMP traps. Traps sent from the device provide this string as a community name. The valid range is from 1 to 60 alphanumeric and special characters.

- **Trap Destination Table** — Enter a list of up to three IP addresses or host names to receive the SNMP traps. Check the box and choose a **Host IP Address Type** (IPv4 or IPv6) before adding the **Host Name/IP Address**.

  An example of a DNS host name is snmptraps.foo.com. Because the SNMP traps are sent randomly from the SNMP agent, it makes sense to specify where exactly the traps should be sent. You can have a maximum of three DNS host names. Ensure that you check **Enabled** and select the appropriate Host IP Address Type.

Step 6 Click **Apply**.

SNMPv3 Views

A SNMP MIB view is a family of view subtrees in the MIB hierarchy. A view subtree is identified by the pairing of an Object Identifier (OID) subtree value with a bit string mask value. Each MIB view is defined by two sets of view subtrees, included in or excluded from the MIB view. You can create MIB views to control the OID range that SNMPv3 users can access.

The WAP device supports a maximum of 16 views.

This section summarizes the critical guidelines for the SNMPv3 view configuration. Please read all the notes before proceeding.

Note A MIB view called all is created by default in the system. This view contains all management objects supported by the system.

Note By default, view-all and view-none SNMPv3 views are created on the WAP device. These views cannot be deleted or modified.

To add and configure an SNMP view, do the following:

Step 1 Select **Management** > **SNMP Settings** > **SNMPv3**.

Step 2 Click ✚ to create a new row in the **SNMPv3 Views** table or check the check box for existing views, then click **Edit**.

- **View Name** — Enter a name that identifies the MIB view. View names can contain up to 32 alphanumeric characters.
- **Type** — Choose whether to include or exclude the view subtree or family of subtrees from the MIB view.
- **OID** — Enter an OID string for the subtree to include or exclude from the view. For example, the system subtree is specified by the OID string.1.3.6.1.2.1.1.
- **Mask** — Enter an OID mask. The mask is 47 characters in length. The format of the OID mask is xx.xx.xx (.)... or xx:xx:xx.... (:) and is 16 octets in length. Each octet is two hexadecimal characters separated by either a period (.) or a colon (:). Only hex characters are accepted in this field. For example, OID mask FA.80 is 11111010.10000000.

A family mask is used to define a family of view subtrees. The family mask indicates which sub identifiers of the associated family OID string are significant to the family's definition. A family of view subtrees enables efficient control access to one row in a table.

Step 3 Click **Apply**.

Note To remove a view, check the view in the list and click **Delete**.

SNMPv3 Groups

The SNMPv3 groups allow you to combine users into groups of different authorization and access privileges. Each group is associated with one of three security levels:

- noAuthNoPriv
- authNoPriv
- authPriv

Access to MIBs for each group is controlled by associating a MIB view to a group for read or write access, separately.

By default, the WAP device has two groups:

- **RO** — A read-only group using authentication and data encryption. Users in this group use the SHA or password for authentication and a DES for encryption. The SHA and DES keys or passwords must be defined. By default, users of this group have read access to the default all MIB view.
- **RW** — A read/write group using authentication and data encryption. Users in this group use the SHA or password for authentication and a DES key for encryption. The SHA and DES keys or passwords must be defined. By default, users of this group have read and write access to the default all MIB view.

Note The default groups RO and RW cannot be deleted. The WAP device supports a maximum of eight groups.

To add and configure the SNMP group, perform the following steps:

Step 1 Select **Management** > **SNMP Settings** > **SNMPv3**.

Step 2 Click ✚ to add a new row to the **SNMPv3 Groups** table.

Step 3 Check the box for the new group and configure the following parameters:

- **Group Name** — Enter the name of the group. The default group names are RO and RW. Group names can contain up to 32 alphanumeric characters.
- **Security Level** — Choose the security level for the group, from the following options:
  - **noAuthNoPriv** — No authentication and no data encryption (no security).
  - **authNoPriv** — Authentication, but no data encryption. With this security level, users send SNMP messages that use the SHA or password for authentication, but not a DES key for encryption.
  - **authPriv** — Authentication and data encryption. With this security level, users send the SHA key or password for authentication and a DES for encryption. For groups that require authentication, encryption, or both, you must define the SHA and DES keys or passwords on the SNMP Users page.
- **Write Views** — Choose the write access for the group's MIBs from one of the following options:
  - **view-all** — The group can create, alter, and delete MIBs.
  - **view-none** — The group cannot create, alter, or delete MIBs.
- **Read Views** — Choose the read access to MIBs for the group, from one of the following options:
  - **view-all** — The group is allowed to view and read all MIBs.
  - **view-none** — The group cannot view or read MIBs.

Step 4 Click **Apply** to add the group to the SNMPv3 Groups list.

Note To delete a group, check the group in the list and click **Delete**. To edit a group, check the group in the list and click **Edit**.

SNMPv3 Users

Use the **SNMP Users** table to define users, associate a security level to each user, and configure the security keys per user.

Each user is mapped to a SNMPv3 group, either from the predefined or user- defined groups, and, optionally, is configured for authentication and encryption. For authentication, only the SHA is supported. For encryption, only the DES type is supported. There are no default SNMPv3 users on the WAP device, and you can add up to eight users.

To add SNMP users follow these steps:

Step 1 Select **Management** > **SNMP Settings** > **SNMPv3**.

Step 2 Click ✚ to add a new row to the **SNMPv3 Users** table.

Step 3 Check the box in the new row and configure these parameters:

- **User Name** — Enter the name that identifies the SNMPv3 user. User names can contain up to 32 alphanumeric characters.
- **Group** — Enter the name of group that the user is mapped to. The default groups are RW and RO. You can define additional groups on the SNMP Groups page.
- **Authentication Type** — Choose the type of authentication to use on the SNMPv3 requests from the user, from the following options:
  - **SHA** — Requires SHA authentication on SNMP requests from the user.
  - **None** — SNMPv3 requests from this user require no authentication.
- **Authentication Pass Phrase** — If you specify SHA as the authentication type, enter the pass phrase to enable the SNMP agent to authenticate the requests sent by the user. The pass phrase must be between 8 and 32 characters in length.
- **Encryption Type** — Choose the encryption/privacy type applied to the user's SNMP requests from the following options:
  - **DES** — Uses DES encryption on the SNMPv3 requests from the user.
  - **None**—SNMPv3 requests from this user require no privacy.
- **Encryption Pass Phrase** — If you specify DES as the encryption type, enter the pass phrase used to encrypt the SNMP requests. The pass phrase must be between 8 and 32 characters in length.

Step 4 Click **Apply**. The user is added to the SNMPv3 Users list and your changes are saved to the Startup Configuration.

Note To remove a user, select the user in the list and click **Delete**. To edit a user, select the user in the list and click **Edit**.

SNMPv3 Targets

The SNMPv3 targets send SNMP notifications using Inform messages to the SNMP manager. For SNMPv3 targets, only the Informs are sent, not traps. For SNMP versions 1 and 2, the traps are sent. Each target is defined with a target IP address, UDP port, and SNMPv3 user name.

Note The SNMPv3 user configuration should be completed before configuring the SNMPv3 targets. For more details, refer to SNMPv3 Users, on page 21.

The WAP device supports a maximum of eight targets.

To add SNMP targets follow these steps:

Step 1 Select **Management** > **SNMP Settings** > **SNMPv3 Targets**.

Step 2 Click ✚ to add a new row to the **SNMPv3 Targets** table.

Step 3 Check the check box in the new row and configure the following parameters:

- **IP Address** — Enter the IPv4 or IPv6 address of the remote SNMP manager to receive the target.
- **UDP Port** — Enter the UDP port to use for sending SNMPv3 targets. The classical port number is 161.
- **Users** — Enter the name of the SNMP user to associate with the target. To configure SNMP users, see the SNMPv3 Users, on page 21 page.

Step 4 Click **Apply**. The user is added to the **SNMPv3 Targets** list and your changes are saved to the Startup Configuration.

Note To remove a SMMP target, select the user in the list and click **Delete**. To edit a SMMP target, select the user in the list and click **Edit**.

Plug and Play (PnP)

Cisco Open Plug-n-Play (PnP) agent is a software application running on a Cisco SMB device. When a device is powered on, the Open Plug-n-Play agent discovery process, which is embedded in the device, attempts to discover the address of the Open Plug-n-Play server which helps automate the process of deploying and provisioning new devices into the network. This helps to apply configuration and install the required image without manual intervention. The Open Plug-n-Play agent uses methods like DHCP, Domain Name System (DNS), and Cisco cloud service discovery to acquire the desired IP address of the Open Plug-n-Play server.

Simplified deployment process of SMB device automates the following deployment related operational tasks

Step 1 Select **Management** > **PnP Settings**.

Step 2 Click **Enable**, and choose **PnP Transport** mode. Enter the following information.

Option	Description
PnP Transport	• **Auto**: Select this mode to download the image automatically from the PnP server through the AP.

Option	Description
	• **Static**: Select and specify values in the **IP/FQDN** and **Port** fields. Select the required certificate from the **CA Certificate** drop-down list. The default port number is 443.

Step 3 Click **Apply**.

Note To use a self-signed SSL certificate or in the absence of your certificate in the pre-installed CA list, select **User Specified** and click **Upload a certificate** to upload the certificate you want.

Security

This section describes how to configure the security settings on the WAP device.

Radius Server

Several features require communication with a RADIUS authentication server. For example, when you configure Virtual Access Points (VAPs) on the AP, you can configure security methods that control wireless client access. For more details, see Radio. The WPA Enterprise security methods use an external RADIUS server to authenticate clients. The MAC address filtering feature, where client access is restricted to a list, may also be configured to use a RADIUS server to control access. The Captive Portal feature also uses RADIUS to authenticate clients.

You can use the Radius Server page to configure the RADIUS servers that are used by these features. You can configure up to two globally available IPv4 or IPv6 RADIUS servers; however, you must select whether the RADIUS client operates in IPv4 or IPv6 mode with respect to the global servers. One of the servers always acts as a primary while the others act as backup servers.

Note In addition to using the global RADIUS servers, you can also configure each VAP to use a specific set of RADIUS servers. For more details, see Networks.

Configuring Global RADIUS Servers

Step 1 Select **Security** > **Radius Server**

Step 2 Configure these parameters:

- **Server IP Address Type**—Select the IP version that the RADIUS server uses. You can toggle between the address types to configure IPv4 and IPv6 global RADIUS address settings, but the WAP device contacts only the RADIUS server or servers with the address type that you select in this field.
- **Server IP Address-1 or Server IPv6 Address-1**—Enter the address for the primary global RADIUS server. When the first wireless client tries to authenticate with the WAP device, the WAP device sends an authentication request to the primary server. If the primary server responds to the authentication request, the WAP device continues to use this RADIUS server as the primary server, and authentication requests are sent to the address specified.

- **Server IP Address-2 or Server IPv6 Address-2** —Enter the addresses for the backup IPv4 or IPv6 RADIUS servers. If authentication fails with the primary server, the configured backup server is tried.
- **Key-1**—Enter the shared secret key that the WAP device uses to authenticate to the primary RADIUS server. You can use from 1 to 64 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server. The text that you enter appears as asterisks.
- **Key-2** —Enter the RADIUS key associated with the configured backup RADIUS servers. The server at Server IP (IPv6) Address 2 uses Key 2.
- **Enable RADIUS Accounting**—Enables tracking and measuring of the resources that a particular user has consumed, such as system time, amount of data transmitted and received, and so on. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.

Step 3 Click **Apply**.

802.1x

The IEEE 802.1X authentication enables the WAP device to gain access to a secured wired network. You can enable the WAP device as an 802.1X supplicant (client) on the wired network. A user name and password with the MD5 algorithm encryption can be configured to allow the WAP device to authenticate using 802.1X.

On the networks that use IEEE 802.1X port-based network access control, a supplicant cannot gain access to the network until the 802.1X authenticator grants access. If your network uses 802.1X, you must configure 802.1X authentication information on the WAP device, so that it can supply it to the authenticator.

Configuring 802.1x for WAP150

To configure the 802.1x settings for Cisco WAP150, do the following:

Step 1 Click **Security > 802.1x**.

Step 2 In the 802.1x area, check **Enable** to enable the **Administrative Mode**.

Step 3 Configure the 802.1X operational status and basic settings:

- **EAP Method** — Choose the algorithm to be used for encrypting authentication user names and passwords. The options are:
  - **MD5** — A hash function defined in RFC 3748 that provides basic security.
  - **PEAP** — Protected Extensible Authentication Protocol, which provides a higher level of security than MD5 by encapsulating it within a TLS tunnel.
  - **TLS** — Transport Layer Security, as defined in RFC 5216, an open standard that provides a high level of security.
- **Username** — Enter the username.
- **Password** — Enter the password. The password character length can be a range from 1-64.

Step 4 In the **Certificate File Upload** area, you can upload a certificate file to the WAP device:

a) Choose either **HTTP** or **TFTP** as the transfer method.

b) If you selected HTTP, click **Browse** to select the file. See Connect Session Settings/HTTP/HTTPS Service for more information on configuring the HTTP server settings.
c) If you selected **TFTP**, enter the **Filename** and the **TFTP Server IPv4 Address**.
d) Click **Upload**. A confirmation window appears, followed by a progress bar to indicate the status of the upload.

Step 5 Click **Apply**.

Configuring 802.1x for WAP361

To configure the 802.1x settings for Cisco WAP361, do the following:

Step 1 Click **Security** > **802.1x**.

Step 2 In the **802.1x** area, check **Enable** to enable the port configuration.

Step 3 Select one of the following to configure the port:

- **Supplicant**—Enable the 802.1x supplicant functionality.
- **Authenticator**—Enable the 802.1x authenticator functionality.

Step 4 To configure using 802.1x **Supplicant** functionality, do the following:

a) Click **More** and use the following parameters as required:

- **EAP Method** — Choose the algorithm to be used for encrypting authentication user names and passwords. The options are:
  - **MD5** — A hash function defined in RFC 3748 that provides basic security.
  - **PEAP** — Protected Extensible Authentication Protocol, which provides a higher level of security than MD5 by encapsulating it within a TLS tunnel.
  - **TLS** — Transport Layer Security, as defined in RFC 5216, an open standard that provides a high level of security.
- **Username** — Enter the username.
- **Password** — Enter the password. The password character length can be a range from 1-64.

Step 5 In the **Certificate File Upload** area, you can upload a certificate file to the WAP device:

a) Choose either **HTTP** or **TFTP** as the transfer method.
b) If you selected HTTP, click **Browse** to select the file. See Connect Session Settings/HTTP/HTTPS Service for more information on configuring the HTTP server settings.
c) If you selected **TFTP**, enter the **Filename** and the **TFTP Server IPv4 Address**.
d) Click **Upload**. A confirmation window appears, followed by a progress bar to indicate the status of the upload.
e) Click **OK** to save and close the dialogue.

Step 6 To configure using the 802.1x **Authenticator** functionality, do the following:

a) Click **More** and use the following parameters as required:

- **Use Global RADIUS Server Settings**—By default, each Ethernet port uses the global RADIUS settings that you define for the WAP device (see RADIUS Server). However, you can configure each port to use a different set of RADIUS servers.

- **Server IP Address Type**—The IP version that the RADIUS server uses. You can toggle between the address types to configure IPv4 and IPv6 global RADIUS address settings, but the WAP device contacts only the RADIUS server or servers for the address type you select in this field.
- **Server IP Address-1**—The address for the primary RADIUS server for this Ethernet port.

  When the first PC plugs in and tries to authenticate with the WAP device, the WAP device sends an authentication request to the primary server. If the primary server responds to the authentication request, the WAP device continues to use this RADIUS server as the primary server, and authentication requests are sent to the address you specify.

  The IPv4 address should be in a form similar to xxx.xxx.xxx.xxx (192.0.2.10). The IPv6 address should be in a form similar to xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).
- **Server IP Address-2**—The address for the backup RADIUS server for this Ethernet port. If authentication fails with the primary server, each configured backup server is tried in sequence.
- **Key-1**—The shared secret key that the WAP device uses to authenticate to the primary RADIUS server. You can use up to 63 standard alphanumeric and special characters. The key is case sensitive and must match the key configured on the RADIUS server.
- **Key-2**—The shared secret key that the WAP device uses to authenticate to the backup RADIUS server.
- **Enable RADIUS Accounting**—Enables tracking and measuring of the resources a particular user has consumed, such as system time, amount of data transmitted and received, and so on. If you enable RADIUS accounting, it is enabled for the primary RADIUS server and all backup servers.
- **Active Server** —Enables administratively selecting the active RADIUS server, rather than having the WAP device attempt to contact each configured server in sequence and choose the first server that is up.
- **Periodic Re-authentication**—Enables EAP re-authentication.
- **Re authentication Period**— Enter the EAP re-authentication period in seconds. The default is 3600. The valid range is from 300 to 4294967295 seconds.
- Click **OK** to save and close the dialogue.

Step 7 Click **Apply**.

Rogue AP Detection

A Rogue AP is an access point that has been installed on a secure network without explicit authorization from a system administrator. The rogue AP poses a security threat because anyone with access to the premises can unconsciously or maliciously install an inexpensive wireless WAP device that can potentially allow unauthorized parties to access the network.

The WAP device performs a RF scan on all channels to detect all APs in the vicinity of the network. If rogue APs are detected, they are shown on the Rogue AP Detection page. If an AP listed as a rogue is legitimate, it can be added to the Known AP List.

Note The Detected Rogue AP List and Trusted AP List provide information. The AP does not have any control over the APs on the list and cannot apply any security policies to APs detected through the RF scan.

When the Rogue AP detection is enabled, the radio periodically switches from its operating channel to scan other channels within the same band.

Viewing the Rogue AP List

In order for the Rogue AP Detection to function, the wireless radio must be enabled. You should first enable the radio interface before enabling the Rogue AP detection for the radio interface.

To enable the radio to collect information about rogue APs:

Step 1 Select **Security** > **Rogue AP Detection**.

Step 2 Check **Enable** to enable the AP Detection for Radio 1 and Radio 2.

Step 3 Click **Apply**.

The **Detected Rogue AP List** table displays all detected rogue APs. The **Trusted AP List** displays all trusted APs. The following settings are displayed for each or the Rogue AP lists:

- **MAC Address** — The MAC address of the rogue AP.
- **Radio** — Indicates whether the rogue AP is detected on Radio 1 or Radio 2.
- **Beacon Interval (Msec.)** — The beacon interval used by the rogue AP. Beacon frames are transmitted by an AP at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second). The Beacon Interval is set on the Radio page.
- **Type** — The type of the device. The options are:
  - **AP** — An AP rogue device that supports the IEEE 802.11 Wireless Networking Framework in infrastructure mode.
  - **Ad hoc** — A rogue station running in Ad hoc mode. The Ad hoc mode is an IEEE 802.11 Wireless Networking Framework also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS).
- **SSID** — The Service Set Identifier (SSID) for the WAP device.
- **Privacy** — Indicates whether there is any security on the rogue device. The options are:
  - **Off** — Security mode is off (no security).
  - **On** — Security mode is on.
- **WPA** — Shows whether the WPA security is on or off for the rogue AP.
- **Band** — The IEEE 802.11 mode being used on the rogue AP, such as IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE 802.11ac.

  The number shown indicates the mode:
  - 2.4 indicates IEEE 802.11b, 802.11g, or 802.11n mode (or a combination of the modes).

- 5 indicates IEEE 802.11a, 802.11n, or 802.11ac mode (or a combination of the modes).

- **Channel** — The channel on which the rogue AP is currently broadcasting.
- **Rate** — The rate in megabits per second at which the rogue AP is currently transmitting. The current rate is always one of the rates shown in the Supported Rates field.
- **Signal** — The strength of the radio signal emitting from the rogue AP. The number representing the strength in decibels (dB) is displayed on the right side of the bar.
- **Beacons** — The total number of beacons received from the rogue AP since it was first discovered.
- **Last Beacon** — The date and time of the last beacon received from the rogue AP.
- **Rates** — Supported and basic (advertised) rates set for the rogue AP. Rates are shown in megabits per second (Mbps). All Supported Rates are listed, with Basic Rates shown in bold. Rate sets are configured on the Radio page.

Step 4 Check the AP List, then click the **Move to Trusted AP List** in order to move the AP to the **Trusted AP List**. If the AP is in the **Trusted AP List**, click the **Move to Rogue AP List** in order to move the AP to the **Detected Rogue AP List**.

Step 5 Click **Refresh** to refresh the screen and display the most current information.

Saving the Trusted AP List

To create a Trusted AP List and save it to a file:

Step 1 Select **Security** and click **View Rogue AP List...** in the **Rogue AP Detection** section. The **Rogue AP Detection** page is displayed.

Step 2 In the **Detected Rogue AP List**, click **Move to Trusted AP List** for the APs that are known to you. The trusted APs move to the **Trusted AP List**.

Step 3 In the **Download/Backup Trusted AP List** area, click **Backup (AP to PC)**.

Step 4 Click **Apply**.

The list contains the MAC addresses of all APs that have been added to the **Trusted AP List**. By default, the filename is Rogue1.cfg. You can use a text editor or web browser to open the file and view its contents.

Importing a Trusted AP List

You can import a list of known APs from a saved list. The list may be acquired from another AP or created from a text file. If the MAC address of an AP appears in the Trusted AP List, it is not detected as a rogue.

To import an AP list from a file:

Step 1 Select **Security > Rogue AP Detection>View Rogue AP List...**.

Step 2 In the **Download/Backup Trusted AP List** area, click **Download (PC to AP)**.

Step 3 In the **Source File Name** field, click **Browse** to choose the file to import.

The imported file must be a plain-text file with a .txt or .cfg extension. Entries in the file are MAC addresses in hexadecimal format with each octet separated by colons, for example, 00:11:22:33:44:55. You must separate entries with a single space. For the AP to accept the file, it must contain only MAC addresses.

Step 4 In the **File Management Destination** field, choose whether to replace the existing **Trusted AP List** or add the entries in the imported file to the **Trusted AP List**. The options are:

- **Replace** — Imports the list and replaces the contents of the **Trusted AP List**.
- **Merge** — Imports the list and adds the APs in the imported file to the APs currently shown in the **Trusted AP List**.

Step 5 Click **Apply**.

When the import is complete, the screen refreshes and the MAC addresses of the APs in the imported file appear in the **Trusted AP List**.

Configure Password Complexity

Use the Password Complexity page to modify the complexity requirements for passwords used to access the configuration utility. Complex passwords increase security.

To configure the password complexity requirements follow the subsequent steps:

Step 1 Select **Security** > **Configure Password Complexity**.

Step 2 Check **Enable** to enable **Password Complexity**.

Step 3 Configure the following parameters:

- **Password Minimum Character Class** — Enter the minimum number of character classes that must be represented in the password string. The four possible character classes are uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard. The default value for this field is 3. The range can be between 0-4 characters.
- **Password Different from Current** — Check to enable that users enter a different password when their current password expires. If left unchecked, users can reenter the same password when it expires.
- **Maximum Password Length** — The maximum password character length is a range from 64 to 127. The default is 64.
- **Minimum Password Length** — The minimum password character length is a range from 0 to 32. The default is 8.
- **Password Aging Support** — Check to enable password expiration after a configured time period.
- **Password Aging Time** — Enter the number of days before a newly created password expires, from 1 to 365. The default is 180 days.

Step 4 Click **Apply**. The changes are saved to the Startup Configuration.

Note When the **Password Aging Time** is up, you will be required to access the Changing Password page.

Configure WAP-PSK Complexity

When you configure the VAPs on the WAP device, you can select a method of securely authenticating clients. If you select the WPA Personal protocol (also known as WPA pre-shared key or WPA-PSK) as the security method, you can configure the complexity requirements on the WPA-PSK Complexity page to be used in the authentication process. More complex keys provide increased security.

To configure the WPA-PSK complexity:

Step 1 Select **Security** > **Configure WPA-PSK Complexity**.

Step 2 Check **Enable** to enable the WAP device to check the WPA-PSK keys against the configured criteria. If disabled, none of the configured settings are used. The **WPA-PSK Complexity** is disabled by default.

Step 3 Configure these parameters:

- **WPA-PSK Minimum Character Class** — Choose the minimum number of character classes that must be represented in the key string. The four possible character classes are uppercase letters, lowercase letters, numbers, and special characters available on a standard keyboard. The default value for this field is 3. The range can be between 0-4 characters.
- **WPA-PSK Different from Current** — Check **Enable** to enable users to configure a different key after their current key expires. If disabled, users can use the old or previous key after their current key expires.
- **Maximum WPA-PSK Length** — Enter a key length value. The maximum key length in number of characters is from 32 to 63. The default is 63.
- **Minimum WPA-PSK Length** — Enter a key length value. The minimum key length in number of characters is from 8 to 16. The default is 8.

Step 4 Click **Apply**.