



## 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 3-137](#).
- **Auto Update**—See [Automating Configurations, page 3-151](#).

## 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 3-132](#)
- [Copying a Template, page 3-133](#)
- [Editing a Template, page 3-134](#)
- [Deleting a Template, page 3-134](#)

- [Importing a Template](#), page 3-135
- [Exporting a Template](#), page 3-137

**Related Topic**

[Managing Configuration Jobs](#), page 3-137

## 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 3-8.
  - **Ethernet**—See [Configuring the Ethernet Port](#), page 3-49.
  - **11b Radio**—See [Configuring the 11b Radio](#), page 3-56.
  - **11a Radio**—See [Configuring the 11a Radio](#), page 3-73.
  - **Security**—See [Defining the Security Settings](#), page 3-92.
  - **Services**—See [Configuring Services](#), page 3-102.
  - **Events**—See [Configuring Events](#), page 3-124.
  - **Custom Values**—See [Configuring Custom Values](#), page 3-130.
3. **Preview**—See [Previewing the Template](#), page 3-131.
  4. **Finish**—See [Finishing the Template](#), page 3-132.

## 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 <a href="#">Naming Guidelines, page A-1</a> .
Description	Enter a description of the purpose of the template. See <a href="#">Naming Guidelines, page A-1</a>

**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
Reboot Device	From the list, select Yes if you want to allow device reboots.
SysName	Enter a system name.  The system name appears in the titles of the management system pages and in the access point's Association Table page.  This is not an essential setting, but it helps identify the access point on your network.
SysLocation	Enter the system's location.  This is not an essential setting, but it helps identify the access point on your network.
SysContact	Enter a contact name.  This is not an essential setting but it helps identify the person responsible for the access point on your network.

**Table 3-1 Express Template Settings (continued)**

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"> <li>• None-Static IP—Use this if your network does not have an automatic system for IP address assignment.</li> <li>• BOOTP—Use this if your network uses Bootstrap Protocol, in which IP addresses are hard-coded based on MAC addresses.</li> <li>• DHCP—Use this if your network uses Dynamic Host Configuration Protocol, in which IP addresses are “leased” for predetermined periods of time.</li> </ul>
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>
Default Gateway	<p>Enter the IP address of your default Internet gateway.</p> <p>The entry 255.255.255.255 indicates no gateway.</p>

**Table 3-1 Express Template Settings (continued)**

Field	Description
Radio Service Set ID (SSID)	<p data-bbox="733 293 1170 350">Enter any alphanumeric, case-sensitive string, from 2 to 32 characters long.</p> <p data-bbox="733 370 1231 553">The SSID is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity and provides access to VLANs by wireless client devices.</p> <p data-bbox="733 573 1157 630">Several access points on a network or subnetwork can share an SSID.</p>

**Table 3-1 Express Template Settings (continued)**

Field	Description
Role in Network	<p data-bbox="736 293 1197 321">From the list, select one of the following:</p> <ul data-bbox="744 337 1228 1317" style="list-style-type: none"> <li data-bbox="744 337 1210 423">• Access Point—Use this setting if the access point is connected to the wired LAN.</li> <li data-bbox="744 448 1224 501">• Repeater—Use this setting for access points not connected to the wired LAN.</li> <li data-bbox="744 526 1224 704">• 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.</li> <li data-bbox="744 729 1228 878">• 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.</li> <li data-bbox="744 902 1224 1081">• 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).</li> <li data-bbox="744 1105 1228 1317">• 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).</li> </ul>

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

**Step 2** Select one of the following:

- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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—See [Defining Spanning Tree Protocol, page 3-9](#).
  - Address Filters—See [Defining Address Filters, page 3-12](#).
  - Ethertype Filters—See [Defining Ethertype Filters, page 3-14](#).
  - IP Protocol Filters—See [Defining IP Protocol Filters, page 3-18](#).
  - IP Port Filters—See [Defining IP Port Filters, page 3-23](#).
  - Policy Groups—See [Configuring Policy Groups, page 3-28](#).
  - VLANs—See [Configuring VLANs, page 3-31](#).
  - Quality of Service—See [Configuring Quality of Service, page 3-36](#).
  - Service Sets—See [Configuring Service Sets, page 3-38](#).
  - Advanced—See [Defining Advanced Associations, page 3-42](#).
  - Port Assignments—See [Configuring Port Assignments, page 3-47](#).
  - DSCP to CoS—See [Configuring DSCP to CoS, page 3-48](#).
- 

## 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"> <li>• Enable—Use this setting to enable STP on the bridge.</li> <li>• Disable—If you do not want STP enabled the bridge.</li> </ul>
Always Unblock Ethernet when STP is disabled	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to maintain a bridge link when STP is disabled</li> <li>• No—Use this setting to not maintain a bridge link when STP is disabled.</li> </ul> <p>Click <b>see details</b> to see which versions this setting is valid for.</p>
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 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>

**Table 3-2 Spanning Tree Protocol Settings (continued)**

Field	Description
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)	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.
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)	<p>Enter a number to indicate the relative efficiency of a port's network link.</p> <p>A port with a high path cost is less likely to become a bridge's root port.</p>
Priority (0-255)	<p>Enter a number to influence whether STP designates a port as a bridge's root port.</p> <p>A port with a low priority setting is more likely to become a bridge's root port.</p>
Enable	<p>From the list, select one of the following for each port configured:</p> <ul style="list-style-type: none"> <li>• Enable—Use this setting to indicate whether the port participates in STP. (This determines whether the port blocks or forwards traffic.)</li> <li>• Disable—Use this setting to indicate that the port does not participate in STP.</li> </ul>

- Step 4** Select one of the following:
- **Preview** to see your changes before you apply them. (See [Previewing the Template, page 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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
Lookup MAC address on Authentication Server if not in an Existing Filter List?	<p>Click one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to allow looking up a MAC address on the authentication server.</li> <li>• No—Use this setting to disallow looking up a MAC address.</li> </ul>
Is MAC Authentication alone sufficient for a client to be fully authenticated?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to specify that client devices that associate to the access point using 802.11 open authentication, first attempt MAC authentication.</li> <li>• No—Use this setting to specify that MAC authentication alone is not sufficient.</li> </ul> <p>Click <b>see details</b> to see which versions this setting is valid for.</p>
New Destination MAC Address	<p>Enter a destination MAC address by entering the address in one of the following ways:</p> <ul style="list-style-type: none"> <li>• With colons separating the character pairs (00:40:96:12:34:56, for example)</li> <li>• Without any intervening characters (004096123456, for example)</li> </ul>
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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-14.](#)
- Delete the Filters—See [Deleting Ethertype Filters, page 3-16.](#)

Using this option you can also:

- Create Special Cases—See [Creating Special Cases, page 3-16.](#)
- Delete Special Cases—See [Deleting Special Cases, page 3-18.](#)

### Creating New Ethertype Filters

#### Procedure

---

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



**Note** Refer to the following URL for a list of Ethertype protocols:  
[http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo\\_350/accsspts/ap350scg/ap350axb.htm#85314](http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350axb.htm#85314)

---

**Table 3-3** *Creating New Ethertype Filters Settings*

Field	Description
Add New Ethertype Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See <a href="#">Naming Guidelines, page A-1</a> .
Default Disposition	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Forward—Use this setting to forward protocol traffic.</li> <li>• Block—Use this setting to block protocol traffic.</li> </ul>
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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - 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"> <li>• Default—Use the disposition you set for the Ethertype filter.</li> <li>• Forward—Use this setting to forward protocol traffic.</li> <li>• Block—Use this setting to block protocol traffic.</li> </ul>

**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"> <li>• Default—This setting is the same as best effort, which applies to normal LAN traffic.</li> <li>• 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.</li> <li>• Excellent Effort—Use this setting for a network’s most important users.</li> <li>• Controlled Load—Use this setting for important business applications that are subject to some form of admission control.</li> <li>• Interactive Video—Use this setting for traffic with less than 100 ms delay.</li> <li>• Interactive Voice—Use this setting for traffic with less than 10 ms delay.</li> <li>• Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.</li> </ul>
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"> <li>• yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point.</li> <li>• no—Use this setting to not send an alert to the event log.</li> </ul>

**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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-19.](#)
  - Delete the filters—See [Deleting IP Protocol Filters, page 3-20.](#)

Using this option you can also:

- Create Special Cases —See [Creating Special Cases, page 3-21](#).
- Delete Special Cases—See [Deleting Special Cases, page 3-23](#).

## Creating New IP Protocol Filters

### Procedure

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



**Note** Refer to the following URL for a list of IP protocols:  
[http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo\\_350/acc/sspts/ap350scg/ap350axb.htm#85314](http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/acc/sspts/ap350scg/ap350axb.htm#85314)

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 <a href="#">Naming Guidelines, page A-1</a> .
Default Disposition	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Forward—Use this setting to forward protocol traffic.</li> <li>• Block—Use this setting to block protocol traffic.</li> </ul>
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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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.
Disposition	From the list, select one of the following: <ul style="list-style-type: none"><li>• Default—Use the disposition you set for the protocol filter.</li><li>• Forward—Use this setting to forward traffic.</li><li>• Block—Use this setting to block traffic.</li></ul>

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

Field	Description
Priority	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Default</b>—This setting is the same as best effort, which applies to normal LAN traffic.</li> <li>• <b>Background</b>—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.</li> <li>• <b>Excellent Effort</b>—Use this setting for a network's most important users.</li> <li>• <b>Controlled Load</b>—Use this setting for important business applications that are subject to some form of admission control.</li> <li>• <b>Interactive Video</b>—Use this setting for traffic with less than 100 ms delay.</li> <li>• <b>Interactive Voice</b>—Use this setting for traffic with less than 10 ms delay.</li> <li>• <b>Network Control</b>—Use this setting for traffic that must get through to maintain and support the network infrastructure.</li> </ul>
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"> <li>• <b>yes</b>—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point.</li> <li>• <b>no</b>—Use this setting to not send an alert to the event log.</li> </ul>

- 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-24.](#)
  - Delete the filters—See [Deleting Port Filters, page 3-25.](#)

Using this option you can also:

- Create Special Cases —See [Creating Special Cases, page 3-26](#).
- Delete Special Cases—See [Deleting Special Cases, page 3-28](#).

## Creating New Port Filters

### Procedure

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



**Note** Refer to the following URL for a list of IP port protocols:  
[http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo\\_350/acc\\_sspts/ap350scg/ap350axb.htm#85314](http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/acc_sspts/ap350scg/ap350axb.htm#85314)

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 <a href="#">Naming Guidelines, page A-1</a> .
Default Disposition	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Forward—Use this setting to forward traffic.</li> <li>• Block—Use this setting to block traffic.</li> </ul>
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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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"> <li>• Default—Use the disposition you set for the port filter.</li> <li>• Forward—Use this setting to forward protocol traffic.</li> <li>• Block—Use this setting to block protocol traffic.</li> </ul>

**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"> <li>• Default—This setting is the same as best effort, which applies to normal LAN traffic.</li> <li>• 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.</li> <li>• Excellent Effort—Use this setting for a network's most important users.</li> <li>• Controlled Load—Use this setting for important business applications that are subject to some form of admission control.</li> <li>• Interactive Video—Use this setting for traffic with less than 100 ms delay.</li> <li>• Interactive Voice—Use this setting for traffic with less than 10 ms delay.</li> <li>• Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.</li> </ul>
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"> <li>• yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point.</li> <li>• no—Use this setting to not send an alert to the event log.</li> </ul>

- 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
- 

### Configuring Policy Groups

Policy groups are used to configure access parameters to a logical group of stations in a consistent manner from a single place. For example, protocol filters can be applied to frames for a selected group of stations.

### Procedure

- Step 1** Select **Association > Policy Group**. The Association: Policy Group dialog box appears.
- Step 2** Click **see details** to see which versions this option is valid for.



**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 3** Using this option you can:
- Add and delete a policy group—See [Adding or Deleting a New Policy Group, page 3-29](#).
  - Delete an exiting Policy Group From a Device—See [Deleting an Existing Policy Group from a Device, page 3-30](#).

### Adding or Deleting a New Policy Group

- Step 1** To add a new policy group, enter the following:

Field	Description
GroupID	Enter an identification number for the policy group.
Group Name	Enter a name for the policy group.
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .
IP Protocol	

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

**Step 2** Click **Add** to add the group to the Policy Groups to Add list.

**Step 3** To delete a group from the Policy Groups to Add list, select the group name, then click **Delete**.

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

---

### Deleting an Existing Policy Group from a Device

---

**Step 1** Enter the group identification number in the **Group ID** text box, then click **Add** to add it to the Policy Groups to Delete list.

- Step 2** To delete an identification number from the Policy Groups to Delete list, select it, then click **Delete**.
- 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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - Another template category to configure more options. (See [Template Categories, page 3-2](#).)
- 

## Configuring VLANs

Access points and bridges in a VLAN network, which are running specific software versions, can provide a wireless VLAN trunk link between two wired segments of the network.

Using this option, you can configure VLANs on the access point.

### Procedure

---

- Step 1** Select **Association > VLANs**. The Association: VLAN dialog box appears.
- Step 2** Click **see details** to see which versions this option is valid for.



**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 3** Enter the following information:

Field	Description
VLAN (802.1Q) Tagging	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Enabled—Use this setting to allow IEEE 802.1Q protocol tagging on VLAN packets.</li> </ul> <p>The IEEE 802.1Q protocol is used to interconnect multiple switches and routers, and for defining VLAN topologies.</p> <ul style="list-style-type: none"> <li>Disabled—Use this setting to not allow tagging.</li> </ul>
Native VLAN ID	<p>Enter identification number of the access point's native VLAN.</p> <p><b>Note</b> This setting must agree with the native VLAN ID setting on the switch.</p>
Single VLAN ID which allows unencrypted packets	<p>Enter an identification number to allow unencrypted packets. An entry with a value of 0 (zero) requires the use of encryption.</p>
Optionally allow Point-to-point Packet Encryption	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>Yes—Use this setting to allow point-to-point encryption.</li> <li>No—Use this setting to not allow point-to-point encryption.</li> </ul>

**Step 4** Using this option you can:

- Add a new VLAN—See [Adding a New VLAN, page 3-33](#).
- Delete an exiting VLAN from a Device—See [Deleting an Existing VLAN, page 3-36](#).

## Adding a New VLAN

**Step 1** To add a new VLAN, enter the following:

**Table 3-7 Adding a New VLAN Settings**

Field	Description
VLAN ID	Enter the identification number of the VLAN. <b>Note</b> This setting must match the setting on the switch.
VLAN Name	Enter the a unique name for the VLAN configured on the access point.
VLAN Enable	From the list, select one of the following: <ul style="list-style-type: none"> <li>Enabled—Use this setting to enable the VLAN.</li> <li>Disabled—Use this setting to disable the VLAN.</li> </ul>
Default Priority	From the list, select one of the following: <ul style="list-style-type: none"> <li>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.</li> <li>Default—Use this setting for normal LAN traffic.</li> <li>Excellent Effort—Use this setting for the network's most important users.</li> <li>Controlled Load—Use this setting for important business applications that are subject to some form of admission control.</li> <li>Interactive Video—Use this setting for traffic with less than 100 ms delay.</li> <li>Interactive Voice—Use this setting for traffic with less than 10ms delay.</li> <li>Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.</li> </ul>
Default Policy Group	Enter the default policy group number, or select one you created using <b>Association &gt; Policy Groups</b> .

**Table 3-7 Adding a New VLAN Settings (continued)**

Field	Description
Enhanced MIC verify WEP	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• None—Use this setting if you do not want Message Integrity Check (MIC) enabled.</li> <li>• MMH—Use this setting if you want MIC enabled to protect WEP keys.</li> </ul> <p><b>Note</b> When you enable MIC, only MIC-capable client devices can communicate with the access point.</p>
Temp Key Integrity Protocol	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• None—Use this setting if you do not want to enable the temporal key integrity protocol (TKIP, or WEP key hashing.)</li> <li>• Cisco—Use this setting to enable TKIP.</li> </ul> <p><b>Note</b> When TKIP is enabled, all WEP-enabled client devices associated to the access point must support WEP key hashing, or they will not be able to communicate with the access point.</p>
WEP Key Rotation Interval	<p>Use this setting to enable or disable broadcast key rotation.</p> <ul style="list-style-type: none"> <li>• To enable it, enter the rotation interval in seconds. If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes.</li> </ul> <p><b>Note</b> When you enable broadcast key rotation, only wireless client devices using LEAP or EAP-TLS authentication can use the access point. Client devices using static WEP (with open, shared key, or EAP-MD5) cannot use the access point when you enable broadcast key rotation.</p> <ul style="list-style-type: none"> <li>• To disable it, enter 0 (zero).</li> </ul>

**Table 3-7 Adding a New VLAN Settings (continued)**

Field	Description
Alert	From the list, select one of the following: <ul style="list-style-type: none"><li>• Yes—Use this setting if you are not adding an encrypted VLAN.</li><li>• No—Use this setting if you are adding an encrypted VLAN.</li></ul>
WEP Keys 1 through 4	Enter the encryption keys used: 40 bit or 128 bit hexadecimal digits.
Size	For each WEP key, select one of the following: Not set, 40 bit, or 128 bit.

**Step 2** Click **Add** to add the VLAN to the VLANs to Add list.

- Step 3** To delete a group from the VLANs to Add list, select the name, then click **Delete**.
- 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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - Another template category to configure more options. (See [Template Categories, page 3-2](#).)
- 

### Deleting an Existing VLAN

#### Procedure

---

- Step 1** Enter the VLAN identification number in the **VLAN ID** text box, then click **Add** to add it to the VLANs to Delete list.
- Step 2** To delete an identification number from the VLANs to Delete list, select it, then click **Delete**.
- 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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - Another template category to configure more options. (See [Template Categories, page 3-2](#).)
- 

### Configuring Quality of Service

This option is used to configure the access point's Quality of Service feature.

## Procedure

**Step 1** Select **Association > Quality of Service**. The Association: Quality of Service 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** Click **see details** to see which versions this option is valid for.

**Step 3** Enter the following information:

**Table 3-8 Quality of Service Settings**

Field	Description
Generate QBBS Element	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Use this setting to enable support for basic 802.11 Quality of Service.</li> <li>• No—Use this setting to disable support for basic 802.11 Quality of Service.</li> </ul>
User Symbol Extensions	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Use this setting enables support for Symbol Voice over IP (VoIP) phones.</li> <li>• No—Use this setting to disable support for Symbol VoIP phones.</li> </ul>
Send IGMP General Query	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Use this setting to allow the access point to send an IGMP General Query to all associated stations when they complete all required high-level authentication.</li> <li>• No—Use this setting to not allow the access point to send an IGMP General Query.</li> </ul>

**Table 3-8 Quality of Service Settings (continued)**

Field	Description
Background (spare)	From the <b>CWmin</b> and <b>CWmax</b> lists, select the minimum and maximum contention window values for each traffic category.
Best Effort (default)	
Excellent Effort	
Controlled Load	
Interactive Video	
Interactive Voice	
Network Control	

**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 3-131.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
- Another template category to configure more options. (See [Template Categories, page 3-2.](#))

## Configuring Service Sets

This option allows you to define service sets.

### Procedure

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

**Step 2** Click **see details** to see which versions this option is valid for.



**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 3** Using this option you can:
- Add a new Service Set—See [Adding a New Service Set, page 3-39](#).
  - Delete an exiting Service Set from a device—See [Deleting an Existing Service Set, page 3-42](#).

---

## Adding a New Service Set

### Procedure

- Step 1** To add a new Service set, enter the following:

**Table 3-9** *New Service Set Settings*

Field	Description
Service Set ID (1-24)	Enter an identification number for the SSID.
Service Set Name	Enter the SSID.
Maximum Number of Associations	Enter a number to limit the maximum number of wireless clients per SSID.
Proxy Mobile IP Enabled	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—This setting allows proxy mobile IP use by all stations associated to this access point.</li> <li>• No—This setting does not allow proxy mobile IP use.</li> </ul>
Default VLAN ID	Enter the identification number for a defined VLAN, or select one of the VLAN IDs you created using <b>Association &gt; VLANs</b> .
Default Policy Group	Enter the identification number of a defined policy group, or select one of the policy groups you created using <b>Association &gt; Policy Groups</b> .
Accept Authentication Type	

**Table 3-9 New Service Set Settings (continued)**

Field	Description
Open	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>
Shared	From the list, select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
Network-EAP	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>
<b>Require EAP</b>	
Open	From the list, select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>

**Table 3-9** *New Service Set Settings (continued)*

Field	Description
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—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.</li> <li>• <b>No</b>—Use this option if you do not use shared and EAP authentication.</li> </ul>
Default Unicast Address Filter	
Open	From the list, select one of the following:
Shared	<ul style="list-style-type: none"> <li>• <b>Allowed</b>—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters.</li> <li>• <b>Disallowed</b>—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.</li> </ul> <p>Select Disallowed for each authentication type that also uses MAC-based authentication.</p>
Network-EAP	

**Step 2** Click **Add** to add the Service Set to the Service Sets to Add list.

**Step 3** To delete a group from the list, select the name, then click **Delete**.

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

## Deleting an Existing Service Set

### Procedure

---

- Step 1** Enter the Service Set number in the **Service Set ID** text box, then click **Add** to add it to the Service Sets to Delete list.
- Step 2** To delete an identification number from the list, select it, then click **Delete**.
- 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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - 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 3-10 Advanced Association Settings**

<b>Field</b>	<b>Description</b>
Alert Severity Level	<p data-bbox="628 310 1083 337">From the list select one of the following:</p> <ul data-bbox="639 354 1204 875" style="list-style-type: none"><li data-bbox="639 354 1188 415">• systemFatal—Indicates an event that prevents operation of the port or device.</li><li data-bbox="639 431 1204 493">• protocolFatal—Indicates an event that prevents operation of the port or device</li><li data-bbox="639 509 1157 571">• portFatal—Indicates an event that prevents operation of the port or device</li><li data-bbox="639 587 1180 649">• systemAlert—Indicates that you need to take action to correct the condition.</li><li data-bbox="639 665 1197 727">• protocolAlert—Indicates that you need to take action to correct the condition.</li><li data-bbox="639 743 1147 805">• portAlert—Indicates that you need to take action to correct the condition.</li><li data-bbox="639 821 1194 883">• externalAlert—Indicates that you need to take action to correct the condition.</li></ul>

**Table 3-10 Advanced Association Settings (continued)**

Field	Description
	<ul style="list-style-type: none"> <li>• systemWarning—Indicates that an error or failure may have occurred.</li> <li>• protocolWarning—Indicates that an error or failure may have occurred.</li> <li>• portWarning—Indicates that an error or failure may have occurred.</li> <li>• externalWarning—Indicates that an error or failure may have occurred.</li> <li>• systemInfo—Notification that some sort of event has occurred.</li> <li>• protocolInfo—Notification that some sort of event has occurred.</li> <li>• portInfo—Notification that some sort of event has occurred.</li> <li>• externalInfo—Notification that some sort of event has occurred.</li> </ul>
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 3-10 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"> <li>• Enable—Use this setting to enable the storage of detailed statistics in the device’s memory.</li> <li>• Disable—Use this setting to disable the storage of detailed statistics in the device’s memory.</li> </ul> <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"> <li>• 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.</li> <li>• Disable—Use this setting to disable Publicly Secure Packet Forwarding.</li> </ul> <p>Click <b>see details</b> to see which versions this setting is valid for.</p>

**Table 3-10 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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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.

---

**Table 3-11 Port Assignments Settings**

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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - Another template category to configure more options. (See [Template Categories, page 3-2](#).)
-

## Configuring DSCP to CoS

This option is use to statically map Differentiated Services Code-Point (DSCP) values to corresponding Class of Service (CoS) values.

### Procedure

---

**Step 1** Select **Association > DSCP to CoS**. The Association: DSCP to CoS Conversion 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** Click **see details** to see which versions this option is valid for.

**Step 3** For each DSCP, enter the CoS conversion. Select one of the following:

- No Change
- Background
- Spare
- Best Effort
- Excellent Effort
- Controlled Load
- Interactive Video
- Interactive Voice
- Network Control

**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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-49](#).
  - Filters—See [Setting Up Ethernet Filters, page 3-50](#).
  - Hardware—See [Setting Up Hardware, page 3-52](#).
  - Advanced—See [Defining the Ethernet Advanced Settings, page 3-53](#).
- 

## 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:

**Table 3-12 Ethernet Port Settings**

Field	Description
Primary Port?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port.</li> <li>• Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port.</li> <li>• Radio 11b—Sets the 11b radio port as the primary port.</li> <li>• Radio 11a—Sets the 11a radio port as the primary port.</li> </ul>
Adopt Primary Port Identity?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port.</li> <li>• no—This uses different MAC and IP addresses for the Ethernet port.</li> </ul>

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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.

**Table 3-13 Ethernet Filters Settings**

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

- 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
- 

## Setting Up Hardware

This option allows you to select the hardware settings used by the access point's Ethernet port.

### Procedure

---

- Step 1** Select **Ethernet > Hardware**. The Ethernet: Hardware 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.

---

- Step 2** Click **see details** to see which versions this option is valid for.

**Step 3** Complete the following:

**Table 3-14 Ethernet Hardware Settings**

Field	Description
Loss of Backbone Connectivity # of Secs (1-1000)	Enter the number of seconds the system must detect loss of backbone connectivity (i.e. loss of Ethernet link and no active trunk available on any of the radios) before taking the specified by Loss of Backbone Connectivity Action.
Loss of Backbone Connectivity Action	From the list, select one of the following: <ul style="list-style-type: none"> <li>• No action</li> <li>• Switch to repeater mode</li> <li>• Shut the radio off</li> <li>• Restrict to SSID</li> </ul>
Loss of Backbone Connectivity SSID	Enter an SSID index required if the Loss of Backbone Connectivity Action is set to Restrict to SSID, or select the SSID from the list.

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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 3-15 Ethernet Advanced Settings**

Field	Description
Status	From the list, select one of the following: <ul style="list-style-type: none"> <li>• up— Enables the Ethernet port for normal operation.</li> <li>• down—Disables the device’s Ethernet port.</li> </ul>
Packet Forwarding	From the list, select one of the following: <ul style="list-style-type: none"> <li>• enabled—Allows normal operation.</li> <li>• disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.</li> </ul>
Default Multicast Address Filter	From the list, select one of the following: <ul style="list-style-type: none"> <li>• allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under <b>Association &gt; Address Filters</b>.</li> <li>• disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under <b>Association &gt; Address Filters</b>.</li> </ul>

**Table 3-15 Ethernet Advanced Settings (continued)**

Field	Description
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"> <li>• allowed—The access point forwards all traffic except packets sent to MAC addresses that have been set as disallowed under <b>Association &gt; Address Filters</b>.</li> <li>• disallowed—The access point discards all traffic except packets sent to the MAC addresses that have been set as allowed under <b>Association &gt; Address Filters</b>.</li> </ul>
Always Unblock Ethernet when STP is disabled	<p>From the list, select one of the following:</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to maintain a bridge link when STP is disabled</li> <li>• No—Use this setting to not maintain a bridge link when STP is disabled.</li> </ul> <p>Click <b>see details</b> to see which versions this setting is valid for.</p>
Optimize Ethernet for	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Performance—Allows faster packet forwarding.</li> <li>• Statistics Collection—Allows better statistics collection.</li> </ul> <p>Click <b>see details</b> to see which versions this setting is valid for.</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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
- 

## Configuring the 11b Radio

Use this option to configure the device's 11b radio.

### Procedure

---

- Step 1** Select **11b 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 11b Radio Port, page 3-56.](#)
  - Filters—See [Setting Up 11b Radio Filters, page 3-59.](#)
  - Hardware—See [Defining the 11b Radio Hardware Settings, page 3-60.](#)
  - Advanced—See [Defining the 11b Radio Advanced Settings, page 3-66.](#)
  - Searched Channels—See [Defining the 11b Radio Searched Channels Settings, page 3-71.](#)
- 

## Identifying the 11b Radio Port

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



---

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

---

### Procedure

---

**Step 1** Select **11b Radio > Identification**. The 11b 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.

---

**Table 3-16 11b Radio Identification Settings**

Field	Description
Primary Port?	<p>From the list, select one of the following:</p> <p><b>Note</b> If the primary port was set using <b>Ethernet &gt; Identification</b>, the selected value is displayed.</p> <ul style="list-style-type: none"> <li>• Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port.</li> <li>• Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port.</li> <li>• Radio 11b—Sets the 11b radio port as the primary port.</li> <li>• Radio 11a—Sets the 11a radio port as the primary port.</li> </ul>
Adopt Primary Port Identity?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port.</li> <li>• no—This uses different MAC and IP addresses for the Ethernet port.</li> </ul>

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

## Setting Up 11b Radio Filters



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

### Procedure

**Step 1** Select **11b Radio > Filters**. The 11b 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 3-17 11b Radio Filters Settings**

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

**Table 3-17 11b 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 <b>Association &gt; IP Port Filters</b> .
Transmit	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using <b>Association &gt; IP Port Filters</b> .

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

## Defining the 11b Radio Hardware Settings

### Procedure

**Step 1** Select **11b Radio > Hardware**. The 11b 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 3-18 11b 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"> <li>• 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.</li> <li>• 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.</li> </ul> <p>With no selected, the SSID used by the client device must match exactly the access point’s SSID.</p>

**Table 3-18 11b Radio Hardware Settings (continued)**

Field	Description
Enable “World Mode” multi-domain operation?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Allows the access point to add channel carrier set information to its beacon.</li> </ul> <p>Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically.</p> <ul style="list-style-type: none"> <li>• no—Does not allow the access point to add channel carrier set information to its beacon.</li> </ul>
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"> <li>• basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic.</li> <li>• yes—Allows transmission at this rate for unicast packets only.</li> <li>• no—Does not allow transmission at this rate.</li> </ul>
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> <p>Click <b>see details</b> to see which versions this setting is valid for.</p>

**Table 3-18 11b Radio Hardware Settings (continued)**

Field	Description
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>
Maximum RTS Retries (1-128)	<p>Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.</p>
Max. Data Retires (1-128)	<p>Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.</p>
Beacon Period (Kusec)	<p>Enter the amount of time between beacons in kilomicroseconds. (One kilomicrosecond equals 1,024 microseconds.)</p>

**Table 3-18 11b Radio Hardware Settings (continued)**

Field	Description
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 kilomicrosecond.</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>
Search for less-congested Radio Channel?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use.</li> <li>• no—Will not allow the access point to scan for a radio channel that is least busy.</li> </ul>

**Table 3-18 11b Radio Hardware Settings (continued)**

Field	Description
Receive Antenna	From the list, select one of the following:
Transmit Antenna	<ul style="list-style-type: none"> <li data-bbox="744 337 1229 521">• <b>Right</b>—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.</li> <li data-bbox="744 618 1229 802">• <b>Left</b>—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.</li> <li data-bbox="744 899 1229 1083">• <b>Diversity</b>—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.</li> </ul>

- 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
- 

## Defining the 11b Radio Advanced Settings

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

### Procedure

---

- Step 1** Select **11b Radio > Advanced**. The 11b 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 3-19 11b Radio Advance Settings**

Field	Description
Status	From the list, select one of the following: <ul style="list-style-type: none"> <li>• up— Enables the Radio port for normal operation.</li> <li>• down—Disables the device’s Radio port.</li> </ul>
Packet Forwarding	From the list, select one of the following: <ul style="list-style-type: none"> <li>• enabled—Allows normal operation.</li> <li>• disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.</li> </ul>
Default Multicast Address Filter	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under <b>Association &gt; Address Filters</b>.</li> <li>• Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under <b>Association &gt; Address Filters</b>.</li> </ul>
Maximum Multicast Packets/Second	Use this setting to control the number of multicast packets that can pass through the Ethernet port each second.  If you enter 0, the access point passes an unlimited number of multicast packets.  If you enter a number other than 0, the device passes only that number of multicast packets per second.

Table 3-19 11b Radio Advance Settings (continued)

Field	Description
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 <b>see details</b> to see which versions this setting is valid for.</p>
Use Aironet Extensions	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li> <li>• no—Does not enable the features listed above.</li> </ul>
Classify Workgroup Bridges as network infrastructure	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Use this setting to limit the number of workgroup bridges that can associate to the access point to 20 or less.</li> <li>• no—Use this setting to allow more than 20 workgroup bridges to associate to the access point.</li> </ul> <p>Click <b>see details</b> to see which versions this setting is valid for.</p>
User Symbol Extensions	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Use this setting to enable the following features: load balancing, message integrity check (MIC), temporal key integrity protocol (TKIP).</li> <li>• no—Use this setting to disable use of Cisco Aironet 802.11 extensions.</li> </ul> <p>Click <b>see details</b> to see which versions this setting is valid for.</p>

**Table 3-19 11b Radio Advance Settings (continued)**

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

**Table 3-19 11b Radio Advance Settings (continued)**

Field	Description
Broadcast WEP Key rotation interval (sec)	<p>Enter a rotation interval in seconds.</p> <ul style="list-style-type: none"> <li>If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes.</li> <li>If you enter 0, you disable broadcast WEP key rotation.</li> </ul> <p>Click <b>see details</b> to see which versions this setting is valid for.</p>
Default Unicast Address Filter	
Open	From the list, select one of the following:
Shared	<ul style="list-style-type: none"> <li>Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters.</li> <li>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.</li> </ul> <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 3-19 11b Radio Advance Settings (continued)**

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

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

## Defining the 11b 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 **11b Radio > Searched Channels**. The 11b Radio: Searched Channels dialog box displays in the right pane.
- Step 2** Click **see details** to see which versions this option is valid for.
- 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 3-20 11b Radio Searched Channels Settings**

Field	Description
Channel Number	Lists 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"> <li>• <b>Yes</b>—Use this option to include the channel in the scan for less-congested channels.</li> <li>• <b>No</b>—Use this option to exclude the channel in the scan for less-congested channels</li> </ul>

- 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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - Another template category to configure more options. (See [Template Categories, page 3-2](#).)

## Configuring the 11a Radio

Use this option to configure the device's 11a radio.

### Procedure

- 
- Step 1** Select **11a Radio**. The menu expands and the 11a Radio dialog box displays in the right pane.
- Step 2** Click **see details** to see which versions this option is valid for.
- Step 3** 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 11a Radio Port](#), page 3-73.
  - Filters—See [Setting Up 11a Radio Filters](#), page 3-75.
  - Hardware—See [Defining the 11a Radio Hardware Settings](#), page 3-76.
  - Advanced—See [Defining the 11a Radio Advanced Settings](#), page 3-81.
  - Searched Channels—See [Defining the 11a Radio Searched Channels Settings](#), page 3-88.
  - Data Encryption—See [Defining the 11a Radio Data Encryption Settings](#), page 3-89.
- 

## Identifying the 11a 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 **11a Radio > Identification**. The 11a Radio: Identification dialog box displays in the right pane.
- Step 2** Click **see details** to see which versions this option is valid for.
- Step 3** 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.

**Table 3-21 11a Radio Identification Settings**

Field	Description
Primary Port?	<p>From the list, select one of the following:</p> <p><b>Note</b> If the primary port was set using <b>Ethernet &gt; Identification</b>, the selected value is displayed.</p> <ul style="list-style-type: none"> <li>• Ethernet—Sets the Ethernet port for all access points other than AP1200's as the primary port.</li> <li>• Ethernet AP 1200—Sets the Ethernet port for AP1200 access points as the primary port.</li> <li>• Radio 11b—Sets the 11b radio port as the primary port.</li> <li>• Radio 11a—Sets the 11a radio port as the primary port.</li> </ul>
Adopt Primary Port Identity?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port.</li> <li>• no—This uses different MAC and IP addresses for the Ethernet port.</li> </ul>

- 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
- 

## Setting Up 11a Radio Filters



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

---

### Procedure

---

- Step 1** Select **11a Radio > Filters**. The 11a Radio Filters dialog box displays in the right pane.
- Step 2** Click **see details** to see which versions this option is valid for.
- 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 3-22 11a Radio Filters Settings**

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using <b>Association &gt; Ethertype Filters</b> .

**Table 3-22 11a Radio Filters Settings (continued)**

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

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

## Defining the 11a Radio Hardware Settings

### Procedure

- Step 1** Select **11a Radio > Hardware**. The 11a Radio: Hardware dialog box displays in the right pane.
- Step 2** Click **see details** to see which versions this option is valid for.

**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 3-23 11a 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"> <li>• 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.</li> <li>• 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.</li> </ul> <p>With no selected, the SSID used by the client device must match exactly the access point’s SSID.</p>

**Table 3-23 11a Radio Hardware Settings (continued)**

Field	Description
Data Rates (Mb/sec)	
6.0	<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"> <li>• basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic.</li> <li>• yes—Allows transmission at this rate for unicast packets only.</li> <li>• no—Does not allow transmission at this rate.</li> </ul>
9.0	
12.0	
18.0	
24.0	
36.0	
48.0	
54.0	
Transmit Power	<p>From the list, select one of the following milliwatt settings: 5, 10, 20, 40.</p> <p>To reduce interference or to conserve power, select a lower power setting.</p> <p>Click <b>see details</b> to see which versions this setting is valid for.</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 3-23 11a Radio Hardware Settings (continued)**

<b>Field</b>	<b>Description</b>
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 kilomicroseconds. (One kilomicrosecond 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	From the list, select the radio channel you want for a default.
Search for less-congested Radio Channel?	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use.</li> <li>• no—Will not allow the access point to scan for a radio channel that is least busy.</li> </ul>

**Table 3-23 11a Radio Hardware Settings (continued)**

Field	Description
Receive Antenna	From the list, select one of the following:
Transmit Antenna	<ul style="list-style-type: none"> <li data-bbox="744 337 1231 521">• <b>Right</b>—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.</li> <li data-bbox="744 618 1231 802">• <b>Left</b>—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.</li> <li data-bbox="744 899 1231 1083">• <b>Diversity</b>—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.</li> </ul>

- 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
- 

## Defining the 11a Radio Advanced Settings

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

### Procedure

---

- Step 1** Select **11a Radio > Advanced**. The 11a Radio: Advanced dialog box displays in the right pane.
- Step 2** Click **see details** to see which versions this option is valid for.

**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 3-24 11a Radio Advanced Settings**

Field	Description
Status	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• up—Enables the Radio port for normal operation.</li> <li>• down—Disables the device’s Radio port.</li> </ul>
Packet Forwarding	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• enabled—Allows normal operation.</li> <li>• disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.</li> </ul>
Default Multicast Address Filter	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under <b>Association &gt; Address Filters</b>.</li> <li>• Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under <b>Association &gt; Address Filters</b>.</li> </ul>
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>

**Table 3-24 11a Radio Advanced Settings (continued)**

Field	Description
Radio Cell Role	<p>From the list, enter one of the following:</p> <ul style="list-style-type: none"> <li>• Client/Non-Root—use this setting for diagnostics or site surveys, such as when you need to test and access point by having it communicate with another access point or bridge without accepting associations from client devices.</li> <li>• Repeater/Non-Root—Use this setting for access points that are not connected to a wired LAN and which transfer data between another access point or repeater.</li> <li>• Access Point/Root—Use this setting if the access point is connected to a wired LAN.</li> </ul>
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 <b>see details</b> to see which versions this setting is valid for.</p>
Use Aironet Extensions	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing.</li> <li>• no—Does not enable the features listed above.</li> </ul>

**Table 3-24 11a Radio Advanced Settings (continued)**

Field	Description
Classify Workgroup Bridges as network infrastructure	From the list, select one of the following: <ul style="list-style-type: none"> <li>• yes—Use this setting to limit the number of workgroup bridges that can associate to the access point to 20 or less.</li> <li>• no—Use this setting to allow more than 20 workgroup bridges to associate to the access point.</li> </ul>
Ethernet encapsulation transform	From the list, select one of the following: <ul style="list-style-type: none"> <li>• 802.1H—Provides optimum performance for Cisco Aironet wireless products.</li> <li>• RFC1042—Ensures interoperability with non-Cisco Aironet wireless equipment.</li> </ul>
Enhanced MIC verification for WEP	From the list, select one of the following: <ul style="list-style-type: none"> <li>• None—Does not enable MIC.</li> <li>• NMH—Enables MIC (Message Integrity Check), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks.</li> </ul>
Temporal Key Integrity Protocol	From the list, select the following: <ul style="list-style-type: none"> <li>• None—Does not enable WEP key hashing.</li> <li>• 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.</li> </ul>

**Table 3-24 11a Radio Advanced Settings (continued)**

Field	Description
Broadcast WEP Key rotation interval (sec)	Enter a rotation interval in seconds. <ul style="list-style-type: none"> <li>• If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes.</li> <li>• If you enter 0, you disable broadcast WEP key rotation.</li> </ul>
Accept Authentication Type	
Open	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>
Shared	From the list, select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>

**Table 3-24 11a Radio Advanced Settings (continued)**

Field	Description
Network-EAP	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>
Require EAP	
Open	From the list, select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>
Shared	From the list, select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• No—Use this option if you do not use shared and EAP authentication.</li> </ul>

**Table 3-24 11a Radio Advanced Settings (continued)**

Field	Description
Default Unicast Address Filter	
Open	From the list, select one of the following: <ul style="list-style-type: none"> <li>• <b>Allowed</b>—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters.</li> <li>• <b>Disallowed</b>—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.</li> </ul> Select Disallowed for each authentication type that also uses MAC-based authentication.
Shared	
Network-EAP	
Specified Access Point 1	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.  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.
Specified Access Point 2	
Specified Access Point 3	
Specified Access Point 4	

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

## Defining the 11a 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 **11a Radio > Searched Channels**. The 11a Radio: Searched Channels dialog box displays in the right pane.

**Step 2** Click **see details** to see which versions this option is valid for.

**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 3-25** 11a Radio Searched Channels Settings

Field	Description
Channel Number	Lists 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"> <li>• Yes—Use this option to include the channel in the scan for less-congested channels.</li> <li>• No—Use this option to exclude the channel in the scan for less-congested channels</li> </ul>

- 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - Another template category to configure more options. (See [Template Categories, page 3-2.](#))
- 

## Defining the 11a Radio Data Encryption 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 **11a Radio > Data Encryption**. The 11a Radio: Data Encryption dialog box displays in the right pane.
- Step 2** Click **see details** to see which versions this option is valid for.

**Step 3** Complete the following:

**Table 3-26 11a Radio Data Encryption Settings**

Field	Description
Data Encryption by Stations	<p>From the list, select the encryption type:</p> <ul style="list-style-type: none"> <li>• No Encryption—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended.</li> <li>• 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.</li> <li>• 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.</li> </ul>
Authentication Type	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>

**Table 3-26 11a Radio Data Encryption Settings (continued)**

Field	Description
Shared Key	From the list, select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
Require EAP	
Open	From the list, select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>
Shared	From the list, select one of the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• No—Use this option if you do not use shared and EAP authentication.</li> </ul>
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.

- 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 3-131.)
  - **Finish** to save the template. (See [Finishing the Template](#), page 3-132.) 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 3-92.
  - Local AP/Client Security—See [Setting Local AP/Client Security](#), page 3-94.
  - Server-Based Security—See [Setting Server-Based Security](#), page 3-97.
- 

## 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.

**Table 3-27 Local Admin Access Settings**

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

**Step 3** Using this option you can:

- Add Users—See [Adding Users, page 3-93](#).
- Delete Users—See [Deleting Users, page 3-94](#).

## Adding Users

### Procedure

**Step 1** To add a new user, enter the following:

Field	Description
User ID	Enter an identification number for the user. <b>Tip</b> If you want to set the same user name on all access points and do not know which user ID's may already be in use, enter a very high value (2000).
User name	Enter the name for the user.
User password	Enter a password for the user.
Capabilities	Select the capabilities you want to allow the user.

- Step 2** Click **Add** to add the users to the Users to Add list.
- Step 3** To delete a user from the list, select the name, then click **Delete**.
- 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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - Another template category to configure more options. (See [Template Categories, page 3-2](#).)
- 

### Deleting Users

Click **see detail** to see which versions this option is valid for.

#### Procedure

---

- Step 1** Enter the user's identification number in the **User ID** text box, then click **Add** to add it to the Users to Delete list.
- Step 2** To delete an identification number from the list, select it, then click **Delete**.
- 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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - 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 3-28 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"> <li>• <b>No Encryption</b>—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended.</li> <li>• <b>Optional</b>—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.</li> <li>• <b>Full Encryption</b>—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.</li> </ul>
Authentication Type	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Yes</b>—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting.</li> <li>• <b>No</b>—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.</li> </ul>

**Table 3-28 Local AP /Client Security Settings (continued)**

Field	Description
Shared Key	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
Network-EAP	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Allows EAP-enabled client devices to authenticate through the access point.</li> <li>• No—Does not allow EAP-enabled client devices to authenticate through the access point.</li> </ul>
Require EAP	
Open	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• No—Use this option if you do not use open and EAP authentication.</li> </ul>
Shared	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• No—Use this option if you do not use shared and EAP authentication.</li> </ul>

Encryption Keys 1 through 4

**Table 3-28 Local AP /Client Security Settings (continued)**

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

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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 3-29 Server-Based Security Settings**

Field	Description
802.1X Protocol Version (For EAP Authentication)	<p><b>Note</b> This setting may cause the device to reboot.</p> <p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.</li> <li>• 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.</li> <li>• 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.</li> </ul> <p>Click * (asterisk) for information on which version this setting is valid</p>
Primary Server Reattempt Period (Min)	<p>Enter the amount of time a before another attempt is made if the server is not responding.</p> <p>Click * (asterisk) for information on which version this setting is valid.</p>
Server Name/IP	Enter the name or IP address of the server.

**Table 3-29 Server-Based Security Settings (continued)**

Field	Description
Server Type	Enter the type of server.  Click * (asterisk) for information on which version this setting is valid
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.
Retran Int (sec)	Enter the number of seconds the access point should wait before retransmitting.  Click * (asterisk) for information on which version this setting is valid.
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.
EAP Auth	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Use this server for EAP authentication.</li> </ul> <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"> <li>• No—Do not use this server for EAP authentication.</li> </ul> <p>Click * (asterisk) for information on which version this setting is valid.</p>

**Table 3-29 Server-Based Security Settings (continued)**

Field	Description
MAC Auth	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this server for MAC-based authentication.</li> </ul> <p>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 style="list-style-type: none"> <li>• No—Do not use this server for MAC-based authentication.</li> </ul> <p>Click * (asterisk) for information on which version this setting is valid.</p>
User Auth	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• Yes—Use this setting to allow user authentication.</li> <li>• No—Use this setting to disallow user authentication.</li> </ul> <p>Click * (asterisk) for information on which version this setting is valid.</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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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 3-103](#).
  - Console/Telnet—See [Configuring Console/Telnet Settings, page 3-107](#).
  - Hot Standby—See [Configuring Hot Standby Settings, page 3-109](#).
  - Routing—See [Configuring Routing Settings, page 3-111](#).
  - CDP—See [Configuring CDP Settings, page 3-112](#).
  - DNS—See [Configuring DNS Settings, page 3-113](#).
  - FTP—See [Configuring FTP Settings, page 3-114](#).
  - HTTP—See [Configuring HTTP Settings, page 3-116](#).
  - SNMP—See [Configuring SNMP Settings, page 3-117](#).
  - SNTP—See [Configuring SNTP Settings, page 3-118](#).
  - Accounting—See [Configuring Accounting Settings, page 3-119](#).
-

## 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 3-30 Start-Up Settings**

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

**Table 3-30 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"> <li>• always—Use this setting for the access point to always load configuration settings from an.ini file on the server.</li> <li>• never—Use this setting for the access point to never load configuration settings from an.ini file on the server.</li> <li>• 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.</li> </ul>
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.

**Table 3-30 Start-Up Settings (continued)**

Field	Description
DHCP Client Identifier Type	<p data-bbox="733 289 1197 318">From the list, select one of the following:</p> <ul data-bbox="744 334 1112 902" style="list-style-type: none"><li data-bbox="744 334 969 363">• Ethernet (10Mb)</li><li data-bbox="744 380 1112 409">• Experimental Ethernet (3Mb)</li><li data-bbox="744 425 1036 454">• Amateur Radio AX.25</li><li data-bbox="744 470 1106 500">• Proteon ProNET Token Ring</li><li data-bbox="744 516 852 545">• Chaos</li><li data-bbox="744 561 1005 591">• IEEE 802 Networks</li><li data-bbox="744 607 892 636">• ARCNET</li><li data-bbox="744 652 938 682">• Hyperchannel</li><li data-bbox="744 698 865 727">• Lanstar</li><li data-bbox="744 743 1042 773">• AutoNet Short Address</li><li data-bbox="744 789 895 818">• LocalTalk</li><li data-bbox="744 834 884 863">• LocalNet</li><li data-bbox="744 880 1018 909">• Other-Non Hardware</li></ul> <p data-bbox="733 922 1220 979">Click <b>see details</b> to see which versions this setting is valid for.</p>

**Table 3-30 Start-Up Settings (continued)**

Field	Description
DHCP Client Identifier Value	<p>Use this setting to include a unique identifier in the access point's DHCP request packet.</p> <ul style="list-style-type: none"> <li>• If you select Other-Non Hardware from the DHCP Client Identifier Type list, you can enter up to 255 alphanumeric characters.</li> <li>• If you select any other option from the DHCP Client Identifier Type list, you can enter up to 12 hexadecimal characters (numbers 0 through 9, and the letters A through F).</li> </ul> <p>Click <b>see details</b> to see which versions this setting is valid for.</p>
DHCP Class Identifier	<p>Enter the access point's group name.</p> <p>The DHCP server uses the group name to determine the response to send to the access point.</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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-31 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"> <li>• None—Use this setting to use no parity bit.</li> <li>• Even—Use this setting to make the total number of bits even.</li> <li>• Odd—Use this setting to make the total number of bits odd.</li> </ul>
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"> <li>• None—Use this setting to indicate no flow control is used.</li> <li>• 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.</li> </ul>
Terminal Type	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• teletype—Use this setting if your terminal emulator does not support ANSI.</li> <li>• ANSI—Use this setting to offer graphic features such as reverse video buttons and underlined links.</li> </ul>

**Table 3-31 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"> <li>• <b>Enable</b>—Use this setting to enable Telnet access to the management system.</li> <li>• <b>Disable</b>—Use this setting to prevent Telnet access to the management system.</li> </ul>

- 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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.

**Table 3-32 Hot Standby Settings**

Field	Description
Hot Standby Mode	From the list, select one of the following: <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to allow hot standby mode.</li> <li>• <b>Disable</b>—Use this setting to disable hot standby mode.</li> </ul>
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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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.

**Table 3-33 Routing Settings**

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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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.

---

**Table 3-34 CDP Settings**

Field	Description
Cisco Discovery Protocol (CDP)	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Enable—Use this setting to enable CDP.</li> <li>• Disable—Use this setting to disable CDP.</li> </ul>

**Table 3-34 CDP Settings (continued)**

Field	Description
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 3-131.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
- 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 3-35 DNS Settings**

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

**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 3-131.](#))
- **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
- 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 3-36 FTP Settings**

Field	Description
File Transfer Protocol (FTP)	From the list select one of the following: <ul style="list-style-type: none"> <li>• TFTP</li> <li>• FTP</li> </ul>
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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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.

---

**Table 3-37 HTTP Settings**

Field	Description
Allow Non-Console Browsing	From the list, select one of the following: <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to allow browsing to the management system.</li> <li>• <b>Disable</b>—Use this setting to make the management system accessible only through the console and Telnet interfaces.</li> </ul>
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 3-131](#).)
  - **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
  - 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.

**Table 3-38** *SNMP Settings*

Field	Description
Simple Network Management Protocol (SNMP)	From the list, select one of the following: <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting to allow event notifications to be sent to an SNMP server.</li> <li>• <b>Disable</b>—Use this setting to not allow event notifications to be sent to an SNMP server.</li> </ul>
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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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.

---

**Table 3-39 SNTP Settings**

Field	Description
Simple Network Time Protocol (SNTP)	From the list, select one of the following: <ul style="list-style-type: none"> <li>• <b>Enable</b>—Use this setting if your network uses Simple Network Time Protocol.</li> <li>• <b>Disable</b>—Use this setting if your network does not use Simple Network Time Protocol.</li> </ul>
Default Time Server	Enter enter the server's IP address.

**Table 3-39** *SNTP Settings (continued)*

Field	Description
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"> <li>• <b>Enable</b>—Use this setting to have the access point automatically adjust to Daylight Savings Time.</li> <li>• <b>Disable</b>—Use this setting to not have the access point automatically adjust to Daylight Savings Time.</li> </ul>

- 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 3-131.](#))
  - **Finish** to save the template. (See [Finishing the Template, page 3-132.](#))
  - 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 3-40 Accounting Settings**

Field	Description
Enable accounting	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• enable—Use this setting to turn on accounting for your wireless network.</li> <li>• disable—Use this setting to turn off accounting for your wireless network</li> </ul>
Enable delaying to report STOP	<ul style="list-style-type: none"> <li>• enable—Use this setting to delay sending a stop report to the server when a client device disassociates from the access point.</li> </ul> <p>The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate.</p> <ul style="list-style-type: none"> <li>• disable—Use this setting to not delay sending a stop report to the server when a client device disassociates from the access point.</li> </ul>
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.

**Table 3-40 Accounting Settings (continued)**

<b>Field</b>	<b>Description</b>
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.
Shared Secret	Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.
Retran (sec)	Enter the amount of time to wait before retransmitting.
Max Retran	Enter the maximum number of times to attempt retransmissions.  Click * (asterisk) for information on which version this setting is valid.

**Table 3-40 Accounting Settings (continued)**

Field	Description
Enable Update	<p>From the list, select one of the following:</p> <ul style="list-style-type: none"> <li>• enable—Use this setting to allow accounting update messages for wireless clients.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• disable—Use this setting to not allow accounting update messages.</li> </ul> <p>With updates disabled, the access point sends only accounting start and accounting stop messages to the server.</p>
Update Delay (sec's)	<p>Enter the update interval in seconds.</p> <p>If you use 360, the access point sends an accounting update message for each associated client device every 6 minutes.</p>

**Table 3-40 Accounting Settings (continued)**

Field	Description
EAP Auth.	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Use this server for EAP authentication.</li> </ul> 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"> <li>• No—Do not use this server for EAP authentication.</li> </ul>
Non-EAP Auth.	From the list, select one of the following: <ul style="list-style-type: none"> <li>• Yes—Use this server for non-EAP authentication.</li> <li>• No—Do not use this server for non-EAP authentication.</li> </ul>

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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 3-124](#).
  - Event Notifications—See [Configuring Event Notification, page 3-129](#).
- 

## 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 3-41 Event Handling Settings**

Field	Description
System Fatal	From the list, select one of the following: <ul style="list-style-type: none"> <li>• <b>Count</b>—Use this option to tally the total events occurring in this category without any form of notification or display.</li> <li>• <b>Display Console</b>—Use this option to provide a read-only display of the event but not record it.</li> <li>• <b>Record</b>—Use this option to make a record of the event in the log and provide a read-only display of the event.</li> <li>• <b>Notify</b>—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.</li> </ul>
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 3-41 Event Handling Settings (continued)**

Field	Description
Handle Alerts as Severity Level	<p data-bbox="736 289 1197 318">From the list, select one of the following:</p> <ul data-bbox="744 337 1231 1143" style="list-style-type: none"> <li data-bbox="744 337 1193 423">• <code>systemFatal</code>—Indicates an event that prevents operation of the device as a whole.</li> <li data-bbox="744 443 1231 565">• <code>protocolFatal</code>—Indicates an event that prevents operation of a specific communications protocol in use, such as HTTP or IP.</li> <li data-bbox="744 584 1193 670">• <code>portFatal</code>—Indicates an event that prevents operation of the Ethernet or radio network interface.</li> <li data-bbox="744 690 1231 781">• <code>systemAlert</code>—Indicates that you need to take action to correct a condition on the device as a whole.</li> <li data-bbox="744 800 1231 922">• <code>protocolAlert</code>—Indicates that you need to take action to correct a condition on a specific communications protocol in use, such as HTTP or IP.</li> <li data-bbox="744 941 1231 1032">• <code>portAlert</code>—Indicates that you need to take action to correct the condition on the Ethernet or radio network interface.</li> <li data-bbox="744 1052 1231 1143">• <code>externalAlert</code>—Indicates that you need to take action to correct the condition on a device on the network.</li> </ul>

**Table 3-41 Event Handling Settings (continued)**

Field	Description
	<ul style="list-style-type: none"> <li>• <code>systemWarning</code>—Indicates that an error or failure may have occurred on the device as a whole.</li> <li>• <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> <li>• <code>portWarning</code>—Indicates that an error or failure may have occurred on an Ethernet or radio network interface.</li> <li>• <code>externalWarning</code>—Indicates that an error or failure may have occurred on a device.</li> <li>• <code>systemInfo</code>—Notification that some sort of event has occurred on a device.</li> <li>• <code>protocolInfo</code>—Notification that some sort of event has occurred on a communications protocol in use, such as HTTP or IP.</li> <li>• <code>portInfo</code>—Notification that some sort of event has occurred on an Ethernet or radio network interface.</li> <li>• <code>externalInfo</code>—Notification that some sort of event has occurred on a device.</li> </ul>

**Table 3-41 Event Handling Settings (continued)**

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

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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 3-42** *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"> <li>• Yes—Use this option to send event notifications to an SNMP server.</li> <li>• No—Use this option if you do not want to send notifications to an SNMP server.</li> </ul>
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"> <li>• Yes—Use this option to send event notifications to a Syslog server.</li> <li>• No—Use this option if you do not want to send notifications to a Syslog server.</li> </ul>

**Table 3-42 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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- 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.



### 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.
Value	Enter a valid MIB value.

**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 3-131](#).)
- **Finish** to save the template. (See [Finishing the Template, page 3-132](#).)
- Another template category to configure more options. (See [Template Categories, page 3-2](#).)

## 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 3-132](#).)

## 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 Checking** 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 3-134](#).)
-

## 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.



**Note** You cannot delete a template if it used in a scheduled job.

- Step 3** Click **OK** to delete it.

## Importing a Template

Use this option to import a configuration to the WLSE, either from a file or from a device. You can import files from devices that are not managed by the WLSE.



**Note** Your login determines whether you can use this option.

### Procedure

- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Click **Import**. The Import Template window appears.
- Step 3** Complete the following:

Field	Description
Template Name	Enter a name for the template.
Description	Enter a description for the template
From file	Enter the template filename or browse to find the file, then click <b>Import</b> .
From device (IP Address)	Enter a device name or IP address, then click <b>Import</b> .

Field	Description
Non-IP-Identity	<p>Select this option if you do not want to download identity parameters, such as IP address, from the access point.</p> <p>Some parameters are ignored using this type of import. The downloaded configuration parameters are not a full representation of the access point's configuration but an optimal representation.</p>
Full	<p>Select this option to import a full configuration from the access point.</p> <p>This type of import includes the access point's identity parameters, such as sysname, IP address, etc.</p> <p><b>Note</b> When using this option, it is recommended you delete all the custom key values from the imported template before applying the template to any device.</p>
Device Credentials	
User Name	If the device is not managed by the WLSE, or if the device is managed but the credentials have not been set, enter the username on the access point.
User Password	If the device is not managed by the WLSE, enter the user password on the access point.

- Step 4** To import another template, click **Back** and repeat [Step 3](#).
- Step 5** When you are finished, click **Done**.
- Step 6** View the template you imported by selecting **Configure > Templates** and selecting it in the Existing Templates list.

**Note**

---

Any configuration options in the imported file, which cannot be configured using the WLSE, will appear in Custom Values. It is recommended that you delete the custom values.

---

## Exporting a Template

Use this option to export a configuration template to your local drive.

**Note**

---

Your login determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Configure > Templates**. The Templates dialog box appears.
- Step 2** Select a template name from Existing Templates, then click **Export**. The Export Template window appears.
- Step 3** From the list, select the template you want to export, then click **Export**. You will be prompted for a location to export the.ini file.
- Step 4** Click **Done**.
- 

## 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 3-144](#)
- [Viewing Configuration Job Status, page 3-144](#)
  - [Filtering a Job, page 3-147](#)
  - [Editing a Job, page 3-148](#)

- [Deleting a Job, page 3-148](#)
- [Copying a Job, page 3-148](#)
- [Viewing Job Run Details, page 3-149](#)

**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**

---

All these steps, except Schedule Job, must be completed but do not have to be done in order. You schedule a job later.

---

1. **Job Name**—See [Naming the Job, page 3-138](#).
2. **Select Devices**—See [Selecting Devices, page 3-139](#).
3. **Select Template**—See [Selecting a Template, page 3-140](#).
4. **Schedule Job**—See [Scheduling a Job, page 3-142](#).
5. **Finish**—See [Finishing the Job, page 3-143](#).

**Caution**

---

Clicking on another Configure subtab 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 3-43 Job Name**

Field	Description
Job Name	Enter a name for the job. See <a href="#">Naming Guidelines, page A-1</a> .
Description	Enter a description of the job. See <a href="#">Naming Guidelines, page A-1</a> .
Protocol	Select the type of protocol used: HTTP or SNMP.

**Step 3** From the menu in the left pane, go to the next step, Select Devices. (For additional information, see [Selecting Devices, page 3-139](#).)

## 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 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 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 3-140](#).)
- 

## 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 3-44** *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 3-142.)

## 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 3-45** *Schedule Job*

Field	Description
Run Now	Click to run the job. <b>Note</b> 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 the Job, page 3-143](#).)



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

## Finishing the Job

### 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** If you want email notification of job completion, use the Email settings section:

Field	Description
On completion, email to	Enter a comma-separated list of email addresses to be notified when the job completes.
Email only if job fails	Select this checkbox if you want recipients to be notified only if the job fails.



**Tip** If email notification is not working, you may need to configure the mailroute by selecting **Administration > Appliance > Configure Mailroute**.

- Step 3** Click **Validate** if you want to check the job.



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

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** It is recommended that you always validate a job before saving it, and to eliminate any errors before saving it. If a job is saved with errors, the devices associated with the errors are ignored when the job runs.

- Step 4** 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 3-138](#).
- 

## 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 6-73](#).

The topics covered in this section are:

- [Viewing the Job, page 3-145](#)
- [Filtering a Job, page 3-147](#)
- [Editing a Job, page 3-148](#)

- [Deleting a Job, page 3-148](#)
- [Copying a Job, page 3-148](#)
- [Viewing Job Run Details, page 3-149](#)

**Note**

Your login determines whether you can use this option.

**Related Topic**

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

## Viewing the Job

**Procedure**

- Step 1** Select the status of the job you want to view from the Job State list.
- Step 2** Select the type of job you want to view from the Job Type list.
- Step 3** Click **Apply**. The window refreshes and the jobs are displayed.

The tables vary depending on the type of Job State and Job Type 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.
	<b>Note</b> Jobs that cause an access point to reboot are listed as Unverified.

- 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.
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. <b>Note</b> 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. <b>Note</b> Jobs that cause an access point to reboot are listed as Unverified.

**Step 4** 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 5** You can do the following:



---

**Note** If the option is not available for the job type, the buttons are grayed.

---

- a. Filter the job—See [Filtering a Job](#), page 3-147.
  - b. Edit the job—See [Editing a Job](#), page 3-148.
  - c. Delete the job—See [Deleting a Job](#), page 3-148,
  - d. Copy a job—See [Copying a Job](#), page 3-148.
  - e. View the run details—See [Viewing Job Run Details](#), page 3-149.
  - f. 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 Job**. 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 3-138.
- 

## 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 Job**.
- 

## Copying a Job

Use this option to copy unscheduled jobs from the displayed list of jobs, which can be run later on demand.

### Procedure

- 
- Step 1** Select the job from the list which you would like to copy.
- Step 2** Click **Copy Job**. A dialog box appears.
- Step 3** Enter a name for the job, then click **OK**. The screen refreshes and the job is listed.
- 

## 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 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 3-150](#).)

- 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 not supported for the following:

- 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
- Routing table configurations (for versions prior to 11.23T only)
- Adding a user in place of an existing user on the access point. The Undo feature works for new users.

## Automating Configurations

This window allows you to automatically upload configuration templates to access points and bridges. Use this feature to:

- Apply startup templates through the DHCP server to newly-installed devices with manufacturer-default configurations.
- Apply a common template to devices after they are discovered, auto managed, and the WLSE has their inventory information.

The topics covered in this section are:

- [Assigning a Startup Configuration, page 3-151](#)
- [Assigning an Auto-Managed Configuration, page 3-154](#)

## Assigning a Startup Configuration

The startup configuration is used for newly-installed devices that have a manufacturer-default configuration. After the devices are powered on and receive an IP address from a DHCP server, the startup configuration will be automatically uploaded to the devices.

**Before You Begin**

1. Create a template for the startup configuration. (See [Creating a Startup Configuration Template, page 3-153](#).)
2. Configure the DHCP server to:
  - a. Return the WLSE's address. This is done by entering the `<IP address of the WLSE>` in the Boot Server **Host Name** field (option number 066) on the DHCP server.
  - b. Return the name of the initial template file in the DHCP reply message. This is done by entering `<startup file name>` in the **BootfileName** field (option number 067) on the DHCP server.

For example, if you had a WLSE with the IP address 10.10.11.12) and an associated startup template with Bootfile Name "newap1200.ini", you would do the following:

- a. On the DHCP server, select **Scope > Scope Options**.
- b. Set Scope option 066 (TFTP boot server name or IP address) with `10.10.11.12` (the WLSE's IP address).
- c. Set Scope option 067 (Bootfile Name) with `new-ap1200.ini` (the new Bootfile Name associated with the startup template file.)

**Tip**


---

After the access point is powered on and the startup configuration is applied, you may want to prevent the startup configuration from being uploaded to devices again if for some reason the access points reboot. To prevent the initial configuration from being uploaded to devices after a reboot, set the **bootconfigReadINI** variable on the access point to **never** by auto-managed configuration or regular configuration.

---

**Related Topics**

- [Creating a Startup Configuration Template, page 3-153](#)
- [Assigning an Auto-Managed Configuration, page 3-154](#)

**Procedure**

- 
- Step 1** Select **Configure > Auto Update > Startup Configuration**. The Startup Configuration Template dialog box appears.

**Step 2** Complete the following:

Field	Description
Startup Templates	Lists the startup templates that have been created.
Bootfile Name	Enter the configuration file name that appears on the DHCP server. This must have an .ini extension.
Description	Enter a description for the configuration.
Configuration Template	From the list select the startup template to assign to the configuration file.  Click <b>Details</b> to see the device types and device versions for which the template is valid.

**Step 3** Click **Save** to save the template.

**Step 4** Click **Delete** to delete the template.

## Creating a Startup Configuration Template

The startup configuration is used to bootstrap a device to allow the WLSE to discover it.



### Caution

The startup configuration template is placed in tftpboot directory and anyone who knows the file name can access it. This template should contain only minimal feature settings.

To create a startup template select **Configure > Templates**. (To configure the access point manually without using a startup configuration, see [Set Up Access Points and Bridges, page 6-12.](#))

Use the following table to guide you in creating a startup configuration template:

Tasks	Template Choice	Notes
1. Enable Cisco Discovery Protocol (CDP).	Select <b>Services &gt; CDP</b> .	CDP is required for the WLSE to discover devices on the network.
2. Enable SNMP. (Optional) Set the location. (Optional) Set the system name and system contact.	Select <b>Services &gt; SNMP</b> .	SNMP is required for the WLSE to discover and manage the device.  Setting the location enables proper grouping of devices into the system-defined Location group. For more information, see <a href="#">Managing Groups, page 6-37</a> .
3. Set the community string by creating a user with all privileges.	Select <b>Security &gt; Local Admin Access</b> .  To create an user with SNMP read/write privileges, enter a username and password and select the Write, SNMP, Firmware, and Administrator capabilities.	The username of the user with Write and SNMP privileges is used as the SNMP read/write community string.  This community string should also have been configured on the WLSE using <b>Administration &gt; Discover &gt; Device Credentials &gt; SNMP Communities</b> .  The Firmware privilege is required for configuring devices from the WLSE.
5. Set up TFTP as the transfer protocol between the WLSE and access points.	Select <b>Services &gt; FTP</b> .	TFTP is used for transferring configuration changes to access points.

## Assigning an Auto-Managed Configuration

Use this option to automatically apply a customized configuration to auto-managed devices after their inventory information has been collected by the WLSE.

The configuration which is applied to the devices is based on the system-defined group with which the devices are associated.

**Tip**

---

It is recommended that as part of the auto-managed configuration template, you create an HTTP user and password by selecting **Security > Local Admin Access**. You also enter this user and password on the WLSE by selecting **Administration > Discover > Device Credentials > HTTP User/Password**.

---

The following topics are covered in this section:

- Assigning a Configuration Template—See [Assigning Auto-Managed Configurations, page 3-156](#)
- Emailing the Configuration Job Results—See [Using Auto-Managed Options, page 3-157](#)

## Assigning Auto-Managed Configurations

### Procedure

- Step 1** Select **Configure > Auto Update > Auto-Managed Configuration**. The Auto-Managed Configuration Templates dialog box appears with the names of the groups for which you can apply an automated template.
- Step 2** Complete the following:

Field	Description
Auto-Managed Templates	Lists the auto-managed templates that have been created.
Name	Enter a name for the auto-managed configuration. This must have a .ini extension.
Description	Enter a description for the configuration.
Automatically apply configuration template to devices matching the criteria below when they get auto managed	<ol style="list-style-type: none"> <li>1. Select the checkbox if you want to automatically apply a template.</li> <li>2. From the list select the template you want to assign.</li> <li>3. Click <b>Details</b> to see the device types and device versions for which this template is valid.</li> </ol>

Field	Description
Device Types	<p><b>Note</b> Auto-managed templates for AP 350's are applied to 350 bridges; you cannot assign a different template for bridges based on device type alone. If the bridges are running a different software version than the AP350s, use a different template for bridges and set the appropriate version numbers.</p> <ol style="list-style-type: none"> <li>1. Select the checkbox to enable the device types.</li> <li>2. From the list, select the device and click &gt;&gt; to add it to the list of valid devices for that template.</li> <li>3. To remove devices from the list, select the device, then click <b>Remove</b>.</li> </ol>
Software Versions	<ol style="list-style-type: none"> <li>1. Select the checkbox to enable the software versions.</li> <li>2. Enter the version numbers if they are not in the list, or from the list, select the version number, then click &gt;&gt; to add it to the list of valid versions for that template.</li> <li>3. To remove version numbers, select the version number from the list, then click <b>Remove</b>.</li> </ol>

**Step 3** Click **Save** to save the template.

**Step 4** To delete a template, select it from the Auto-Managed Templates listbox, then click **Delete**.

## Using Auto-Managed Options

This option allows you to email the results of your auto-managed configuration job.

### Procedure

**Step 1** Select **Configure > Auto Update > Auto-Managed Configuration > Auto-Managed Options**. The Auto-Managed Configuration Options dialog box appears.

- Step 2** Select the checkbox to enable email notification.
- Step 3** Enter the email address for the recipients of the notification.

**Tip**

---

If email notification is not working, you may need to configure the mailroute by selecting **Administration > Appliance > Configure Mailroute**.

---

- Step 4** Click **Save**.
-