



Configuring Devices

The Configure tab allows you to view, create, copy, edit, and delete configuration templates and apply them to large numbers of devices at a time. It also allows you to schedule a configuration job and to check on the job's status.

Following are the subtabs under Configure:



Note

Some of the subtabs may not be visible to some users.

- **Templates**—See [Using the Templates, page 3-1](#).
- **Jobs**—See [Managing Configuration Jobs, page 3-91](#).

Using the Templates

This window allows you to create, modify, and delete configuration templates.

The topics covered in this section are:

- [Creating a Template, page 3-89](#)
- [Copying a Template, page 3-90](#)
- [Editing a Template, page 3-90](#)
- [Deleting a Template, page 3-91](#)

Related Topic

[Managing Configuration Jobs, page 3-91](#)

Template Choices

**Note**

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

When you create or edit a configuration template, the following choices appear in the left pane of the Templates window:

1. **Template Name**—See [Naming the Template, page 3-3](#).
2. **Template Categories**

**Note**

Any or all of the template categories can be completed in any order.

- **Express Template**—See [Using Express Template, page 3-3](#).
 - **Association**—See [Setting Up Association, page 3-7](#).
 - **Ethernet**—See [Configuring the Ethernet Port, page 3-31](#).
 - **Radio**—See [Configuring the Radio, page 3-36](#).
 - **Security**—See [Defining the Security Settings, page 3-50](#).
 - **Services**—See [Configuring Services, page 3-59](#).
 - **Events**—See [Configuring Events, page 3-78](#).
 - **Custom Values**—See [Configuring Custom Values, page 3-84](#).
3. **Preview**—See [Previewing the Template, page 3-88](#).
 4. **Finish**—See [Finishing the Template, page 3-88](#).

Naming the Template

This option enables to you to name the template.

Procedure



Note Clicking **Clear** removes all the entries you have made.

Step 1 Select **Template Name**. The Template Name dialog box appears:

Field	Description
Name	Enter a name for the template. See Naming Guidelines, page A-1 .
Description	Enter a description of the purpose of the template. See Naming Guidelines, page A-1

Step 2 Select a template category. (For additional information, see [Template Categories, page 3-2](#).)

Using Express Template

Use this option if you need to set up an access point quickly with a simple configuration. This will allow you to enter all the access point's essential settings for basic operation.

Procedure

Step 1 Select **Express Template**. The Express dialog box displays in the right pane:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-1 *Express Template Settings*

Field	Description
Configuration Server Protocol	<p>Set this entry to match the network's method of IP address assignment.</p> <p>From the list, select one of the following options:</p> <ul style="list-style-type: none"> • None-Static IP—Use this if your network does not have an automatic system for IP address assignment. • BOOTP—Use this if your network uses Bootstrap Protocol, in which IP addresses are hard-coded based on MAC addresses. • DHCP—Use this if your network uses Dynamic Host Configuration Protocol, in which IP addresses are “leased” for predetermined periods of time.
Default Subnet Mask	<p>Enter an IP subnet mask to identify the subnetwork so the IP address can be recognized on the LAN.</p> <p>If DHCP or BOOTP is not enabled, this field is the subnet mask.</p> <p>If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's DHCP or BOOTP request.</p>

Table 3-1 Express Template Settings (continued)

Field	Description
Default Gateway	Enter the IP address of your default Internet gateway. The entry 255.255.255.255 indicates no gateway.
Radio Service Set ID (SSID)	Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 2 to 32 characters long. Several access points on a network or sub-network can share an SSID.

Table 3-1 Express Template Settings (continued)

Field	Description
Role in Network	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Access Point—Use this setting if the access point is connected to the wired LAN. • Repeater—Use this setting for access points not connected to the wired LAN. • Survey Client—Use this setting when performing a site survey for a repeater access point. When you select this setting, clients are not allowed to associate and the bridge's STP function is disabled. • Root Bridge—Use this setting to set a bridge as the root bridge. (One bridge in each group of bridges must be set as the root bridge). The root bridge cannot associate with another root bridge. • Non-Root Bridge w/ Client—Use this setting for non-root bridges that accept associations from client devices and for bridges acting as repeaters. A non-root bridge will only associate to another bridge (root or non-root). • Non-Root Bridge w/o Client—Use this setting for non-root bridges that should not accept associations from client devices. A non-root bridge (without clients) can connect to a wired LAN and only associates to another bridge (root or non-root).

Table 3-1 Express Template Settings (continued)

Field	Description
Ensure Compatibility with Cisco	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to automatically configure the device to be compatible with other Cisco devices on your wireless LAN. • Disable—Use this setting to not automatically configure the device to be compatible with other Cisco devices on your wireless LAN.
Ensure Compatibility with 2MB/sec Clients	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable— Use this setting to operate at a maximum speed of two megabits per second. • Disable—Use this setting if you do not want devices to operate at a maximum speed of two megabits per second.

Step 2 Select one of the following:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Setting Up Association

Use this option to set up spanning tree protocol (STP) on bridges and to set up filtering to control the flow of data through the access point.

Procedure

- Step 1** Select **Association**. The menu expands and the Association dialog box displays in the right pane.
- Step 2** Select one of the following from the Association menu:
- Spanning Tree—[Defining Spanning Tree Protocol, page 3-8](#).
 - Address Filters—[Defining Address Filters, page 3-11](#).
 - Ethertype Filters—[Defining Ethertype Filters, page 3-12](#).
 - IP Protocol Filters—[Defining IP Protocol Filters, page 3-16](#).
 - IP Port Filters—[Defining IP Port Filters, page 3-21](#).
 - Advanced—[Defining Advanced Associations, page 3-25](#).
 - Port Assignments—[Configuring Port Assignments, page 3-30](#).
-

Defining Spanning Tree Protocol

This option is used for only bridges.

Procedure

- Step 1** Select **Association > Spanning Tree**. The Association: Spanning Tree Protocol dialog box appears.
- Step 2** Click **see details** for information on which bridges this configuration is valid.

Step 3 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-2 Spanning Tree Protocol Settings

Field	Description
Spanning Tree Protocol (STP)	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable STP on the bridge. • Disable—If you do not want STP enabled the bridge.
Root Configuration	
Priority (0-65535)	<p>Enter a number to influence which bridge is designated the root bridge in the spanning tree.</p> <p>When bridges have the same priority setting, STP uses the bridges' MAC addresses as a tiebreaker.</p> <p>The bridge with the lowest priority setting is likely to be designated the root bridge in the tree.</p>
Max Age (6-40 Seconds)	<p>Enter the number of seconds to define how long the bridge waits before deciding the network has changed and the spanning tree needs to be rebuilt.</p> <p>For example, with Max Age set to 20, the bridge attempts to rebuild the spanning tree if it does not receive a hello BPDU from the root bridge in the spanning tree within 20 seconds.</p>
Hello Time (1-10 Seconds)	<p>Enter the number of seconds to define how often the root bridge in the spanning tree sends out a hello BPDU telling the other bridges that the network topology has not changed and that the spanning tree should remain the same.</p>

Table 3-2 Spanning Tree Protocol Settings (continued)

Field	Description
Forward Delay (4-30 Seconds)	Enter the number of seconds to define how long the bridge's ports should stay in the listening and learning transition states if there is a change in the spanning tree.
Port Configuration	
Path Cost (1-65535)	Enter a number to indicate the relative efficiency of a port's network link. A port with a high path cost is less likely to become a bridge's root port.
Priority (0-255)	Enter a number to influence whether STP designates a port as a bridge's root port. A port with a low priority setting is more likely to become a bridge's root port.
Enable	From the list, select one of the following for each port configured: <ul style="list-style-type: none"> • Enable—Use this setting to indicate whether the port participates in STP. (This determines whether the port blocks or forwards traffic.) • Disable—Use this setting to indicate that the port does not participate in STP.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Defining Address Filters

Using this option, you can:

- Create a MAC address filter
- Remove a MAC address filter

Procedure

Step 1 Select **Association > Address Filters**. The Association: Address Filters dialog box appears.

Step 2 To add a new MAC address filter complete the following fields:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
New Destination MAC Address	Enter a destination MAC address by entering the address in one of the following ways: <ul style="list-style-type: none"> • With colons separating the character pairs (00:40:96:12:34:56, for example) • Without any intervening characters (004096123456, for example)
Allowed	Click to pass traffic to the MAC address.
Disallowed	Click to discard traffic to the MAC address.

Step 3 Click **Add** to add the MAC address to the Current MAC Address Filters list.

Step 4 To remove a MAC Address, select it from the Current MAC Address Filters list, then click **Remove**.

- Step 5** Select one of the following:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
-

Defining Ethertype Filters

Procedure

Step 1 Select **Association > Ethertype Filters**. The Association: Ethertype Filters dialog box appears.

Step 2 Using this option:

- Create new filters—See [Creating New Ethertype Filters, page 3-12.](#)
- Delete the Filters—See [Deleting Ethertype Filters, page 3-14.](#)

Using this option you can also:

- Create Special Cases —See [Creating Special Cases, page 3-14.](#)
- Delete Special Cases—See [Deleting Special Cases, page 3-16.](#)

Creating New Ethertype Filters

Procedure

Step 1 To create and enable protocol filters for the access point's Ethernet port, enter the following:

Table 3-3 *Creating New Ethertype Filters Settings*

Field	Description
Add New Ethertype Filter	
Set ID	Enter an identification number for the filter set.

Table 3-3 *Creating New Ethertype Filters Settings (continued)*

Field	Description
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page A-1 .
Default Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.
Default Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click **Add**. The new name is added to the Ethertype Filters list.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Deleting Ethertype Filters

Procedure

-
- Step 1** To delete protocol filters for the access point's Ethernet port, select the set name from the Current Ethertype Filters list, then click **Delete**.
- Step 2** Select one of the following:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
 - **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
 - Another template category to configure more options. (See [Template Categories, page 3-2](#).)
-

Creating Special Cases

Procedure

-
- Step 1** Select the default filter for which you want to define a special case.
- Step 2** Enter the following:

Table 3-4 Ethertype Filter Special Cases Settings

Field	Description
Special Cases	
Ethertype	Enter the Ethertype filter name.
Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Default—Use the disposition you set for the Ethertype filter. • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.

Table 3-4 Ethertype Filter Special Cases Settings (continued)

Field	Description
Priority	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network’s most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point’s buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point’s buffer before they are discarded.
Alert	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • no—Use this setting to not send an alert to the event log.

Step 3 Click **Add**. The new name is added to the list box.

- Step 4** Select one of the following:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
-

Deleting Special Cases

Procedure

- Step 1** To delete special cases for the access point's Ethernet port, select the Ethertype name from the list box, then click **Delete**.
- Step 2** Select one of the following:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
-

Defining IP Protocol Filters

Procedure

- Step 1** Select **Association > IP Protocol Filters**. The Association: IP Protocol Filters dialog box appears.
- Step 2** With this option you can:
- Create new filters—See [Creating New IP Protocol Filters, page 3-17.](#)
 - Delete the filters—See [Deleting IP Protocol Filters, page 3-18.](#)

Using this option you can also:

- Create Special Cases—See [Creating Special Cases, page 3-18](#).
- Delete Special Cases—See [Deleting Special Cases, page 3-21](#).

Creating New IP Protocol Filters

Procedure

Step 1 To create and enable IP protocol filters, enter the following:

Field	Description
Add New Protocol Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page A-1 .
Default Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.
Default Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click **Add**. The new name is added to the Current Protocol Filters list.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)

- **Finish** to save the template. (See [Finishing the Template](#), page 3-88.)
 - Another template category to configure more options. (See [Template Categories](#), page 3-2.)
-

Deleting IP Protocol Filters

Procedure

- Step 1** To delete an IP protocol filter, select the name from the Current Protocol Filters list, then click **Delete**.
- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template](#), page 3-88.)
 - **Finish** to save the template. (See [Finishing the Template](#), page 3-88.)
 - Another template category to configure more options. (See [Template Categories](#), page 3-2.)
-

Creating Special Cases

Procedure

- Step 1** Select the default filter for which you want to define a special case.
- Step 2** Enter the following:

Table 3-5 IP Protocol Filters Special Cases Settings

Field	Description
Special Cases	
Protocol	Enter the IP protocol name.

Table 3-5 IP Protocol Filters Special Cases Settings (continued)

Field	Description
Disposition	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Default—Use the disposition you set for the protocol filter. • Forward—Use this setting to forward traffic. • Block—Use this setting to block traffic.
Priority	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.

Table 3-5 IP Protocol Filters Special Cases Settings (continued)

Field	Description
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.
Alert	From the list, select one of the following: <ul style="list-style-type: none"> • yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • no—Use this setting to not send an alert to the event log.

Step 3 Click **Add**. The new name is added to the list box.

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Deleting Special Cases

Procedure

- Step 1** To delete special cases, select the protocol name from the list box, then click **Delete**.
- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
 - **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
 - Another template category to configure more options. (See [Template Categories, page 3-2](#).)
-

Defining IP Port Filters

Procedure

- Step 1** Select **Association > IP Port Filters**. The Association: IP Port Filters dialog box appears.
- Step 2** With this option you can:
- Create new filters—See [Creating New Port Filters, page 3-22](#).
 - Delete the filters—See [Deleting Port Filters, page 3-23](#).
- Using this option you can also:
- Create Special Cases —See [Creating Special Cases, page 3-23](#).
 - Delete Special Cases—See [Deleting Special Cases, page 3-25](#).
-

Creating New Port Filters

Procedure

Step 1 To create and enable port filters, enter the following:

Field	Description
Add New Protocol Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page A-1 .
Default Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Forward—Use this setting to forward traffic. • Block—Use this setting to block traffic.
Default Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click **Add**. The new name is added to the Current Port Filters list.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Deleting Port Filters

Procedure

-
- Step 1** To delete a protocol filter, select the name from the Current Port Filters list, then click **Delete**.
- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
 - **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
 - Another template category to configure more options. (See [Template Categories, page 3-2](#).)
-

Creating Special Cases

Procedure

-
- Step 1** Select the default filter for which you want to define a special case.
- Step 2** Enter the following:

Table 3-6 IP Port Filters Special Cases Settings

Field	Description
Special Cases	
Port	Enter the IP Port filter name.
Disposition	From the list, select one of the following: <ul style="list-style-type: none"> • Default—Use the disposition you set for the port filter. • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.

Table 3-6 IP Port Filters Special Cases Settings (continued)

Field	Description
Priority	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the buffer before they are discarded.
Alert	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • no—Use this setting to not send an alert to the event log.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
-

Deleting Special Cases

Procedure

- Step 1** To delete special cases, select the port name from the list box, then click **Delete**.
- Step 2** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
-

Defining Advanced Associations

Use this option to control the total number of devices an access point can list in the Association Table and the amount of time the access point continues to track each device class when a device is inactive.

Procedure

Step 1 Select **Association > Advanced**. The Association: Advanced dialog box appears.

Step 2 To define advanced associations, enter the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-7 Advanced Association Settings

Field	Description
Alert Severity Level	<p>From the list select one of the following:</p> <ul style="list-style-type: none"> • <code>systemFatal</code>—Indicates an event that prevents operation of the port or device. • <code>protocolFatal</code>—Indicates an event that prevents operation of the port or device • <code>portFatal</code>—Indicates an event that prevents operation of the port or device • <code>systemAlert</code>—Indicates that you need to take action to correct the condition. • <code>protocolAlert</code>—Indicates that you need to take action to correct the condition. • <code>portAlert</code>—Indicates that you need to take action to correct the condition. • <code>externalAlert</code>—Indicates that you need to take action to correct the condition.

Table 3-7 Advanced Association Settings (continued)

Field	Description
	<ul style="list-style-type: none"> • systemWarning—Indicates that an error or failure may have occurred. • protocolWarning—Indicates that an error or failure may have occurred. • portWarning—Indicates that an error or failure may have occurred. • externalWarning—Indicates that an error or failure may have occurred. • systemInfo—Notification that some sort of event has occurred. • protocolInfo—Notification that some sort of event has occurred. • portInfo—Notification that some sort of event has occurred. • externalInfo—Notification that some sort of event has occurred.
Max Bytes Stored Per Alert Packet	<p>Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled.</p> <p>If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event.</p>
Max Fwd Table Entries	<p>From the list, select one of the following to designate the maximum number of devices that can appear in the Association Table:</p> <p>1024, 2048, 4096, 8192, 16384, 32768, 65536.</p>

Table 3-7 Advanced Association Settings (continued)

Field	Description
Enable Extended Stats in MIB	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable the storage of detailed statistics in the device’s memory. • Disable—Use this setting to disable the storage of detailed statistics in the device’s memory. <p>When you disable extended statistics you conserve memory, and the device can include more devices in the Association Table.</p>
Enable PSPF	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Enable—Use this setting to enable Publicly Secure Packet Forwarding, which ensures that client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses. • Disable—Use this setting to disable Publicly Secure Packet Forwarding. <p>Click see detail to see for which versions this setting is valid.</p>

Table 3-7 Advanced Association Settings (continued)

Field	Description
Unknown Class Timeout	Enter the number of seconds the access point continues to track an inactive device depending on its class. A setting of zero tells the access point to track a device indefinitely no matter how long it is inactive. A setting of 300 equals 5 minutes; 1800 equals 30 minutes; 28800 equals 8 hours.
Multicast Addresses Timeout	
Infrastructure Hosts Timeout	
Client Stations Timeout	
Repeaters Timeout	
Access Points Timeout	
Across Bridge Hosts Timeout	
Non-Root Bridges Timeout	
Root Bridges Timeout	

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Configuring Port Assignments

When you assign specific ports, your network topology remains constant even when devices reboot.

Procedure

Step 1 Select **Association > Port Assignments**. The Association: Port Assignments dialog box appears.

Step 2 To define port assignments, enter the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
ifIndex	Lists the port's designator in the Standard MIB-II (RFC1213-MIB.my) interface index.
dot1dBasePort	Lists the port's designator in the Bridge MIB (RFC1493; BRIDGE-MIB.my) interface index.
AID	Lists the port's 802.11 radio drivers association identifier.
Station	Enter the MAC address of the device to which you want to assign the port.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Configuring the Ethernet Port

Use this option to configure the device's Ethernet port.

Procedure

Step 1 Select **Ethernet**. The menu expands and the Ethernet dialog box displays in the right pane.

Step 2 Select one of the following from the Ethernet menu:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Identification—See [Identifying the Ethernet Port, page 3-31](#).
 - Filters—See [Setting Up Ethernet Filters, page 3-32](#).
 - Advanced—See [Defining the Ethernet Advanced Settings, page 3-34](#).
-

Identifying the Ethernet Port

Use this option to define basic identity information for the Ethernet port.

Procedure

Step 1 Select **Ethernet > Identification**. The Ethernet: Identification dialog box displays in the right pane.

Step 2 Enter the following information to identify the port:

Field	Description
Primary Port?	From the list, select one of the following: <ul style="list-style-type: none"> • yes—Sets the Ethernet port as the primary port. • no—Sets the radio port as the primary port.
Adopt Primary Port Identity?	From the list, select one of the following: <ul style="list-style-type: none"> • yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port. • no—This uses different MAC and IP addresses for the Ethernet port.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Setting Up Ethernet Filters

Use this option to define filters for the Ethernet port, the IP Protocol, and the IP Port.



Note

Changing this setting may cause the access point to reboot.

Procedure

- Step 1** Select **Ethernet > Filters**. The Ethernet: Filters dialog box displays in the right pane.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using Association > Ethertype Filters .
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using Association > Ethertype Filters .
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
IP Port	
Receive	Enter the ID of a defined IP port filter, or select one of the filters you created using Association > IP Port Filters .
Transmit	Enter the ID of a defined IP port filter, or select one of the filters you created using Association > IP Port Filters .

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
 - **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)

- Another template category to configure more options. (See [Template Categories](#), page 3-2.)

Defining the Ethernet Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Procedure

Step 1 Select **Ethernet > Advanced**. The Ethernet: Advanced dialog box displays in the right pane.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-8 Ethernet Advanced Settings

Field	Description
Status	From the list, select one of the following: <ul style="list-style-type: none"> • up— Enables the Ethernet port for normal operation. • down—Disables the device’s Ethernet port.
Packet Forwarding	From the list, select one of the following: <ul style="list-style-type: none"> • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.

Table 3-8 Ethernet Advanced Settings (continued)

Field	Description
Default Multicast Address Filter	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under Association > Address Filters. disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under Association > Address Filters.
Maximum Multicast Packets/Second	<p>Use this setting to control the number of multicast packets that can pass through the Ethernet port each second.</p> <p>If you enter 0, the access point passes an unlimited number of multicast packets.</p> <p>If you enter a number other than 0, the device passes only that number of multicast packets per second.</p>
Default Unicast Address Filter	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> allowed—The access point forwards all traffic except packets sent to MAC addresses that have been set as disallowed under Association > Address Filters. disallowed—The access point discards all traffic except packets sent to the MAC addresses that have been set as allowed under Association > Address Filters.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Configuring the Radio

Use this option to configure the device's radio.

Procedure

- Step 1** Select **Radio**. The menu expands and the Radio dialog box displays in the right pane.
- Step 2** Select one of the following from the Radio menu:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Identification—See [Identifying the Radio Port](#), page 3-36.
- Filters—See [Setting Up Radio Filters](#), page 3-38.
- Hardware—See [Defining the Radio Hardware Settings](#), page 3-39.
- Advanced—See [Defining the Radio Advanced Settings](#), page 3-44.
- Searched Channels—See [Defining the Radio Searched Channels Settings](#), page 3-48.

Identifying the Radio Port

Use this option to define basic identity information for the Ethernet port.



Note Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **Radio > Identification**. The Radio: Identification dialog box displays in the right pane.

Step 2 Enter the following information to identify the port:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Primary Port?	From the list, select one of the following: <ul style="list-style-type: none"> • yes—Sets the radio port as the primary port. • no—Sets the Ethernet port as the primary port.
Adopt Primary Port Identity?	From the list, select one of the following: <ul style="list-style-type: none"> • yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port. • no—This uses different MAC and IP addresses for the Ethernet port.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Setting Up Radio Filters


Note

Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **Radio > Filters**. The Radio Filters dialog box displays in the right pane.

Step 2 Complete the following:


Note

Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-9 Radio Filters Settings

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using Association > Ethertype Filters .
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using Association > Ethertype Filters .
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using Association > IP Protocol Filters .

Table 3-9 Radio Filters Settings (continued)

Field	Description
IP Port	
Receive	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using Association > IP Port Filters .
Transmit	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using Association > IP Port Filters .

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Defining the Radio Hardware Settings

Procedure

Step 1 Select **Radio > Hardware**. The Radio: Hardware dialog box displays in the right pane.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-10 Radio Hardware Settings

Field	Description
Service SetID (SSID)	<p>Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 2 to 32 characters long.</p> <p>Several access points on a network or sub-network can share an SSID.</p>
Allow “Broadcast” SSID to Associate	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Allows devices that do not specify an SSID (devices that are “broadcasting” in search of an access point to associate with) to associate with the access point. • no—Does not allow devices that do not specify an SSID (devices that are “broadcasting” in search of an access point to associate with) to associate with the access point. <p>With no selected, the SSID used by the client device must match exactly the access point’s SSID.</p>
Enable “World Mode” multi-domain operation?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Allows the access point to add channel carrier set information to its beacon. <p>Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically.</p> <ul style="list-style-type: none"> • no—Does not allow the access point to add channel carrier set information to its beacon.

Table 3-10 Radio Hardware Settings (continued)

Field	Description
Data Rates (Mb/sec)	
1.0	<p>From the list, select one of the following for each of the four rates in megabits per second:</p> <ul style="list-style-type: none"> • basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic. • yes—Allows transmission at this rate for unicast packets only. • no—Does not allow transmission at this rate.
2.0	
5.5	
11.0	
Transmit Power	<p>From the list, select one of the following milliwatt settings: 1, 5, 20, 30, 50, 100.</p> <p>To reduce interference or to conserve power, select a lower power setting.</p>
Fragmentation Threshold (256-2338)	<p>Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block).</p> <p>Use a low setting in areas where communication is poor or where there is a great deal of radio interference.</p>
RTS Threshold (0-2339)	<p>Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet.</p> <p>A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other.</p>

Table 3-10 Radio Hardware Settings (continued)

Field	Description
Maximum RTS Retries (1-128)	Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.
Max. Data Retires (1-128)	Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.
Beacon Period (Kusec)	Enter the amount of time between beacons in Kilo microseconds. (One Kmsec equals 1,024 microseconds.)
Data Beacon Rate (DTIM)	<p>Enter the amount of time, always a multiple of the beacon period, to determine how often the beacon contains a delivery traffic indication message (DTIM).</p> <p>The DTIM tells power-save client devices that a packet is waiting for them.</p> <p>If the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 Kmsecs. (One Kmsec equals 1,024 microseconds.)</p>
Default Radio Channel	<p>From the list, select the radio channel you want for a default. Each channel covers 22 MHz.</p> <p>The factory setting for Cisco wireless LAN systems is Radio Channel 6 transmitting at 2437 MHz.</p>

Table 3-10 Radio Hardware Settings (continued)

Field	Description
Search for less-congested Radio Channel?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use. • no—Will not allow the access point to scan for a radio channel that is least busy.
Receive Antenna	<p>From the list, select one of the following:</p>
Transmit Antenna	<ul style="list-style-type: none"> • Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector. (When you look at the access point's back panel, the right antenna is on the right.) Use this setting for both receive and transmit. • Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.) Use this setting for both receive and transmit. • Diversity—Use this setting if your access point has two fixed (non-removable) antennas; it tells the access point to use the antenna that receives the best signal. Use this setting for both receive and transmit.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
-

Defining the Radio Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Procedure

- Step 1** Select **Radio > Advanced**. The Radio: Advanced dialog box displays in the right pane.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-11 Radio Advanced Settings

Field	Description
Status	From the list, select one of the following: <ul style="list-style-type: none"> • up— Enables the Radio port for normal operation. • down—Disables the device’s Radio port.
Packet Forwarding	From the list, select one of the following: <ul style="list-style-type: none"> • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.

Table 3-11 Radio Advanced Settings (continued)

Field	Description
Default Multicast Address Filter	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under Association > Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under Association > Address Filters.
Maximum Multicast Packets/Second	<p>Use this setting to control the number of multicast packets that can pass through the Ethernet port each second.</p> <p>If you enter 0, the access point passes an unlimited number of multicast packets.</p> <p>If you enter a number other than 0, the device passes only that number of multicast packets per second.</p>
Maximum Number of Associations	<p>Enter the maximum number of wireless networking devices that are allowed to associate to the access point.</p> <p>If you enter 0 it means that the maximum possible number of associations is allowed.</p> <p>Click see details to see for which versions this setting is valid.</p>
Use Aironet Extensions	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • no—Does not enable the features listed above.

Table 3-11 Radio Advanced Settings (continued)

Field	Description
Ethernet encapsulation transform	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • 802.1H—Provides optimum performance for Cisco Aironet wireless products. • RFC1042—Ensures interoperability with non-Cisco Aironet wireless equipment.
Enhanced MIC verification for WEP	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • None—Does not enable MIC. • NMH—Enables MIC (Message Integrity Check), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks. <p>Click see details to see for which versions this setting is valid.</p>
Temporal Key Integrity Protocol	<p>From the list, select the following:</p> <ul style="list-style-type: none"> • None—Does not enable WEP key hashing. • Cisco— Enables WEP key hashing that defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. <p>Click see details to see for which versions this setting is valid.</p>

Table 3-11 Radio Advanced Settings (continued)

Field	Description
Broadcast WEP Key rotation interval (sec)	<p>Enter a rotation interval in seconds.</p> <ul style="list-style-type: none"> If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. If you enter 0, you disable broadcast WEP key rotation. <p>Click see details to see for which versions this setting is valid.</p>
Default Unicast Address Filter	
Open	From the list, select one of the following:
Shared	<ul style="list-style-type: none"> Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p>
Network-EAP	
Specified Access Point 1	<p>If this access point is a repeater, enter the MAC address of one or more root-unit access points with which you want this access point to associate.</p> <p>With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.</p>
Specified Access Point 2	
Specified Access Point 3	
Specified Access Point 4	

Table 3-11 Radio Advanced Settings (continued)

Field	Description
Radio Modulation	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Standard—This setting is the modulation type specified in IEEE 802.11, the wireless standard published by the Institute of Electrical and Electronics Engineers (IEEE) Standards Association. • MOK—This modulation was used before the IEEE finished the high-speed 802.11 standard and may still be in use in older wireless networks.
Radio Preamble	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Long—Ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). • Short—Cisco Aironet’s Wireless LAN Adapter supports short preambles; it improves throughput performance.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Defining the Radio Searched Channels Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.

Procedure

Step 1 Select **Radio > Searched Channels**. The Radio: Searched Channels dialog box displays in the right pane.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Channel Number	List the available channels by number.
Frequency (mHz)	Lists the channel frequency.
Search?	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this option to include the channel in the scan for less-congested channels. • No—Use this option to exclude the channel in the scan for less-congested channels

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Defining the Security Settings

Use this option to configure the device's security settings.

Procedure

Step 1 Select **Security**. The menu expands and the Security dialog box displays in the right pane.

Step 2 Select one of the following from the Security menu:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Local Admin Access—See [Setting Local Admin Access, page 3-50](#).
 - Local AP/Client Security—See [Setting Local AP/Client Security, page 3-51](#).
 - Server-Based Security—See [Setting Server-Based Security, page 3-54](#).
-

Setting Local Admin Access

Use this option to enable or disable local admin access.

Procedure

Step 1 Select **Security > Local Admin Access**. The Security: Local Admin Access dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Local Admin Authentication	Select Enable to enable local admin authentication, or Disable to disable it.
Allow read-only browsing without login	Select Yes to allow it, or No to disallow it.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Setting Local AP/Client Security

Use this option to set up the local access point and client security.

Procedure

Step 1 Select **Security > Local AP/Client Security**. The Security: Local AP/Client Security dialog box appears:

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-12 Local AP /Client Security Settings

Field	Description
Data Encryption by Stations	<p>From the list, select the encryption type:</p> <ul style="list-style-type: none"> • No Encryption—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended. • Optional—Allows clients to communicate with the Access Point either with or without data encryption. Typically, this option is used when you have client devices that cannot make a WEP connection, such as non-Cisco clients in a 128-bit WEP environment. • Full Encryption—Requires clients to use data encryption when communicating with the Access Point. Clients not using data encryption are allowed to communicate. This option is recommended if you want to maximize the security of your Wireless LAN.
Authentication Type	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared Key	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.

Table 3-12 Local AP /Client Security Settings (continued)

Field	Description
Network-EAP	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.
Shared	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Encryption Keys 1 through 4	
Transmit Key	Click to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.

Table 3-12 Local AP /Client Security Settings (continued)

Field	Description
Encryption Key	Enter the type of encryption key used: <ul style="list-style-type: none"> For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F). For 128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).
Key Size	From the list, select one of the following: <ul style="list-style-type: none"> Not set 40 bit 128 bit

- Step 3** Select one of the following in the left pane:
- Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
 - Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
 - Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Setting Server-Based Security

Use this option to set up server-based security.



Note

Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **Security > Server-Based Security**. The Security: Server-Based dialog box appears:

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-13 Server-Based Security Settings

Field	Description
Server Name/IP	Enter the name or IP address of the server.
Server Type	Enter the type of server.
Port	Enter the port number your server uses for authentication.
Shared Secret	Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.
Time Out (sec's)	Enter the number of seconds the access point should wait before authentication fails. If the server does not respond within this time, the access point tries to contact the next defined authentication server.
Use this server for	

Table 3-13 Server-Based Security Settings (continued)

Field	Description
EAP Authentication	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Yes—Use this server for EAP authentication. <p>In this type of authentication, the access point relays authentication messages between the server and the authenticating client device.</p> <ul style="list-style-type: none"> • No—Do not use this server for EAP authentication. <p>Click see detail to see for which versions this setting is valid.</p>

Table 3-13 Server-Based Security Settings (continued)

Field	Description
MAC Address Authentication	<p data-bbox="733 293 1197 321">From the list, select one of the following:</p> <ul data-bbox="744 337 1197 394" style="list-style-type: none"><li data-bbox="744 337 1197 394">• Yes—Use this server for MAC-based authentication. <p data-bbox="778 415 1228 634">This allows only client devices with specified MAC addresses to associate and pass data through the access point. Client devices with MAC addresses not in a list of allowed MAC addresses are not allowed to associate with the access point.</p> <ul data-bbox="744 651 1126 708" style="list-style-type: none"><li data-bbox="744 651 1126 708">• No—Do not use this server for MAC-based authentication. <p data-bbox="733 724 1228 781">Click see detail to see for which versions this setting is valid.</p>

Table 3-13 Server-Based Security Settings (continued)

Field	Description
802.1X Protocol Version (For EAP Authentication)	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting. • Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23, or if workgroup bridges associating with this access point use firmware version 8.58 or earlier. • Draft 10—Select this option if client devices that associate with this access point or bridge use Microsoft Windows XP EAP authentication, if LEAP-enabled client devices that associate with this bridge use radio firmware version 4.25 or later, or if workgroup bridges associating with this access point use firmware version 8.65 or later. <p>This is the default setting in access point and bridge firmware versions 11.06 and later.</p>

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Configuring Services

Use this option to configure various system features and support services on the device.

Procedure

-
- Step 1** Select **Services**. The menu expands and the Services dialog box displays in the right pane.
- Step 2** Select one of the following from the Services menu:
- Start-Up—See [Configuring Start-Up Settings, page 3-60](#).
 - Console/Telnet—See [Configuring Console/Telnet Settings, page 3-62](#).
 - Hot Standby—See [Configuring Hot Standby Settings, page 3-64](#).
 - Routing—See [Configuring Routing Settings, page 3-66](#).
 - CDP—See [Configuring CDP Settings, page 3-67](#).
 - DNS—See [Configuring DNS Settings, page 3-68](#).
 - FTP—See [Configuring FTP Settings, page 3-69](#).
 - HTTP—See [Configuring HTTP Settings, page 3-71](#).
 - SNMP—See [Configuring SNMP Settings, page 3-72](#).
 - SNTP—See [Configuring SNTP Settings, page 3-73](#).
 - Accounting—See [Configuring Accounting Settings, page 3-74](#).

Configuring Start-Up Settings

Use this option to configure the access point for your network's BOOTP or DHCP servers for automatic assignment of IP addresses.

Procedure

Step 1 Select **Services > Start-Up**. The Services: Start-Up dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-14 Services Start-Up Settings

Field	Description
Configuration Server Protocol	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • None—Use this setting if your network does not have an automatic system for IP address assignment. • BOOTP—Use this setting if IP addresses are hard-coded based on MAC addresses. • DHCP—Use this setting if IP addresses are “leased” for predetermined periods of time.
Use prior Config Server settings if no server responds?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • yes— Use this setting to have the access point save the boot server's most recent response. • no—Use this setting to not use the most recent response.

Table 3-14 Services Start-Up Settings (continued)

Field	Description
Read “.ini” file from file server?	From the list, select one of the following: <ul style="list-style-type: none"> • always—Use this setting for the access point to always load configuration settings from an .ini file on the server. • never—Use this setting for the access point to never load configuration settings from an .ini file on the server. • if specified by server—Use this setting for the access point to load configuration settings from an .ini file on the server if the server’s DHCP or BOOTP response specifies that an .ini file is available.
BOOTP Server Timeout (sec’s)	Enter the length of time the access point waits to receive a response from a single BOOTP server.
DHCP Multiple-Offer Timeout (sec’s)	Enter the length of time the access point waits to receive a response when there are multiple DHCP servers.
DHCP Requested Lease Duration (min’s)	Enter the length of time the access point requests for an IP address lease from your DHCP server.
DHCP Minimum Lease Duration (min’s)	Enter the shortest amount of time the access point accepts for an IP address lease. The access point ignores leases shorter than this period.
DHCP Class Identifier	Enter the access point’s group name. The DHCP server uses the group name to determine the response to send to the access point.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
-

Configuring Console/Telnet Settings

Use this option to configure the access point to work with a terminal emulator or through Telnet.

Procedure

- Step 1** Select **Services > Console/Telnet**. The Services: Console/Telnet dialog box appears.
- Step 2** Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-15 Services > Console/Telnet Settings

Field	Description
Baud Rate	<p>Enter a rate from 110 to 115,200, expressed in bits per second.</p> <p>The rate you enter is dependent on the capability of the computer you use to open the access point management system.</p>
Parity	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • None—Use this setting to use no parity bit. • Even—Use this setting to make the total number of bits even. • Odd—Use this setting to make the total number of bits odd.
Data Bits	<p>From the list, select one of the data bit settings.</p>
Stop Bits	<p>From the list, select one of the stop bit settings.</p>
Flow Control	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • None—Use this setting to indicate no flow control is used. • SW Xonn/Xoff—Use this setting to indicate the method information is sent between pieces of equipment to prevent loss of data when too much information arrives at the same time on one device.
Terminal Type	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> • teletype—Use this setting if your terminal emulator does not support ANSI. • ANSI—Use this setting to offer graphic features such as reverse video buttons and underlined links.

Table 3-15 Services > Console/Telnet Settings (continued)

Field	Description
Columns (64-132)	Enter a number to define the width of the terminal emulator display within the range of 64 characters to 132 characters.
Lines (16-50)	Enter a number to define the height of the terminal emulator display within the range of 16 characters to 50 characters.
Telnet	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable Telnet access to the management system. • Disable—Use this setting to prevent Telnet access to the management system.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Configuring Hot Standby Settings

Use this option to configure a standby access point as a client device associated to a monitored access point.

Procedure

Step 1 Select **Services > Hot Standby**. The Services: Hot Standby dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Hot Standby Mode	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow hot standby mode. • Disable—Use this setting to disable hot standby mode.
Service Set ID (SSID)	Enter the monitored access point's SSID.
MAC Address for the Monitored AP	Enter the monitored access point's MAC address.
Polling Frequency (1-30)	Enter the number of seconds between each query the standby access point sends to the monitored access point.
Timeout for Each Polling (1-600)	Enter the number of seconds the standby access point should wait for a response from the monitored access point before it assumes that the monitored access point has malfunctioned.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Configuring Routing Settings

Use this option to configure the access point to communicate with the IP network routing system.

Procedure

Step 1 Select **Services > Routing**. The Services: Routing dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Default Gateway	Enter the IP address of your network's default gateway in this entry field. The entry 255.255.255.255 indicates no gateway.
New Network Route	
Destination Network	Enter the IP address of the destination network.
Gateway	Enter the IP address of the gateway used to reach the destination network.
Subnet Mask	Enter the subnet mask associated with the destination network.

Step 3 Click **Add** to add an additional network route for the access point.

Step 4 To remove a network route, select it from the list, then click **Remove**.

- Step 5** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Configuring CDP Settings

Use this option to enable, disable, or adjust the access point's CDP settings.

Procedure

Step 1 Select **Services > CDP**. The Services: CDP dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Cisco Discovery Protocol (CDP)	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to enable CDP. • Disable—Use this setting to disable CDP.
Packet Hold Time	Enter the number of seconds other CDP-enabled devices should consider the access point's CDP information valid.
Packet Sent Every	Enter the number of seconds between each CDP packet the access point sends. This value should always be less than the packet hold time.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
-

Configuring DNS Settings

Use this option to configure the access point to work with your network's Domain Name System (DNS) server.

Procedure

Step 1 Select **Services > DNS**. The Services: DNS dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-16 Services > DNS Settings

Field	Description
Domain Name System (DNS)	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this option if your network DNS. • Disable—Use this option if you network does not use DNS.
Default Domain	Enter the name of your network's IP domain. Your entry might look like this: mycompany.com

Table 3-16 Services > DNS Settings (continued)

Field	Description
Domain Name Servers	Enter the IP addresses of up to three domain name servers on your network.
Domain Suffix	Enter the portion of the full domain name that you would like omitted from access point displays. For example, the full name of a computer might be “mycomputer.mycompany.com.” If you set the domain suffix to “mycompany.com,” the computer’s name would be displayed as “mycomputer.”

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Configuring FTP Settings

Use this option to configure File Transfer Protocol settings for the access point. All non-browser file transfers are governed by these settings.

Procedure

Step 1 Select **Services > FTP**. The Services: FTP dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-17 Services > FTP Settings

Field	Description
File Transfer Protocol (FTP)	From the list select one of the following: <ul style="list-style-type: none"> • TFTP • FTP
Default File Server	Enter the IP address or DNS name of the file server where the access point should look for FTP files.
FTP Directory	Enter the file server directory that contains the firmware image files.
FTP User Name	Enter the username assigned to your FTP server. You do not need to enter a name in this field if you selected TFTP.
FTP User Password	Enter the password associated with the file server's username. You do not need to enter a password in this field if you selected TFTP.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Configuring HTTP Settings

Use this option to configure HTTP settings for the access point.

Procedure

Step 1 Select **Services > HTTP**. The Services: HTTP dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Allow Non-Console Browsing	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow browsing to the management system. • Disable—Use this setting to make the management system accessible only through the console and Telnet interfaces.
HTTP Port	Enter the port through which the access point provides web access.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Configuring SNMP Settings

Use this option to configure settings for notifications to be sent to an SNMP server.

Procedure

Step 1 Select **Services > SNMP**. The Services: SNMP dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Simple Network Management Protocol (SNMP)	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to allow event notifications to be sent to an SNMP server. • Disable—Use this setting to not allow event notifications to be sent to an SNMP server.
SNMP Trap Destination	Enter the IP address or the host name of the server running the SNMP Management software.
SNMP Trap Community	Enter the SNMP community name.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-88](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

Configuring SNTP Settings

Use this option to configure time server settings.

Procedure

Step 1 Select **Services > SNTP**. The Services: SNTP dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Simple Network Time Protocol (SNTP)	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting if your network uses Simple Network Time Protocol. • Disable—Use this setting if your network does not use Simple Network Time Protocol.
Default Time Server	Enter enter the server's IP address.
GMT Offset (hr)	From the list, select the time zone in which the access point operates.
Use Daylight Savings Time	From the list, select one of the following: <ul style="list-style-type: none"> • Enable—Use this setting to have the access point automatically adjust to Daylight Savings Time. • Disable—Use this setting to not have the access point automatically adjust to Daylight Savings Time.

- Step 3** Select one of the following in the left pane:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
 - **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
 - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
-

Configuring Accounting Settings

Use this option to configure settings that enable you to send network accounting information about wireless client devices to a RADIUS server on your network.

Procedure

Step 1 Select **Services > Accounting**. The Services: Accounting dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-18 Accounting Settings

Field	Description
Enable accounting	From the list, select one of the following: <ul style="list-style-type: none"> • enable—Use this setting to turn on accounting for your wireless network. • disable—Use this setting to turn off accounting for your wireless network
Enable delaying to report STOP	<ul style="list-style-type: none"> • enable—Use this setting to delay sending a stop report to the server when a client device disassociates from the access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate. • disable—Use this setting to not delay sending a stop report to the server when a client device disassociates from the access point.
Minimum delay time to report STOP (sec)	Enter the number of seconds the access point waits before sending a stop report to the server when a client device disassociates from the access point.
Server Name/IP	Enter the name or IP address of the server to which the access point sends accounting data.
Server Type	Select RADIUS from the list. (Additional types may be added in future software releases.)
Port	Enter the communication port setting used by the access point and the server. The default setting, 1813, is the correct setting for Cisco Aironet access points and Cisco secure ACS.

Table 3-18 Accounting Settings (continued)

Field	Description
Shared Secret	Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.
Time Out (sec's)	Enter the number of seconds the access point should wait before authentication fails. If the server does not respond within this time, the access point tries to contact the next defined authentication server.
Enable Update	From the list, select one of the following: <ul style="list-style-type: none"> • enable—Use this setting to allow accounting update messages for wireless clients. With updates enabled, the access point sends an accounting start message when a wireless client associates to the access point, sends updates at regular intervals while the wireless client is associated to the access point, and sends an accounting stop message when the client disassociates from the access point. • disable—Use this setting to not allow accounting update messages. With updates disabled, the access point sends only accounting start and accounting stop messages to the server.
Update Delay (sec's)	Enter the update interval in seconds. If you use 360, the access point sends an accounting update message for each associated client device every 6 minutes.

Table 3-18 Accounting Settings (continued)

Field	Description
Use this server for	
EAP Authentication	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this server for EAP authentication. In this type of authentication, the access point relays authentication messages between the server and the authenticating client device. <ul style="list-style-type: none"> • No—Do not use this server for EAP authentication.
non-EAP Authentication	From the list, select one of the following: <ul style="list-style-type: none"> • Yes—Use this server for non-EAP authentication. • No—Do not use this server for non-EAP authentication.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Configuring Events

This option enables to you to customize the display of access point events (alerts, warnings, and normal activity).

Procedure

- Step 1** Select **Events**. The menu expands and the Events dialog box displays in the right pane.
- Step 2** Select one of the following from the Events menu:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Event Handling—See [Configuring Event Handling, page 3-78](#).
 - Event Notifications—See [Configuring Event Notification, page 3-83](#).
-

Configuring Event Handling

The event settings control how events are handled by the access point: counted, displayed in the log, recorded, or announced in a notification. The settings are color coded: red for fatal errors, magenta for alerts, blue for warnings, and green for information.

Procedure

- Step 1** Select **Events > Event Handling**. The Events: Event Handling dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-19 Event Handling Settings

Field	Description
System Fatal	From the list, select one of the following: <ul style="list-style-type: none"> • Count—Use this option to tally the total events occurring in this category without any form of notification or display. • Display Console—Use this option to provide a read-only display of the event but not record it. • Record—Use this option to make a record of the event in the log and provide a read-only display of the event. • Notify—Use this option to makes a record of the event in the log, display the event, and tell the access point to notify someone of the occurrence.
Protocol Fatal	
Network Port Fatal	
System Alert	
Protocol Alert	
Network Port Alert	
External Alert	
System Warning	
Protocol Warning	
Network Port Warning	
External Warning	
System Information	
Protocol Information	
Network Port Information	
External Information	

Table 3-19 Event Handling Settings (continued)

Field	Description
Handle Alerts as Severity Level	<p data-bbox="736 293 1197 321">From the list, select one of the following:</p> <ul data-bbox="744 337 1231 1138" style="list-style-type: none"> <li data-bbox="744 337 1193 423">• systemFatal—Indicates an event that prevents operation of the device as a whole. <li data-bbox="744 444 1231 565">• protocolFatal—Indicates an event that prevents operation of a specific communications protocol in use, such as HTTP or IP. <li data-bbox="744 586 1193 672">• portFatal—Indicates an event that prevents operation of the Ethernet or radio network interface. <li data-bbox="744 693 1231 779">• systemAlert—Indicates that you need to take action to correct a condition on the device as a whole. <li data-bbox="744 800 1231 920">• protocolAlert—Indicates that you need to take action to correct a condition on a specific communications protocol in use, such as HTTP or IP. <li data-bbox="744 941 1231 1027">• portAlert—Indicates that you need to take action to correct the condition on the Ethernet or radio network interface. <li data-bbox="744 1049 1231 1138">• externalAlert—Indicates that you need to take action to correct the condition on a device on the network.

Table 3-19 Event Handling Settings (continued)

Field	Description
	<ul style="list-style-type: none"> <li data-bbox="744 293 1229 380">• <code>systemWarning</code>—Indicates that an error or failure may have occurred on the device as a whole. <li data-bbox="744 402 1229 521">• <code>protocolWarning</code>—Indicates that an error or failure may have occurred on a specific communications protocol in use, such as HTTP or IP. <li data-bbox="744 544 1229 630">• <code>portWarning</code>—Indicates that an error or failure may have occurred on an Ethernet or radio network interface. <li data-bbox="744 652 1229 738">• <code>externalWarning</code>—Indicates that an error or failure may have occurred on a device. <li data-bbox="744 761 1229 816">• <code>systemInfo</code>—Notification that some sort of event has occurred on a device. <li data-bbox="744 839 1229 958">• <code>protocolInfo</code>—Notification that some sort of event has occurred on a communications protocol in use, such as HTTP or IP. <li data-bbox="744 980 1229 1066">• <code>portInfo</code>—Notification that some sort of event has occurred on an Ethernet or radio network interface. <li data-bbox="744 1089 1229 1144">• <code>externalInfo</code>—Notification that some sort of event has occurred on a device.

Table 3-19 Event Handling Settings (continued)

Field	Description
Maximum Number of Bytes Stored per Alert Packet (0- 2312)	<p>Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled.</p> <p>If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event.</p> <p>Note Changing this setting may cause the access point to reboot.</p>
Maximum Memory Reserved for Detailed Event Trace Buffer (bytes) (0-8388608)	<p>Enter the number of bytes reserved for the Detailed Event Trace Buffer.</p> <p>The Detailed Event Trace Buffer is a tool for tracing the contents of packets between specified stations on your network.</p> <p>Note Changing this setting may cause the access point to reboot.</p>

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Configuring Event Notification

Use this option to enable and configure notification of fatal, alert, warning, and information events to destinations external to the access point, such as an SNMP server or a Syslog system.

Procedure

Step 1 Select **Events > Event Notification**. The Events: Event Notification dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-20 Events > Event Notification Settings

Field	Description
Should Notify-Disposition Events generate SNMP Traps?	From the list, select one of the of the following: <ul style="list-style-type: none"> • Yes—Use this option to send event notifications to an SNMP server. • No—Use this option if you do not want to send notifications to an SNMP server.
SNMP Trap Destination	Enter the IP address or the host name of the server running the SNMP Management software.
SNMP Trap Community	Enter the SNMP community name.
Should Notify-Disposition Events generate Syslog Messages?	From the list, select one of the of the following: <ul style="list-style-type: none"> • Yes—Use this option to send event notifications to a Syslog server. • No—Use this option if you do not want to send notifications to a Syslog server.

Table 3-20 Events > Event Notification Settings (continued)

Field	Description
Syslog Destination Address	Enter the IP address or the host name of the server running Syslog.
Syslog Facility Number	Enter the Syslog Facility number for the notifications.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Configuring Custom Values

This option enables to you to enter custom values that might not be available in the Template Menu. It also allows you to quickly enter a value, if you know the exact value you want to change, instead of going through the menu. (See [Examples, page 3-85.](#))



Note

This option should be used only by advanced users who have a good understanding of the MIB variables they are setting.

Templates with custom key values are not validated.

Procedure

Step 1 Select **Configure > Templates > Custom Values**. The Custom Values dialog box appears.



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Step 2 Complete the following:



Note You must enter the exact syntax for the setting to work properly.

Field	Description
Key	Enter a valid MIB key. (See Examples, page 3-85.)
Value	Enter a valid MIB value. (See Examples, page 3-85.)

Step 3 Click **Add** to add the custom value to the list.



Note If the custom value you enter is the same as an existing one in the Template Menu, the custom value will override the value in the menu.

Step 4 To remove a custom value, select it from the list, then click **Remove**.

Step 5 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-88.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-88.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

Examples

Following are examples of custom key values that can be entered:

- Set system contact on access points.

- **Key:** sysContact.0
 - **Value:** ABC, XYZ Inc.
- Set system location for access points.
 - **Key:**sysLocation.0
 - **Value:** Bldg ABC, XYZ Inc.
- Set up a user for an access point
 - **Key:**userMgrUserName.x
 - **Value:** testUser
 - **Key:**userMgrPassword.x
 - **Value:** testPassword
 - **Key:**userMgrCapabilities.x
 - **Value:** 20

where:

- x is the next available index in the user manager table (userMgrConfig Table)
 - Capabilities are the sum of any of the following: 0=none; 1=Administrator; 2=Write; 4=Firmware Update; 8=Identity Update; 16=SNMP Community
- Reboot an access point.
 - **Key:**tsMsgSend0
 - **Value:** 2

- Classify workgroup bridges as network infrastructure
 - **Key:**awcDot11DesiredSSIDInfrastructureWGB.2
 - **Value:** false

where the possible values are T (true) and F (false)

- Set the DHCP Client Identifier Type
 - **Key:**bootconfigDhcpClientIdType
 - **Value:** ethernet10Mb

where the possible values are text or numeric:

- ethernet10Mb or 1
 - experimentalEthernet3Mb or 3
 - amateurRadioAxDot25 or 3proteonProNetTokenRing or 4
 - chaos or 5
 - ieee802Networks or 6
 - arcnet or 7
 - hyperchannel or 8
 - lanstar or 9
 - autonet or 10
 - localTalk or 11
 - localNet or 12
 - nonHardware or 128
- Set the DHCP client Identifier Value
 - **Key:** bootconfigDhcpClientIdValue
 - **Value:** 22

- Is MAC alone sufficient for to be fully authenticated
 - **Key:** awcFtEnableMacOrEapAuth
 - **Value:** F

where the possible values are T (true) and F (false)
- Set Rogue AP alert timeout (minutes)
 - **Key:** awcFtRogueApAlertTimeout
 - **Value:** 29
- Use symbol extensions
 - **Key:** awcDot11SymbolExtensionsEnabled.2
 - **Value:** 2

where the possible values are T (true) and F (false)

Previewing the Template

Procedure

-
- Step 1** Click **Preview**. A window displays the configuration choices you have made to the template.
- Step 2** Click **Finish**. (See [Finishing the Template, page 3-88.](#))
-

Finishing the Template

Procedure

-
- Step 1** Click **Finish** in the left pane to complete creating a template. The Finish dialog box appears in the right pane.



Note It is recommended that you always validate the template before saving it.

- Step 2** Click **Validate** if you want to check the template configuration. A window displays a message indicating for which devices and versions the configuration template you just created is valid.



Note Templates containing custom key values are not validated.

- Step 3** Check **Enable Version Check** if you want the system to make sure you apply the templates only to devices with valid versions.

If you do not enable the version check, templates will be applied to devices even when the configuration is not valid for the device version.

- Step 4** Click **Save** to create the template. The screen refreshes and the template name appears in the Existing Templates listbox.
-

Creating a Template

Use this option to create a configuration template.



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Enter a unique name. (See [Naming Guidelines, page A-1](#) for details.)
- Step 3** Click **Create New**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.
- Step 4** Select the choices in the left pane to create a configuration template. For a description, see [Template Choices, page 3-2](#).
-

Copying a Template

Use this option to copy a configuration template that you can use as a base for another template.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
 - Step 2** Select the template you want to copy from the Existing Templates box, then click **Create Copy**. A dialog box appears asking you to enter a name for the copy.
 - Step 3** Enter a unique name. (See [Naming Guidelines, page A-1](#) for details.)
 - Step 4** Click **OK**. The Templates window refreshes and the new name appears in the Existing Templates list.
 - Step 5** Click **Edit**. (See [Editing a Template, page 3-90](#).)
-

Editing a Template

Use this option to edit a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
 - Step 2** Select the template you want to edit from the Existing Templates box, then click **Edit**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.

- Step 3** Select the choices in the Template Menu to create a configuration template. For a description, see [Template Choices, page 3-2](#).
-

Deleting a Template

Use this option to delete a configuration template.

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select the template you want to delete from the Existing Templates box, then click **Delete**. A window appears asking if you want to delete the template.
- Step 3** Click **OK** to delete it.
-

Managing Configuration Jobs

This window allows you view a list of all the jobs in their various states. It also allows you to create, edit, and filter, and undo configuration jobs.

The topics covered in this section are:

- [Creating a Configuration Job, page 3-98](#)
- [Viewing Configuration Job Status, page 3-98](#)
 - [Filtering a Job, page 3-101](#)
 - [Editing a Job, page 3-101](#)
 - [Deleting a Job, page 3-102](#)
 - [Stopping a Job, page 3-102](#)
 - [Viewing Job Run Details, page 3-102](#)

Related Topic

[Using the Templates, page 3-1.](#)

Job Choices

When you create or edit a configuration job, the following choices appear in the left pane of the Jobs window:

**Note**

These are steps that must be completed but do not have to be done in order.

1. **Job Name**—See [Naming the Job, page 3-92](#).
2. **Select Devices**—See [Naming the Job, page 3-92](#).
3. **Select Template**—See [Selecting a Template, page 3-94](#).
4. **Schedule Job**—See [Scheduling a Job, page 3-96](#).

**Caution**

Clicking on another tab before you have saved your entries in this window will cause the window to reset and you will lose all the information you entered.

Naming the Job

Procedure

-
- Step 1** Click **Job Name**. The Job Name dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 3-21 Job Name

Field	Description
Job Name	Enter a name for the job. See Naming Guidelines, page A-1 .
Description	Enter a description of the job. See Naming Guidelines, page A-1 .
Protocol	Select the type of protocol used: HTTP or SNMP. Note If you select SNMP, you will not be able to use the Undo feature; it is only supported for HTTP-based configuration jobs.

Step 3 From the menu in the left pane, go to the next step, Select Devices. (For additional information, see [Selecting Devices, page 3-93](#).)

Selecting Devices

Procedure

Step 1 Click **Select Devices**. The Select window appears.



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

- Step 2** From the device selector, click the folder from which you want to build a device list.
- Clicking the folder displays the folder's contents in the All Available Devices list box.
- Repeat this step as many times as necessary to select devices from the folder in which they reside.
- Step 3** From the All Available Devices list, select folders or individual devices, then click **Add**. The devices appear in the Selected Devices list box.



Note If you select a folder, the template will be applied to all of the devices in that folder. If a device is subsequently added to the folder, the template is applied to that device.

- Step 4** To remove devices, select them from the Devices in Group list, then click **Remove**.
- Step 5** From the menu in the left pane, go to the next step, Select Template. (For additional information, see [Selecting a Template, page 3-94](#).)
-

Selecting a Template

Procedure

- Step 1** Click **Select Template**. The Select Template window appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 3-22 *Select Template*

Field	Description
Configuration Template	From the list, select the template which you want to apply to the devices.
Details	
Name	Displays the name of the selected template.
Device Types	Displays the device types that are valid for the selected template.
Device Versions	Displays the device versions for the device types listed in the Device Type field. Each device type's valid versions are displayed in sequence and grouped using parentheses.
Description	Displays the template description.
Version Check Enabled	Indicates whether the version check is enabled. (The check is enabled using the Finish step in the Template Menu.)

Step 3 From the menu in the left pane, go to the next step, Schedule Job. (For additional information, see [Scheduling a Job](#), page 3-96.)

Scheduling a Job

Procedure

Step 1 Click **Schedule Job**. The Schedule Job dialog box appears.

Step 2 Complete the following:



Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 3-23 *Schedule Job*

Field	Description
Run Now	Click to run the job. (The job begins running in 2 minutes.) Note This option ignores any dates you have entered in Start Date and Start Time.
Start Date	From the lists, select the month, day, and year you want your job to run.
Start Time	From the list, select the hour and minutes of the day you want your job to run.
Repeat	
Enable	Check to run the job repeatedly.
Every	Indicate how often you want the job to repeat by entering a numerical value, then selecting an interval of time: Hours, Days, Months, or Years.

Step 3 From the menu in the left pane, go to the next step, Finish. (For additional information, see [Finishing Scheduling, page 3-97](#).)



Tip You can stop a running job by clicking **Stop Job**.

Finishing Scheduling

Procedure

Step 1 Click **Finish** in the left pane to complete creating a job. The Finish dialog box appears in the right pane.

Step 2 Do one of the following:



Note It is recommended that you always validate the job before saving it.

- Click **Validate** if you want to check the job.

A window displays a confirmation message if the job is successful, and an informational message if the selected template in the job is not valid for the selected devices.



Note Jobs with templates containing custom key values are not validated.

- Click **Save** to create the job. The screen refreshes and
 - The job name appears in the Scheduled Jobs list.
 - A confirmation window appears with the job summary.
-

Creating a Configuration Job

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Configure > Jobs**. The Jobs window appears.
- Step 2** Enter a name for the job. See [Naming Guidelines, page A-1](#).
- Step 3** Click **Create Job**. The window refreshes with Job Creation menu in the left pane and the Job Name dialog box in the right pane.
- Step 4** Select the numbered choices in the left pane to create a job. For a description, see [Job Choices, page 3-92](#).

Viewing Configuration Job Status

This window allows you to view job status. It also allows you to filter a job, edit a job, view details about the job and undo a job.

Device data is polled every 15 minutes by default, and the duration that job data is retained is 30 days. To change either default, see [Managing System Parameters, page 5-58](#).

The topics covered in this section are:

- [Viewing the Job State, page 3-99](#)
- [Filtering a Job, page 3-101](#)
- [Editing a Job, page 3-101](#)
- [Deleting a Job, page 3-102](#)
- [Stopping a Job, page 3-102](#)
- [Viewing Job Run Details, page 3-102](#)

**Note**

Your login determines whether you can use this option.

Related Topic

[Using the Templates, page 3-1](#)

Viewing the Job State**Procedure**

Step 1 From the Job State list, select the type of job whose status you want to check. The window refreshes and the jobs are displayed.

The tables vary depending on which type of Job State you selected: [Scheduled and Unscheduled](#), [Running](#), or [All](#):

- Scheduled and Unscheduled

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.
Last Run Status	The status of the last run.

- Running

**Tip**

You can stop a running job by clicking **Stop Job**.

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job Start Time	The time the job started.

Field	Description
Percent Complete	The percent of the job that has completed running.
Next Schedule	The next time the job is scheduled to run.

- All

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job State	The state of the job. Note A job in a DidNotStart state must be rescheduled.
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.
Last Run Status	The status of the job the last time it run.

Step 2 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 3 You can do any of the following:

- Filter the job—See [Filtering a Job, page 3-101](#).
- Edit the job—See [Editing a Job, page 3-101](#).
- Delete the job—See [Deleting a Job, page 3-102](#),
- Stop a job—See [Stopping a Job, page 3-102](#).
- View the run details—See [Viewing Job Run Details, page 3-102](#).
- Refresh the screen—Click **Refresh**.

Filtering a Job

Use this option to filter jobs from the displayed list. Filtering this way allows you to display a limited set of jobs, making it easier to search for a particular job if you know the name.

Procedure

- Step 1** Click **Filter Job**. The Filter Job dialog box appears.
- Step 2** Enter the name, or part of the a name, on which to filter. (Use % as a wildcard to filter jobs. For example, entering %name% will filter all the jobs that contain "name.")
- Step 3** Click **Apply filter**. The Job window refreshes and the matching jobs are displayed on the Jobs list.



Note The filter is only applied until the page is refreshed.

Editing a Job

Use this option to edit jobs from the displayed list of jobs.

Procedure

- Step 1** Select the job from the list which you would like to edit.
- Step 2** Click **Edit**. The Job Name dialog box appears.
- Step 3** Select the choices in the Template Menu to create a configuration template. For a description, see [Job Choices, page 3-92](#).
-

Deleting a Job

Use this option to delete jobs from the displayed list of jobs. Jobs that are scheduled, unscheduled, completed and did not start can be deleted. Jobs that are running cannot be deleted; they can be stopped.

Procedure

- Step 1** Select the job from the list which you would like to edit.
 - Step 2** Click **Delete**.
-

Stopping a Job

Use this option to stop a job when it is in a running state.

Procedure

- Step 1** Select the job from the list which you would like to stop.
 - Step 2** Click **Stop Job**. A window displays to confirm that you want to stop the job.
 - Step 3** Click **OK**, and the job stops.
-

Viewing Job Run Details

Use this option to view details about a job, or to undo a job from the displayed list of jobs.

Procedure

- Step 1** From the All Jobs table displayed in **Configure > Jobs** window, select a job for which you would like to see details, then click **Job Run Detail**.

Step 2 The details window appears with the Job Runs table:

Field	Description
Select Run	Used to select a job for which you want to see more details.
Job Start Time	The time the job started.
Job End Time	The time the job ended.
Job Status	The status of the job.
Percent Complete	The percent of the job that completed.

Step 3 Do any of the following:

- To view details for a particular job run or to undo a job, select the job, then click **Show Run Details**. The Job Run details table displays the information. (See [Viewing the Job Run Details Table, page 3-103](#).)
- To view the job run log, click **Job Run Log**. A window displays all the details for the selected job number.
- To refresh the table, click **Refresh**.

Viewing the Job Run Details Table

The Job Runs Details table displays the following information:

Field	Description
Device Name	The name of the device.
Start Time	The time the job started.
End Time	The time the job ended.
Status	The status of the job.

- To sort table data, click on the column heading by which you want to sort the data:
 - A triangle indicates ascending order.
 - An upside-down triangle indicates descending order.
 - No triangle indicates that the data is not sorted.
- To select all the jobs in the table, click **Select All**.
- To deselect all the jobs in the table, click **DeSelect All**.



Note If you have multiple screens, you must Select All or DeSelect All one screen at a time.

- To undo the selected configuration job, click **Undo**.
The Undo feature is supported only for HTTP-based configuration jobs (not SNMP-based configurations jobs). It is not supported for:
 - Custom Values
 - Security options: Local Admin Authentication under the Local Admin Access; Encryption Key Values under Local AP/Client Security; Shared Secret under Server-Based Security; and Shared Secret under Accounting.
 - FTP username and password
 - Previously undone jobs

