



## Performing Administrative Tasks

---

The Administration tab allows you to perform administrative tasks.



### Note

---

Some of the subtabs may not be visible to some users; what you view under the Administration tab depends on your login.

---

The Administration subtabs have the following functions:

- **Discover**—Manage devices, configure discovery, specify device credentials, import devices, and set up LEAP servers (see [Using Discovery and Managing Devices, page 6-2](#)).
- **Group Management**—Place devices in groups for efficient management (see [Managing Groups, page 6-28](#)).
- **Appliance**—Manage the Wireless LAN Solution Engine server (see [Managing the Appliance, page 6-34](#)).
- **System Parameters**—Configure parameters for reporting performance and fault data (see [Managing System Parameters, page 6-59](#)).
- **User Admin**—Manage users and user roles (see [Administering Users, page 6-61](#)).
- **My Profile**—Change your password (see [Modifying Your Profile, page 6-66](#)).
- **Connectivity**—Test device connectivity and reachability and troubleshoot nonresponding devices (see [Using Connectivity Tools, page 6-67](#)).

# Using Discovery and Managing Devices

The Discover window contains the following options:

- **Discover**—Set up discovery, perform an immediate discovery, and view discovery history (see [Managing Device Discovery, page 6-2](#)).
- **Managed Devices**—View newly discovered devices, change device status, and view device management history (see [Managing Devices, page 6-13](#)).
- **Inventory**—Run a one-time, immediate inventory to collect information from managed devices before the next *scheduled* inventory (see [Running Inventory Now, page 6-17](#)).
- **Device Credentials**—Specify community strings and specify the HTTP username and password for access points (see [Setting Device Credentials, page 6-17](#)).
- **Import Devices**—Import devices from a file or from a CiscoWorks2000 server (see [Importing Devices, page 6-21](#)).
- **Export Devices**—Export devices to a CiscoWorks2000 server (see [Exporting Devices, page 6-24](#)).
- **LEAP Server**—Add, modify, or delete LEAP servers (see [Managing LEAP Servers, page 6-26](#)).

## Managing Device Discovery

The discovery options are:

- **Modify Discovery Settings**—Set up scheduled discoveries (see [Add Seed Devices and Schedule Discovery, page 6-10](#)).
- **Run Discovery Now**—Run a one-time, immediate discovery (see [Run Discovery Now, page 6-11](#)).
- **Discovery History**—View discovery details (see [View Discovery History and Status, page 6-12](#)).

### Related Topics

- [Overview: Discovery, page 6-3](#)
- [Set Up Devices, page 6-4](#)

## Overview: Discovery

You can set up regularly scheduled discoveries and run one-time discoveries.

Before the WLSE can discover devices:

- You must configure discovery on the WLSE. See [Add Seed Devices and Schedule Discovery, page 6-10](#).

As an alternative to using Cisco Discovery Protocol (CDP) to run discovery, you can import devices from a file or from CiscoWorks2000. See [Importing Devices, page 6-21](#).

- Devices must be properly configured for access by the WLSE. See [Set Up Devices, page 6-4](#).
- Community strings must be entered on the WLSE. See [Specify Community Strings, page 6-18](#)).



---

**Note**

Routers and switches are only discovered if they have properly configured access points attached to them.

---

Discovery proceeds according to the [seed](#) devices and CDP distance that you specify. The CDP distance determines the depth of the discovery. With a CDP distance of 1, only the immediate neighbors of the seed device are discovered. With a CDP distance of 2, devices A and B that are directly connected to the seed device are discovered, and the immediate neighbors of A and B are also discovered. You should set the CDP distance so that your entire wireless network is discovered.

After devices are discovered, you must move them to the managed state. Unmanaged devices do not appear in WLSE displays.

**Related Topic**

[Importing Devices, page 6-21](#)

[Managing Devices, page 6-13](#)

## Set Up Devices

You must set up devices so the WLSE can discover and manage them. This section describes both required and optional setup tasks for:

- [Access Points and Bridges, page 6-4](#)
- [Routers and Switches, page 6-7](#)
- [LEAP Servers, page 6-9](#)

### Access Points and Bridges

Before you begin, Web browsing must be enabled on each access point. If Web browsing is not enabled, attach a console to the access point and enable web browsing.

On each access point and bridge, open a web browser session on the device and perform the tasks in the following table.

Tasks	Procedure	Notes
1. Enable Cisco Discovery Protocol (CDP).	<ol style="list-style-type: none"> <li>1. In the Summary Status page, click <b>Setup</b>. The Cisco Services Setup page appears.</li> <li>2. Under Services: Cisco Services, click <b>Cisco Discovery Protocol</b>. The CDP Setup page appears.</li> <li>3. Select Enabled. Click <b>Apply</b> or <b>OK</b>.</li> </ol>	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.	<ol style="list-style-type: none"> <li>1. In the Summary Status page, click <b>Setup</b>. The Cisco Services Setup page appears.</li> <li>2. Under Services, click <b>SNMP</b>. The SNMP Setup page appears.</li> <li>3. Select Enabled.</li> <li>4. Enter a System Name, System Location, and System Contact.</li> <li>5. Click <b>Apply</b> or <b>OK</b>.</li> </ol>	<p>SNMP is required for the WLSE to discover and manage the device.</p> <p>Setting the location enables proper grouping of devices into the system-defined Location group. For more information, see <a href="#">Managing Groups, page 6-28</a>.</p> <p>Setting the system name and system location displays this information when you display device details.</p>

Tasks	Procedure	Notes
<p>3. Set the community string by creating a user with all privileges.</p> <p>(If you already entered an SNMP Admin Community name, the user created has Write, SNMP, Firmware, and Admin privileges, and the User Manager is enabled, you do not need to create another user.)</p>	<ol style="list-style-type: none"> <li>1. In the Summary Status page, click <b>Setup</b>. The Cisco Services Setup page appears.</li> <li>2. Under Services, click <b>Security</b>. The Security Setup page appears.</li> <li>3. Click <b>User Information</b>; then click <b>Add New User</b>. The User Management window appears.</li> <li>4. To create a user with SNMP read/write privileges, enter a username and password and select the Write, SNMP, Firmware, and Admin capabilities.</li> <li>5. Click <b>Apply</b> or <b>OK</b>.</li> </ol>	<p>The username of the user with Write and SNMP privileges is used as the SNMP read/write community string.</p> <p>The Firmware privilege is required for configuring devices from the WLSE.</p>

Tasks	Procedure	Notes
<p>4. Add an HTTP user with the ability to modify firmware, and enable the User Manager.</p> <p>You can use the same user that you created in Task 3, if the user has firmware privileges.</p>	<ol style="list-style-type: none"> <li>1. In the Summary Status page, click <b>Setup</b>. The Cisco Services Setup page appears.</li> <li>2. Click <b>Security</b>. The Security Setup page appears.</li> <li>3. Click <b>User Information</b>; then click <b>Add New User</b>. The User Management window appears.</li> <li>4. Enter a username and password and select Firmware; then click <b>Apply</b>.</li> <li>5. Navigate back to the Security Setup page and click <b>User Manager</b>. The User Manager Setup window appears.</li> <li>6. Select Enabled; then click <b>Apply</b> or <b>OK</b>.</li> </ol>	<p>This allows configuration uploads from the WLSE to the access point.</p> <p>All access points must be configured with the same HTTP user and password. You also enter this user and password on the WLSE (see <a href="#">Specify the HTTP Username and Password, page 6-20</a>).</p>
<p>5. Set up TFTP as the transfer protocol between the WLSE and access points.</p>	<ol style="list-style-type: none"> <li>1. In the Summary Status page, click <b>Setup</b>. The Cisco Services Setup page appears.</li> <li>2. Under Services, click <b>FTP</b>. The FTP Setup page appears.</li> <li>3. Use the pulldown menu to select TFTP as the file transfer protocol.</li> <li>4. In the Default File Server text box, enter the IP address of the WLSE.</li> <li>5. Click <b>Apply</b> or <b>OK</b>.</li> </ol>	<p>TFTP is used for transferring configuration changes to access points.</p>

## Routers and Switches



### Note

Only routers and switches that have properly configured access points or bridges attached to them will be discovered.

On each router and switch, configure the following:

Task	Procedure	Notes
1. Enable CDP and verify that access points and bridges are visible from the router or switch.	<ol style="list-style-type: none"> <li>1. Enter enable mode.</li> <li>2. Verify that CDP is running on the switch or router:  On IOS-based devices, use the <b>show cdp run</b> command.  On Hybrid OS-based Catalyst switches, use the <b>show cdp</b> command</li> <li>3. If CDP is not running, use the <b>set cdp enable</b> command to enable CDP.</li> <li>4. To verify that access points or bridges are visible in the device's CDP table, use the <b>show cdp neighbors</b> command.</li> </ol>	CDP is required for the WLSE to discover the device.

Task	Procedure	Notes
2. Enable SNMP and set up community strings.	<p>On IOS-based devices, enter configuration mode and use the <b>snmp community <i>community_string</i> ro</b> command.</p> <p>On Hybrid OS-based Catalyst devices, enter enable mode and use the <b>set snmp community read-only <i>community_string</i></b> command.</p>	SNMP is required for the WLSE to discover and manage the device.
3. (Optional) Set the system name, contact, and location variables.	<p>On IOS-based devices, enter configuration mode and use the following commands:</p> <ul style="list-style-type: none"> <li>• To set the system name, use the <b>hostname <i>name</i></b> command.</li> <li>• To set the system contact, use the <b>snmp contact <i>contact</i></b> command.</li> <li>• To set the location, use the <b>snmp location <i>location</i></b> command.</li> </ul> <p>On Hybrid OS-based Catalyst switches, enter enable mode and use the following commands:</p> <ul style="list-style-type: none"> <li>• To set the system name, use the <b>set system name <i>name</i></b> command.</li> <li>• To set the system contact, use the <b>set system contact <i>contact</i></b> command.</li> <li>• To set the location, use the <b>set system location <i>location</i></b> command.</li> </ul>	<p>These variables make the device more manageable. The location variable enables proper grouping of devices into the system-defined Location group. For more information about groups, see <a href="#">Managing Groups, page 6-28</a>.</p> <p>The system name, system contact, and location will appear in the device detail displays.</p>

## LEAP Servers

The WLSE can monitor a [LEAP server](#) (CiscoSecure ACS Server) that provides LEAP services to a wireless LAN using synthetic transactions.

**Note**

Each LEAP server must be specified on the WLSE. For more information, see [Managing LEAP Servers, page 6-26](#).

**Procedure**

To set up a LEAP server and add the WLSE as a Network Access Server (NAS) on the LEAP server:

- Step 1** Log into the CiscoSecure ACS Server.
- Step 2** Click **User Setup** on the left side of the initial page. The User Setup page appears.
- Step 3** In the User text box, enter the name of the user that the WLSE will use for synthetic transactions.
- Step 4** Click **Add/Edit**; then enter the appropriate information for the user, including the password. Click **Submit**.
- Step 5** Click **Network Configuration** on the left side of the page. The Network Configuration screen appears.
- Step 6** Click **Add Entry**. The Add Access Server screen appears.
- Step 7** Enter the WLSE information in the following text boxes:
  - Network Access Server Hostname
  - Network Access Server IP
  - Key (the shared key)
- Step 8** Select RADIUS (Cisco Aironet) from the Authenticate Using list.
- Step 9** Click **Submit** or **Submit+Restart**. A restart is required for the changes to take effect.

## Add Seed Devices and Schedule Discovery

Neighbors of seed devices are discovered by examining the contents of CDP tables. Before discovery can proceed, you must specify at least one seed device. Any supported device can function as a seed.

You may want to specify multiple seed devices to:

- Shorten the discovery time.
- Discover “disconnected” networks; that is, discover devices across links on which CDP is disabled or discover devices outside the firewall.



**Note**

---

Your login determines whether you can use this option.

---

### Procedure

**Step 1** Select **Administration > Discover > DISCOVER > Modify Discovery Settings**.

**Step 2** To delete a seed device, select the IP address from the Seed Values list and click **Delete**.

**Step 3** To add a seed device, enter its IP address in the Seed Values text box and click >>.



**Note**

---

Before you can modify the discovery schedule, you must have at least one seed device in the Seed Values list.

---

**Step 4** Repeat step 3 to add more seed devices.

**Step 5** Select the **CDP distance** from the list. Set CDP distance appropriately to discover the entire wireless network; a CDP distance of 1 only discovers the immediate neighbors of the seed devices.



**Note**

---

Routers and switches that do not have access points attached to them are used when computing CDP distance. However, such devices will not appear in the discovered devices list.

---

**Step 6** To schedule discovery, click **Next: Modify Schedule**. The Modify Discovery Schedule dialog box appears.

- Select the State Date and Start Time from the pulldown lists.
  - To repeat discovery at specified intervals, click **Enable**. Then enter a number and select the interval from the Every list.
- Step 7** Click **Next**. The CDP Discovery - Summary dialog box appears.
- Step 8** Click **Finish** to submit your settings or **Back** to make changes in your settings.
- 

## Run Discovery Now

This option allows you to run an immediate one-time discovery.



### Note

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Administration > Discover > DISCOVER > Run Discovery Now**. The Discovery - Seeds dialog box appears.
- Step 2** If necessary, add seed devices:



**Note** If you add seed devices in the Discovery - Seeds dialog box, they will not be saved. Any seed devices added here are used for this one-time discovery only.

---

- a. Enter the seed device's IP address in the Add Seed Value text box and click >>.
  - b. Set the [CDP distance](#) by selecting a number from the list.
- Step 3** Click **Run Now**. The Discovery - Summary dialog box appears.
- Click **Back** if you want to make changes.
  - Click **Finish** to run the discovery. The discovery will begin within 2 minutes.
-

## View Discovery History and Status

The Discovery History table shows completed and scheduled discovery jobs.



### Note

Your login determines whether you can use this option.

### Procedure

- Step 1** Select **Administration > Discover > DISCOVER > Discovery History**. The Discovery History table appears:

Field	Description
Discovery Name	The job name. The scheduled discovery is called CDPDiscovery. One-time discoveries and discoveries initiated by device imports are called CDPDiscovery_type_number; for example, CDPDiscovery_Import_Devices_4.
Recurring	Whether the job is recurring.
Schedule Time	The next time the job will run.



### Note

If the Discovery History table grows too large, you can reset the Job History Truncation Interval parameter in **Administration > System Parameters** so that the table is truncated more often. For more information on this parameter, see [Managing System Parameters, page 6-59](#).

- Step 2** From the Discovery State list, select the discoveries you want to view: scheduled discoveries, discoveries that are currently running, or all discoveries. The Discovery History table is displayed.
- Step 3** To view more information about a discovery in the Discovery History table, select the radio button and click **Discovery Run Detail**. This Discovery Run Details window appears, showing the Discovery Start and End times.

- Step 4** To view the detailed log for a particular discovery run, select the run and click **Discovery Run Log**. The following information is displayed in the Discovery Run Log:
- The seed devices used.
  - The [CDP distance](#) configured for the seed devices.
  - When the discovery started and ended (displayed as [UTC](#)).
  - The number of devices that were discovered or rediscovered.
  - A list of the devices that were discovered. Devices listed as *being updated* were already discovered in a previous discovery run.
  - A list of devices that were previously discovered but are now unreachable.
  - Devices that are unreachable because CDP is not enabled on the device or SNMP is not configured on the device.
- Step 5** 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.
- 

## Managing Devices

Before you can view devices or perform any operations on them, you must move the devices to the managed state. The device management options are:

- **Manage/Unmanage**—View newly discovered devices, change device management status, or delete devices (see [Manage Devices, page 6-13](#)).
- **Device History**—View the management history of each discovered device (see [View Device Management History, page 6-16](#)).

## Manage Devices

You can use this option to change a device's management status or delete a device.



---

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

---

### Procedure

---

**Step 1** Select **Administration > Discover > Managed Devices > Manage/Unmanage**. The device selector is displayed, showing:

- Newly discovered devices (New folder). All new devices are also listed in the Unmanaged folder.
- Managed devices (Managed folder)
- Unmanaged devices (Unmanaged folder).

**Step 2** To view the contents of a folder, expand the folder.

**Step 3** To modify the status of the devices in a folder, click the folder name. The Group Status pane appears. Select one or more devices from the list and click **Manage** or **Unmanage** in the Group Change Status window. Devices are moved into the Managed or Unmanaged folders.

You must move newly discovered devices to the managed state. Only managed devices appear in WLSE displays.



---

**Note** You can only manage a total of 525 access points and wireless bridges. After you have placed 500 of these devices into the Managed folder, warning messages are displayed when you place more devices in the folder. After the 525 limit is reached, no more devices can be placed in the Managed folder. Discovery of access points and wireless bridges is not limited to 525 devices.

---

**Step 4** After you move devices to the managed state, it is recommended that you run inventory. This ensures that devices appear in displays such as reports and system-defined groups without waiting for the next inventory cycle. To run inventory:

- a. Select **Administration > Discover > DISCOVER > Inventory**.
- b. Click **Run Inventory**.

For more information, see [Running Inventory Now, page 6-17](#).

- Step 5** To view details about a device, select the device from the device selector. The Device Details pane appears. You can change the device's status by using the Manage and Unmanage buttons.



**Note** Some details may not be displayed if the corresponding parameters are not set on the device; for example, Location and Contact.

The details in the Device Details pane are:

Field	Description
Device Name	Hostname, IP address, or SNMP sysname.
Description	Detailed device description.
Version	Software version installed on the device.
Device Family	Device type.
SysName	The system name.
SysObjectId	Unique identifier that identifies the device type.
Location	Where the device is located.
IP Address	Device IP address.
Subnet	Subnet in which the device is located.
Network Segment	The network segment in which the device is located.
Contact	The person to contact for this device.

- Step 6** To delete a device, select the device from the device selector or dialog box and click **Delete**.
- The device will be removed from the device selector and from all tables (including trend tables).

### Related Topics

[Managing Device Discovery, page 6-2](#)

[Device Name Display on the WLSE, page 1-3](#)

## View Device Management History

The Historical Operations table shows information on all changes in device state (from unmanaged to managed or vice versa).



### Note

Your login determines whether you can use this option.

### Procedure

- Step 1** To view the Historical Operations table, select **Administration > Discover > Managed Devices > Device History**. The following information is displayed:

Field	Description
Timestamp	Date and time when the state change occurred.
Device Name	The device's hostname.
IP Address	The device's IP address.
State	The device's state: <ul style="list-style-type: none"> <li>• New—Device was discovered but has not been moved to the managed or unmanaged state.</li> <li>• Managed—Device has been moved to the managed state.</li> <li>• Unmanaged—Device is unmanaged.</li> </ul>

- Step 2** To sort table data, click on the column heading by which you want to sort the data:
- A triangle indicates ascending order.
  - An upside-down triangle indicates descending order.
  - No triangle indicates that the data is not sorted.

## Running Inventory Now

By default, the WLSE collects device configuration information every hour. You can use this option to run a one-time, immediate inventory. Running an immediate inventory after you move devices to the managed state is recommended so you can see the devices in displays such as reports and system-defined groups, without waiting for the next scheduled inventory cycle.

To change the scheduled inventory interval, you can reset the Inventory Polling Interval parameter. See [Managing System Parameters, page 6-59](#).



---

**Note**

Your login determines whether you can use this option

---

### Procedure

---

- Step 1** Select **Administration > Discover > Inventory**.
- Step 2** Click **Run Inventory**. The inventory job will start within 2 minutes. A confirmation message appears, managed devices are polled, and configuration information is collected. WLSE displays will be updated accordingly.
- If a scheduled inventory or previous immediate inventory is already running, a message appears. You should wait for the running inventory to complete before starting another immediate inventory.
- 

## Setting Device Credentials

This option allows you specify device [community strings](#) and HTTP credentials.

- **SNMP Communities**—Specify community strings for managed devices. See [Specify Community Strings, page 6-18](#).
- **HTTP User/Password**—Specify the HTTP username and password for configuring access points. See [Specify the HTTP Username and Password, page 6-20](#).

## Specify Community Strings

The Wireless LAN Solution Engine uses a device's read-only community string for discovery and the read/write community string to configure the device. If community strings are not entered correctly, the Wireless LAN Solution Engine cannot communicate with the device. Both read-only and read/write community strings are required.

The default community string is *public* for both the read-only string and the read-write string. If the community strings on your devices differ from the defaults, you must specify the community strings before the discovery process can begin and before you can configure the devices.



### Note

---

Your login determines whether you can use this option.

---

### Procedure

- Step 1** Select **Administration > Discover > Device Credentials > SNMP Communities**. The Bulk SNMP Settings dialog box appears.

This dialog box contains a default entry that covers all devices, provided device community strings are set to the default (*public*).

- Step 2** Add new entries or modify existing entries in the text box using the following syntax:

```
target:read_community::timeout:retries:::write_community
```



### Note

---

You must enter the correct number of colons between variables. Otherwise, the community strings cannot be read.

---

Information about the variables follows. For more details, see [Community String Guidelines, page 6-20](#).

Variable	Description	Notes
target	A device or range of devices that use these community strings.	If you do not specify a target, the default community strings apply to all devices in the network.
read_community	A password allowing read-only access to the target devices.	You must specify a read community string. Otherwise, the default value of public is used.
timeout	The length of time (seconds) the server waits for a response from the device before performing the first retry.	The default is 10 seconds. If you increase the timeout period, discovery could take significantly longer to complete. The minimum value is one and the maximum value is 60.
retries	The number of times the server attempts to communicate with the device before declaring that the device has timed out.	The default is one retry. If you increase the number of retries, discovery takes significantly longer to complete. The default retry policy doubles the previous timeout value for retry.
write_community	The password that allows write access to the target devices.	You must specify the write community string. Otherwise, the default value of public is used.

- Step 3** Select **Reverse DNS Lookup** if DNS is configured on the device.
- If DNS Lookup fails, the device IP address will be used; however, discovery will take longer.
  - If DNS Lookup succeeds, the WLSE displays will show the device's hostname instead of the IP address in device name fields.
- Step 4** Click **Save** to apply your changes.
- 

#### Related Topic

[Community String Guidelines, page 6-20](#)

## Community String Guidelines

Use these guidelines when adding or modifying community strings:

- You can assign community strings to any of the following:
  - Complete IP address; for example, 172.20.4.9
  - Any wild cards (based on IP addresses); for example:  
\*. \*.\*.\*  
172.\*.\*.\*
  - Address ranges, which can include wild cards; for example:  
27.20.[4-55].\*  
172.[21-30].[44-88].\*  
172.\*.\*.[121-255]
- You can add a combination of general and specific entries, but the Wireless LAN Solution Engine reads the community strings from most specific to least specific.
- If you enter duplicate community strings for a device, the most specific community string is used.
- A # sign as the first character on a line indicates a comment.
- All printable characters, except for colons (:), are allowed in community strings.
- Spaces are not allowed in community strings.

## Specify the HTTP Username and Password

The HTTP username and password are required for downloading configuration files to access points. The password must be set on each access point. For more information, see [Set Up Devices, page 6-4](#).



---

**Note**

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1 Select **Administration > Discover > Device Credentials > HTTP User/Password**.
  - Step 2 Enter a username or modify the username in the User field.
  - Step 3 Enter or modify the password in the Password field.
  - Step 4 Enter or modify the password in the Confirm Password field.
  - Step 5 Click **Save**.
- 

### Related Topic

[Chapter 3, “Configuring Devices”](#)

## Importing Devices

Instead of running discovery on the WLSE, you can import devices:

- From a file (see [Import Devices from a File, page 6-22](#)).
- From CiscoWorks2000 Resource Manager Essentials (see [Import Devices from CiscoWorks2000, page 6-23](#)).

A one-time discovery job starts within 2 minutes after you import devices. All WLSE-supported devices in the file are used as seed devices with a [CDP distance](#) of 1. These devices are not added to the list of available seed devices in the Discovery - Configuring Seeds dialog box, but they do appear in the Discovery Run Log. See [Add Seed Devices and Schedule Discovery, page 6-10](#) and [View Discovery History and Status, page 6-12](#).

Devices not supported by the WLSE are ignored.

You can choose to discover some devices and import others.

The following information is imported:

- IP addresses are accepted, and hostnames are resolved to obtain the IP address. Hostnames that cannot be resolved are ignored.
- Read-only and read/write community strings are appended to the end of the Bulk SNMP Settings table (**Administration > Discover > Device Credentials**). See [Setting Device Credentials, page 6-17](#).



---

**Note** Imported credentials are not matched with existing entries that contain wildcards or ranges.

---

## Import Devices from a File

You can import devices from a file that contains device information in the CSV format. You can create a CSV file by exporting devices from CiscoWorks2000 or by creating the file with a text editor. You can view a sample CSV file in the dialog box for importing files.



---

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

---

### Procedure

---

- Step 1** Select **Administration > Discover > Import Devices > From File**. The Import Devices from File dialog box appears.
- To see a sample file, click **See Sample CSV File**.
- Step 2** You can enter a pathname for the file in the Choose File dialog box or click **Browse** to find the file in the client directory structure.
- Step 3** Click **Import**. Devices are imported and a one-time discovery begins within 2 minutes.
- Step 4** To verify the discovery, see [View Discovery History and Status, page 6-12](#).
- 

### Related Topics

- [Import Devices from CiscoWorks2000, page 6-23](#)
- [Add Seed Devices and Schedule Discovery, page 6-10](#)
- [Setting Device Credentials, page 6-17](#)
- [View Discovery History and Status, page 6-12](#)

## Import Devices from CiscoWorks2000

You can import devices directly from CiscoWorks2000 by connecting to a CiscoWorks2000 server.

The time required to import devices depends on the response from the CiscoWorks2000 server and the number of devices imported. The following procedure explains how to check the status of the operation.



### Note

---

Your login determines whether you can use this option.

---

### Procedure

---

**Step 1** Select **Administration > Discover > Import Devices > From CiscoWorks2000**.

**Step 2** Enter the following information. All fields are required; if any are left blank, the display will clear.

- The CiscoWorks2000 server IP address.
- The port number at which the CiscoWorks2000 server listens for HTTP requests. You may need to contact the administrator of the CiscoWorks2000 server to obtain this information.
- The username and password of any user who has the authority to export and import device credentials on the CiscoWorks2000 server.

Click **Import**. After devices are imported, a one-time discovery begins.

**Step 3** To see the Import Status log, click **Status**. The CiscoWorks2000 Import Status window appears. To refresh the status display, click **Refresh**.

- If the Last Status button is displayed in place of the Status button, you can review the results of a previous import.
- If the import fails because you entered the wrong data in the Import dialog box, one of the following error messages is included in the Import Status log:
  - The following message means that either the host or the port specified in the WLSE import dialog was wrong:

Error: Could not connect to CiscoWorks2000 server:*ip\_address* on port:*port\_number*.

- The following message means that either the user or password specified in the WLSE import dialog was wrong:

Error: Connected to CiscoWorks2000 server:*ip\_address* on port:*port\_number* successfully, but server returned error after connection.

- If the import succeeds, you can view detailed information in the Discovery Run Log. See [View Discovery History and Status, page 6-12](#).

---

### Related Topics

- [Import Devices from a File, page 6-22](#)
- [Add Seed Devices and Schedule Discovery, page 6-10](#)

## Exporting Devices

You can export all WLSE-discovered devices to a CiscoWorks2000 server running Resource Manager Essentials. The information exported consists of the device IP addresses and their credentials.

The time required to export devices depends on the number of devices exported and the response from the CiscoWorks2000 server. The following procedure explains how to check the status of the operation.



### Note

Your login determines whether you can use this option.

---

### Procedure

- Step 1 Select **Administration > Discover > Export Devices > To CiscoWorks2000**.
- Step 2 Enter the following information:
  - The CiscoWorks2000 server IP address.
  - The CiscoWorks2000 server port number. You may need to contact the administrator of the CiscoWorks2000 server.
  - The username and password of any user who has the authority to export and import device credentials on the CiscoWorks2000 server.

**Step 3** Click **Export**.

The Export to CiscoWorks2000 Started window appears.

**Step 4** To see the export status log, click **Status**. The CiscoWorks2000 Export Status window appears. To refresh the status display, click **Refresh**.

If the Last Status button is displayed in place of the Status button, you can review the results of a previous export.

The following information is included in the export status log:

Type of Information	Description
Device information	Name of the device, device status, and device status details. The string !{[NO VALUE]}! does not indicate an error; it means information was not available to the CiscoWorks2000 server while it was sending a response to the WLSE.
Error messages	The following message means that either the host or the port specified in the WLSE export dialog was wrong: Error: Could not connect to CiscoWorks2000 server: <i>ip_address</i> on port: <i>port_number</i> . The following message means that either the user or password specified in the WLSE export dialog was wrong: Error: Connected to CiscoWorks2000 server: <i>ip_address</i> on port: <i>port_number</i> successfully, but server returned error after connection.

After you export devices, you can view the exported devices in CiscoWorks2000 Resource Manager Essentials (see the Resource Manager Essentials online help for details).

## Managing LEAP Servers

This window allows you to manage LEAP servers (CiscoSecure ACS Servers). LEAP servers monitor the authentication servers, detecting performance problems and ensuring availability. LEAP servers must be configured for synthetic transactions.

After you save LEAP server credentials, the WLSE automatically performs periodic LEAP logins to monitor the response time and availability of LEAP servers. To change the default polling interval and fault thresholds, select **Faults > Specify Fault Thresholds > LEAP > Response Time**.

A LEAP server must be set up for LEAP logins. For information on setting up LEAP servers, see [Set Up Devices, page 6-4](#).

You can use the LEAP server options to:

- [Add a LEAP Server, page 6-26](#)
- [Modify a LEAP Server, page 6-27](#)
- [Remove a LEAP Server, page 6-28](#)

### Related Topics

- [Setting LEAP Server Response Time, page 2-12](#)
- [Displaying Faults, page 2-1](#)
- [Specifying Fault Thresholds, page 2-7](#)
- [Specifying Policies, page 2-13](#)
- [Forwarding Faults, page 2-15](#)

## Add a LEAP Server



### Note

---

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1** Select **Administration > Discover > LEAP SERVER > Add Server**. The LEAP Server: Add Server dialog box appears.

**Step 2** Complete the following:

Text Box	Description
Server Name	Enter the name of the server.
Server Port	Enter the number of the port the server uses for authentication.
Username	Enter the LEAP username.
Password	Enter the LEAP password.
Secret	Enter the shared secret key.

**Step 3** Click **Submit** to apply your settings, or **Reset** to apply the default values.

## Modify a LEAP Server



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

### Procedure

**Step 1** Select **Administration > Discover > LEAP Server > Modify Server**. The LEAP Server: Modify Server dialog box appears.

**Step 2** Modify attributes as desired:

Text Box	Description
Server Name	From the list, select the server name you want to modify.
Server Port	Modify the port number used for authentication.
Username	Change the LEAP server name.
Password	Change the LEAP password
Secret	Change the shared secret.

Step 3 Click **Submit** to apply your settings, or **Reset** to apply the default values.

---

## Remove a LEAP Server



### Note

Your login determines whether you can use this option.

---

### Procedure

---

- Step 1 Select **Administration > Discover > LEAP Server > Remove Server**. The LEAP Server: Remove Server dialog box appears.
- Step 2 From the list, select the server you want to remove, then click **Submit**.
- 

# Managing Groups

This window contains a group selector and a dialog box for creating, editing, and deleting groups.

### Related Topics

- [Overview: Groups, page 6-28](#)
- [Creating, Editing, and Deleting Groups, page 6-29](#)

## Overview: Groups

The Group Management window allows you to view the existing device groups and categorize devices into named groups so that you can perform management tasks on a group of devices as a single operation.

A group is a named entity consisting of a set of devices, a set of groups, or a combination of devices and groups. A group can consist of both user-defined groups and system-defined groups.

There are five folders containing system-defined groups. You cannot edit or delete a system-defined group. The system defined groups are automatically populated using information read from the devices during discovery and inventory collection. Any changes on devices are reflected in the system-defined groups only after the next discovery or inventory collection has completed. The system-defined groups and folders are:

- Device Type folder—Contains groups for 1200 APs, 340 APs, 350 APs, 350 Bridges, Routers, and Switches.
- Location folder—Contains groups based on the locations of the devices. To enable creation of system-defined location groups, you must configure a parameter on the device that identifies the device location. See [Set Up Devices, page 6-4](#) for information on setting location. The null location group contains all devices that are not configured with their location information.
- SSID folder—Contains a group for each radio service set ID (SSID) configured on access points. For information on configuring the SSID, see [Set Up Devices, page 6-4](#)
- Subnet folder—Contains a group for each subnet configured in the network.
- Software Version folder—Contains a group for each software version detected on the devices.

#### Related Topics

- [Managing Device Discovery, page 6-2](#)
- [Running Inventory Now, page 6-17](#)

## Creating, Editing, and Deleting Groups

You can create groups and edit or delete groups that were created by users. The system-defined groups cannot be edited or deleted.

Use the options in the Group Management window to:

- [Add a Group, page 6-30](#)
- [Edit a Group, page 6-32](#)
- [Delete a Group, page 6-33](#)

To view the devices in a group, select **Administration > Group Management**. Click a group folder in the group selector in the left pane. The group name, description, creator, and devices are listed in the Group window.

## Add a Group

You can add groups by:

- [Creating a New Group, page 6-30](#)
- [Copying an Existing Group, page 6-31](#)



### Note

---

Your login determines whether you can use this option.

---

## Creating a New Group

### Procedure

- 
- Step 1** Select **Administration > Group Management**. The group selector pane and group window are displayed.
- The group selector lists all the current groups, both system-defined groups and user-defined groups. The number after a group name or folder shows how many devices are in the group or how many groups are in the folder. Every managed device appears in one or more of the system-defined groups, and may also appear in user-defined groups.
- Step 2** To create a new group, click **Create New**. The Create Group dialog appears.
- Step 3** Enter a name in the Name text box. Enter a description in the Description text box (optional).
- For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).
- Step 4** From the group selector in the left pane, select a group that contains devices you want to add to your new group. Devices in that group are added to the All Available Devices list in the Create Group dialog.
- Step 5** To add devices to the new group, select the group or individual devices from the All Available Devices list and click **Add >>**. Devices are moved to the Devices in Group list.

- Step 6** To add more devices to the new group, repeat Steps 4 and 5.
  - Step 7** To remove devices from the group, select them from the Devices in Group list and click **Remove**.
  - Step 8** To save the group, click **Save**. The new group is displayed and added to the end of the group selector list. To cancel the group creation and discard your changes, click **Cancel**.
- 

## Copying an Existing Group

Use this procedure to create a new group by copying an existing group.

### Procedure

---

- Step 1** Select **Administration > Group Management**. The group selector pane and group dialog box are displayed.  
  
The group selector lists all the current groups, both system-defined groups and user-defined groups. The number after a group name or folder show how many devices are in the group or how many groups are in the folder. Every discovered and managed device appears in one or more of the system-defined groups, and may also appear in user-defined groups.
- Step 2** To copy an existing group, select the group and click **Copy**. The Copy Group dialog appears. The devices in the group are placed in the Devices in Group list.
- Step 3** Edit the name, if desired. Add a description in the Description text box (optional).  
  
For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).
- Step 4** To add more devices to the group, select another existing group. Devices in that group are added to the All Available Devices list in the Create Group dialog.
- Step 5** Select the group or individual devices from the All Available Devices list and click **Add >>**.
- Step 6** To add more devices, repeat Steps 4 and 5.
- Step 7** To remove devices from the group, select them from the Devices in Group list and click **Remove**.

- Step 8** To save the group, click **Save**. The new group is displayed and added to the end of the group selector list. To cancel the group creation and discard your changes, click **Cancel**.
- 

#### Related Topics

- [Edit a Group, page 6-32](#)
- [Delete a Group, page 6-33](#)
- [Overview: Groups, page 6-28](#)

## Edit a Group

You can edit user-defined groups, but system-defined groups cannot be edited.



#### Note

Your login determines whether you can use this option.

---

#### Procedure

---

- Step 1** Select **Administration > Group Management**. The group selector pane and Group dialog box appear.
- Step 2** Select a group to edit from the group selector in the left pane and click **Edit**. The Edit Group dialog appears.
- Step 3** Change the Name or Description by editing the text in the text boxes.  
For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).
- Step 4** To add devices to the group, select a group from the group selector. The devices in the group appear in the All Available Devices list. Select the group or individual devices from the list and click **Add**. Devices are placed in the Devices in Group list.
- Step 5** To add more devices, repeat Step 4.
- Step 6** To delete devices from the group, select one or more devices from the Devices in the Group list and click **Remove**.

- Step 7** To save your changes, click **Save**. The edited group is displayed. To discard your changes, click **Cancel**.
- 

#### Related Topics

- [Add a Group, page 6-30](#)
- [Delete a Group, page 6-33](#)
- [Overview: Groups, page 6-28](#)

## Delete a Group



#### Note

You can delete user-defined groups, but you cannot delete system-defined groups.

---

Your login determines whether you can use this option.

---

#### Procedure

---

- Step 1** Select **Administration > Group Management**. The group selector appears in the left pane and the Group window appears.
- Step 2** Select the group from the group selector list. The group is displayed.
- Step 3** Click **Delete**.
- 

#### Related Topic

- [Overview: Groups, page 6-28](#)
- [Edit a Group, page 6-32](#)
- [Add a Group, page 6-30](#)

# Managing the Appliance

The Appliance window contains the following options:

- **Status**—Gather and view WLSE statistics and restart the machine (see [Viewing WLSE Status, page 6-34](#)).
- **Software**—Update, reinstall, view status, and define the repository for the WLSE software (see [Managing the Software, page 6-37](#)).
- **Security**—Manage the WLSE security features, such as telnet, SSL, authentication modules (see [Managing Security, page 6-45](#)).
- **Backup and Restore**—Configure backup location, backup data, and restore data (see [Backing Up and Restoring Data, page 6-50](#)).
- **Diagnostics**—Troubleshoot, run self-tests, view process status (see [Using Diagnostics, page 6-54](#)).
- **Splash Screen**—Customize the splash screen message (see [Setting Up the Splash Screen Message, page 6-58](#)).



Note

---

Your login determines whether you can use these options.

---

## Viewing WLSE Status

The Status options include:

- Log file statistics (see [Viewing Log File Reports, page 6-35](#)).
- Restart (see [Restarting the Wireless LAN Solution Engine, page 6-36](#)).

## Viewing Log File Reports

This option allows you to gather and view file system statistics.

### Procedure

- Step 1** Select **Administration > Appliance > Status > View Log File**. The Log File Utilities dialog box appears with the following information:

Field	Description
Log file	Name of the log file displayed.
Directory	Location of log file.
File Size	Size of file.
Size Limit	Recommended maximum file size.
File Size Utilization %	Percentage of the maximum size (500MB) being used.

- Step 2** To see log file details, click the name of the log file. A window appears with log file information.
- Step 3** To search for specific data within the log files, click the check boxes of the log files you want to search, and enter a keyword into the **Keyword** text box. Click **Case Sensitive** if you want your search to be case sensitive, then click **Search**. A window displays the results of the search.

## Log Files Displayed

Log File	Content
access_log	Web server user access log.
daemons.log	Log file for logging messages that dmgttd does not log.
dmgttd.log	Process Management daemon log file.
error_log	Web server error log.

Log File	Content
faults.log	Log for device fault information.
install.log	Software package installation log.
jobvm.log	Log for all scheduled tasks.
mfgtest.log	Log for the manufacturing test.
mod_jk.log	Message log for hook between Tomcat and Apache.
snmpd.log	SNMP agent log file.
ssl_request_log	Log for secure socket layer web server events for https.
tomcat.log	Java servlet messages.

## Restarting the Wireless LAN Solution Engine

This option allows you to restart the WLSE.

After the Wireless LAN Solution Engine restarts, discovery (see [Managing Device Discovery, page 6-2](#)) will begin immediately, the performance thresholds will resume collecting, the views will update, and all other functions will resume.

### Procedure

- 
- Step 1** Select **Administration > Appliance > Status > Restart**. The Restart System screen appears.
- Step 2** Click **OK** to restart the Wireless LAN Solution Engine.




---

**Note** If you need to perform a manual soft restart (for example, when modifying a network interface) you can use the CLI commands. (Refer to *User Guide for the CiscoWorks1105 Wireless LAN Solution Engine*—From the Online Help, click **View PDF**.)

---

## Managing the Software

The Software options include:

- **Status**—Currently installed software information, such as software description, installation date, and installation status (see [Viewing Software Status](#), page 6-37).
- **Define Repository**—Specify the repository location. The repository provides software update services to the WLSE (see [Defining the Repository](#), page 6-38).
- **Software Updates**—Select and install a software update from the repository. You must specify the repository before updating software so the Wireless LAN Solution Engine can locate the software updates (see [Installing Software Updates](#), page 6-41).
- **Browse Repository**—Browse the available complete images and software upgrades on the repository (see [Browsing the Repository](#), page 6-43).
- **Software Update History**—Information about current and previous versions of installed software, including version number, install date, and installation status (see [Viewing Software Update History](#), page 6-44).

## Viewing Software Status

### Procedure

- Step 1** Select **Administration > Appliance > Software > Status**. The Software Status window appears with the Installed Software table, which contains the following information about all the software currently installed on the Wireless LAN Solution Engine:

Field	Description
Software Name	Brief description of the software.
Installation Date	Date and time (UTC) the software was installed.
Status	Status of the installation.
Details	Detailed install log for this software.

The Last Installation Information table displays the following about the most recent software installation:

Field	Description
Name	Brief description of the software.
Installation Status	Status of the installation.
Log File	Detailed install log for this software.

**Step 2** To view details about an installation, click **View Log** in the Details field.

The install log for the selected installation opens. The information about the latest software installed is displayed.

#### Related Topics

- [Viewing Software Update History, page 6-44](#)
- [Installing Software Updates, page 6-41](#)
- [Managing the Software, page 6-37](#)

## Defining the Repository

The repository warehouses the available software updates for the WLSE. The repository can be either local (on the Wireless LAN Solution Engine), or remote (on a Windows NT or Windows 2000 server). The default is a local repository.

By defining the repository, you are telling the WLSE where to look for available software updates. You can download software from the repository and install it on the Wireless LAN Solution Engine, and you can browse the available software versions on the repository.

However, before you can define the repository using the GUI, you must first create the repository:

- To create a local repository, see [Creating a Local Repository, page 6-39](#).
- To create a remote repository, see [Creating a Remote Repository, page 6-40](#).

## Procedure

- Step 1** Select **Administration > Appliance > Software > Define Repository**. The Define Repository dialog box appears.
- Step 2** To define or redefine the repository, complete the following:

Text Box	Description
Host Name	The hostname or IP address of the repository. For the local repository, enter <code>localhost</code> .
Port Number	The port number used by the software on the repository. The default port number for the local repository is 9851.
Description	A description of the repository. This text box is optional; you can enter any description.

- Step 3** Click **Connect to Repository** to verify that the hostname and port number you entered are correct. If the data is incorrect, an error message appears.

## Related Topics

- [Installing Software Updates, page 6-41](#)
- [Browsing the Repository, page 6-43](#)
- [Managing the Software, page 6-37](#)

## Creating a Local Repository

The repository warehouses the available software updates for the Wireless LAN Solution Engine. A single Wireless LAN Solution Engine can serve as the repository for itself and multiple other Wireless LAN Solution Engines.

To create a local repository, configure the repository using the [CLI](#).



### Note

To use the local repository, you must be downloading software updates from an FTP site.

For more information, see *Installing and Configuring the Cisco 1105 Wireless LAN Solution Engine*, “Updating your Wireless LAN Solution Engine” section.

### Procedure

---

- Step 1** Open a [CLI](#) window to the Wireless LAN Solution Engine.
- Step 2** Specify the source of the software updates. Use the following CLI command:

```
repository source ftp://hostname/path
```

The FTP site is the source for downloading software updates.

- Step 3** Find the software you want on the FTP site.
- Step 4** Download the software you want from the FTP site to the repository using the following command:

```
repository add package
```

---

## Creating a Remote [Repository](#)

The repository warehouses the available software updates for the Wireless LAN Solution Engine. A remote repository can serve as the repository for one or more Wireless LAN Solution Engines. One Wireless LAN Solution Engine can function as the remote repository for other Wireless LAN Solution Engines, or the remote repository can be a Windows NT or Windows 2000 server. (A remote repository created on a Windows NT or Windows 2000 server will be temporary. It will not exist after the server reboots.)



### Note

If you are using a Wireless LAN Solution Engine as a remote repository, see [Creating a Local Repository, page 6-39](#).

---

### Procedure

---

- Step 1** Download the ZIP file containing the update. The latest updates can be found at [ftp.cisco.com](http://ftp.cisco.com).

**Step 2** Extract the file to any empty directory. For example, extract the file to C:\hse\hse\_repository.

**Step 3** Open a command window and enter the following command:

```
subst <drive2:><drive1:>\<path>
```



---

**Note** Drive2 is a virtual drive. It will be removed after rebooting the Windows 2000 or Windows NT machine.

---

**Step 4** Open <drive2:>.

**Step 5** If Autoplay is enabled, the autorun.bat file will automatically run. If it does not, double-click it. A browser window opens, displaying the Appliance Update screen.

**Step 6** Enter the hostname or IP address of the appliance.

The remote repository is now on the Windows NT or Windows 2000 server. To install software updates from this repository, see [Installing Software Updates, page 6-41](#).

---

#### Related Topic

[Creating a Local Repository, page 6-39](#)

## Installing Software Updates



---

**Note** When you update or reinstall software, the Wireless LAN Solution Engine stops and restarts. Therefore, you cannot access the Wireless LAN Solution Engine during a software update, and you must log in again after updating software.

---

#### Procedure

---

**Step 1** Select **Administration > Appliance > Software > Install Software Updates**. The Install Software Updates window opens and displays information about the Wireless LAN Solution Engine, the currently defined repository, and the compatible software available for updating.

- Step 2** Select a software version from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.

These tables display the following information about the software you can install.

Field	Description
Name	Software identifier.
Version	Version number of the software.
Summary	Brief description of the software.
Release Date	Release date of the software.
Details	Detailed description of the software.

- Step 3** To view details about any of the listed software, click **README** in the Details field.
- Step 4** To begin the installation, make a selection from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.
- Step 5** To install the selected software, click **Install**. The Install Software Updates window opens.
- Step 6** Click **Confirm** to continue the installation. Click **Cancel** to cancel the installation.

When the installation is complete, the WLSE will be unavailable for a few minutes while it restarts. The Login screen will appear when the update is complete.

You can view details of the installation after the installation is complete (**Software > Status > View Log**).

### Related Topics

- [Defining the Repository, page 6-38](#)
- [Viewing Software Status, page 6-37](#)
- [Viewing Software Update History, page 6-44](#)
- [Browsing the Repository, page 6-43](#)
- [Managing the Software, page 6-37](#)

## Browsing the Repository

You can browse the available complete images and software upgrades on the repository using this option.



### Note

A repository must be defined in order to browse software. To define the repository, see [Defining the Repository, page 6-38](#).

### Procedure

- Step 1** Select **Administration > Appliance > Software > Browse Repository**. The Browse Repository dialog box appears.
- Step 2** To view detailed information about a complete image or update, click **README** in the Complete Images table or Updates table. These tables display the following about all the software available on the repository:

Field	Description
Name	Software identifier.
Version	Version number of the software.
Appliance Type	The appliance type that the software is designed for.
Release Date	Release date of the software.
Summary	Brief description of the software.
Details	Detailed description of the software. Click <b>README</b> to display details.

### Related Topics

- [Installing Software Updates, page 6-41](#)
- [Managing the Software, page 6-37](#)

## Viewing Software Update History

This window shows only the update history, not a history of installed images. If you install a complete new image, the previous update history will be erased.

### Procedure

- Step 1** Select **Administration > Appliance > Software > Software Update History**. The Software Update History window displays the following:

Field	Description
Name	Software identifier.
Version	Software version.
Summary	Summary of the installed software.
Install Date	The date and time ( <b>UTC</b> ) the software was installed.
Status	The status of the installed software.
Details	The detailed install log for this software.
Status	The status of the installation: Success—Software was installed with no errors. Warning—Software installed successfully with minor errors. Error—Software installation was unsuccessful.
Details	The detailed install log for this installation, including warning and error messages.

- Step 2** Click **View Log** in the Details field to view the detailed install log for a software installation.

### Related Topics

- [Viewing Software Status, page 6-37](#)
- [Browsing the Repository, page 6-43](#)
- [Managing the Software, page 6-37](#)

## Overview: Security

The WLSE provides the following security features:

- Optional secure connection through a Web browser
- Connection through the [CLI](#) via Telnet
- Secure connection through the CLI via SSH
- Authentication through the local database or through alternative authentication services
- Flexible user access to managed devices and Wireless LAN Solution Engine services through configurable roles.

You can manage your system's security by:

- [Selecting an Authentication Module, page 6-47](#)
- [Disabling or Enabling Telnet and Selecting SSH, page 6-49](#)
- [Viewing the Last 10 Logged-On Users, page 6-49](#)
- [Managing Roles, page 6-61](#)

## Managing Security

The Security options include:

- **Authentication Modules**—Choose the authentication module used (see [Overview: Authentication Modules, page 6-46](#)).
- **SSL (HTTPS)**—Obtain a permanent, signed Certificate Signed Request (see [Managing SSL \(HTTPS\), page 6-48](#)).
- **Telnet and SSH**—Configure Telnet and SSH settings (see [Disabling or Enabling Telnet and Selecting SSH, page 6-49](#)).
- **Last 10 Logins**—View information about the last 10 users who have logged on to the WLSE (see [Viewing the Last 10 Logged-On Users, page 6-49](#)).

## Overview: Authentication Modules

The Wireless LAN Solution Engine provides a mechanism for authenticating users through the local authentication module and a local database of user IDs and passwords. Many network managers, however, already have an authentication service. To use your own authentication service instead of the local module, you can select one of the alternative modules:

- TACACS+
- Radius
- MS NT Domain

After you select and configure a module, all authentication transactions are performed by the authentication service associated with that module. Users log in with the user ID and password associated with the current authentication module.

The Wireless LAN Solution Engine determines user roles; therefore, all users must be in the local database of user IDs and passwords. A user's role determines the services and devices that the user can access. Users must have the same user ID locally as they have in the alternative authentication source, but the local password and authentication service password do not have to be same.

Users who are authenticated by an alternative service and who are not in the local database have no roles assigned to them. Users who have no roles see only the splash screen after logging in and cannot view screens or perform tasks.

If the alternative authentication service fails, the Wireless LAN Solution Engine defaults to the Local authentication module. Even if the local user database fails, you can always log in as the admin user.

### Related Topics

- [Selecting an Authentication Module, page 6-47](#)
- [Administering Users, page 6-61](#)

## Selecting an Authentication Module

The Local login module is selected by default, but you can select a different module.

### Procedure

- 
- Step 1** Select **Administration > Appliance > Security > Authentication Modules**. The Authentication Modules dialog box appears.
- Step 2** Select an authentication module from the Select Module drop down list, then click **Submit**. A Configuration dialog box appears for all selections except the Local module.
- Step 3** Depending on the authentication module you selected, enter the following data, then click **Submit**:
- Radius module or TACACS+ module:
    - Primary Server and Secondary Server—IP addresses or DNS names of the primary and secondary authentication servers. A secondary server is optional.
    - Shared Secret—Secret key.
  - MS NT Domain module:
    - Domain—Name of the Windows domain.
    - Primary Domain Controller and Backup Domain Controller—Names of the primary and backup Windows domain controllers. A backup domain controller is optional.
- 

After you change the authentication module, you do not have to restart the Wireless LAN Solution Engine. Changing the module does not affect users who are currently logged on. Users who log on after the change use the new module.

### Related Topic

[Overview: Security, page 6-45](#)

## Managing SSL (HTTPS)

SSL (secure socket layer) protocol provides a secure connection between Web clients and the Wireless LAN Solution Engine. When you initially set up the Wireless LAN Solution Engine, an unsigned certificate and a CSR (Certificate Signed Request) are automatically generated and SSL is enabled. The unsigned certificate expires in one year. To obtain a permanent, signed certificate, use the following procedure.

**Note**

---

To establish a connection to the Wireless LAN Solution Engine using SSL, use the prefix `https` instead of `http` when entering the URL into the browser and do not append a port number to the URL.

---

**Procedure**

- 
- Step 1** Select **Administration > Appliance > Security > SSL (HTTPS)**. The SSL (HTTPS) dialog box appears.
  - Step 2** Click **View CSR**. The encrypted CSR is displayed.
  - Step 3** Copy the encrypted CSR (between the *begin* and *end* lines). Send the CSR to a certificate authority (such as Verisign), following the authority's procedure.
  - Step 4** When you receive the signed certificate:
    - a. Copy it into an ASCII file on a client system.
    - b. On the same client, select **Administration > Security**.
    - c. Under SSL (HTTPS), type the path to the signed certificate or click **Browse** to locate the file, then click **Submit Certificate**.
    - d. To use the new certificate, you need to restart the Wireless LAN Solution Engine by logging on through the **CLI**, running the **services stop** command to stop the system, then running the **services start** command to restart the system.
- 

**Related Topic**

[Overview: Security, page 6-45](#)

## Disabling or Enabling Telnet and Selecting SSH

Telnet is used for connecting to the Wireless LAN Solution Engine through the [CLI](#). By default, Telnet is enabled. To prevent unsecure connections through the CLI, you can disable Telnet.

SSH provides a secure Telnet connection, encrypting all traffic, including passwords. By default, both SSH1 and SSH2 are used.

### Procedure

---

- Step 1** Select **Administration > Appliance > Security > SSH and Telnet**. The SSH and Telnet control panel appears.
  - Step 2** To change the type of SSH used, select the desired SSH version from Select Protocol, then click **Change Protocol**.
  - Step 3** To enable or disable Telnet, make a selection from Telnet, then click **Configure**. Changes takes place immediately.
- 

### Related Topic

[Overview: Security, page 6-45](#)

## Viewing the Last 10 Logged-On Users

You can view information about the last 10 users who have logged on to the WLSE.

### Procedure

---

- Step 1** Select **Administration > Appliance > Security > Last 10 Logins**.  
The Last 10 Logins table appears, showing the following information for the last 10 logins.

Field	Description
Login Name	User's login name.
Logged In Since	Date and time the user logged in (GMT).
IP Address	IP address of the system from which the user logged in.
Associated role	Role assigned to the user.

#### Related Topic

[Overview: Security, page 6-45](#)

## Backing Up and Restoring Data

The Backup and Restore options include:

- **Backup**—Back up data, including all Wireless LAN Solution Engine role and user information (see [Backing Up Data, page 6-52](#)).
- **Restore**—Restore an available backup image (see [Restoring Data, page 6-53](#)).
- **Configure**—Set the backup location (see [Specifying the Backup Location, page 6-51](#)).
- **Using a Windows 2000 or Windows XP Server for backups**—see [Configuring a Windows 2000 or Windows XP Server as a Backup Location, page 6-52](#).

## Specifying the Backup Location

The backup location should be running an FTP server, because the Wireless LAN Solution Engine pushes the backed-up data to the FTP server.

### Procedure

---

**Step 1** Select **Administration > Appliance > Backup and Restore > Configure**.

**Step 2** Enter the hostname/IP for the backup location.

**Step 3** Enter the username you use on the backup location machine.

**Step 4** Enter the password you use on the backup location machine.

**Step 5** Reenter the password to verify that it is correct.

**Step 6** Optional—Specify the path to which the backup image is saved.

When specifying the path on a Windows 2000 or Windows XP server:

- Use either forward slashes (/) or backslashes (\) as the directory separators.
- Do not include the drive specifier (for example c:\) in the path specification.
- The path is relative to the ftproot.

**Step 7** Click **Save**.

---

### Related Topics

- [Backing Up Data, page 6-52](#)
- [Restoring Data, page 6-53](#)
- [Configuring a Windows 2000 or Windows XP Server as a Backup Location, page 6-52](#)

## Configuring a Windows 2000 or Windows XP Server as a Backup Location

To serve as a backup location, a Windows 2000 or Windows XP server must be configured for UNIX directory mode.

### Procedure

- 
- Step 1** On the server, select **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.
- If this option is not available on the server, enable it as follows:
- Select **Start > Settings > Control Panel > Add/Remove Programs**.
  - On the left side of the Add/Remove window, click **Add/Remove Windows Components**. The Windows Components wizard starts.
  - Check the checkbox for Internet Information Services, then click **Next**.
- Step 2** From the Tree panel, select the Windows 2000 or Windows XP system name.
- Step 3** In the Description panel, right-click **Default FTP Server**. Then click **Properties**.
- Step 4** In the Home Directory tab, click **UNIX** under Directory Listing Style.
- 

## Backing Up Data

Data backed up includes Wireless LAN Solution Engine role and user information, [seed](#) and discovery (see [Managing Device Discovery, page 6-2](#)) configuration information, and customized view information.



**Note** You should perform a backup every time you add a user, or whenever user views have changed.

### Procedure

- 
- Step 1** Configure the backup location (see [Specifying the Backup Location, page 6-51](#)).
- Step 2** Select **Administration > Appliance > Backup and Restore > Backup**.
- Step 3** Click **Backup**.

The WLSE saves the backup image.

- Step 4** To confirm that your data has been backed up, look at your backup location for a backup directory with saved `<WLSE hostname_date_time.inf` and `<WLSE hostname_date_time.tar` files.
- 

#### Related Topic

[Restoring Data, page 6-53](#)

## Restoring Data

#### Procedure

---

- Step 1** Select **Administration > Appliance > Backup and Restore > Restore**.
- Step 2** From the Available Images list, select a backup image. Images are listed by Wireless LAN Solution Engine hostname and date and time of backup.
- Step 3** Click **Restore**. The Restore Backup window opens.
- Step 4** Click **OK**.

The Wireless LAN Solution Engine shuts down and restarts while data is being restored.

---

#### Related Topics

- [Backing Up Data, page 6-52](#)
- [Specifying the Backup Location, page 6-51](#)

## Using Diagnostics

The Diagnostics options are:

- **WLSE Info**—Gather troubleshooting information about the WLSE status and create status reports (see [Viewing and Creating a Status Report, page 6-54](#)).
- **Self Test**—Create and display self tests (see [Viewing and Creating a Self-Test Report, page 6-55](#)).
- **Processes**—View WLSE processes status, stop and start processes (see [Viewing Processes, page 6-55](#)).

## Viewing and Creating a Status Report

You can gather troubleshooting information about the status of the Wireless LAN Solution Engine using this option.

Status reports show information about the product database status, product process status, log files, and so on.




---

**Note** Status reports reflect the [UTC](#) time.

---

### Procedure

- 
- Step 1** Select **Administration > Appliance > Diagnostics > WLSE Info**. The WLSE Information and Status Report dialog box appears.
  - Step 2** To display a report, click its name. If there are no reports listed, you must create a new report by clicking **Create**.
  - Step 3** To create a new report, click **Create**. It will take five to seven minutes for the report to be complete. To display the new report, click its name. If the new report is not listed, click **Refresh**.
  - Step 4** To delete a report, click the report check box, then click **Delete**.
- 

### Related Topics

- [Viewing and Creating a Self-Test Report, page 6-55](#)

- [Viewing Processes, page 6-55](#)

## Viewing and Creating a Self-Test Report

Self-tests include memory, database, DNS setup, and backup location configuration tests. Self-test reports indicate whether the tests passed or failed.



---

**Note** Self-test reports reflect **UTC** time.

---

### Procedure

---

- Step 1** Select **Administration > Appliance > Diagnostics > Self Test**. The WLSE Self-Test Report dialog box appears.
- Step 2** To display a report, click its name. If there are no reports listed, you must create a new report by clicking **Create**.
- Step 3** To display the new report, click its name. If the report is not displayed, click **Refresh**.
- Step 4** To delete a report, select the report check box, then click **Delete**.
- 

### Related Topics

- [Viewing and Creating a Status Report, page 6-54](#)
- [Viewing Processes, page 6-55](#)

## Viewing Processes

You can view the status of the major processes running on the Wireless LAN Solution Engine using this option. You can also start and stop processes and access complete reports.

### Procedure

---

- Step 1** Select **Administration > Appliance > Diagnostics > Processes**. The Process Report displays the following:

Column	Description
Process name	Describes how a process is registered.
State	Process status and a summary of the log file entries for the process.
Pid	Process ID. A unique number by which the operating system identifies each running program.
RC	Return code. “0” represents normal program operation. Any other number typically represents an error. Refer to the error log.
Signo	Signal number. “0” represents normal program operation. Any other number is the last signal delivered to the program before it terminated.
Start Time	Time (UTC) and date the process was started.
Stop Time	Time (UTC) and date the process was stopped.
Core	The entry “Not applicable” means the program is running normally.  The entry “Core file created” means the program is not running normally and the operating system has created a file called a core file. The core file stores important data about processes.
Information	The entry indicates what the process is doing. “Not applicable” means the program is not running normally.

**Step 2** Perform any or all of these tasks:

- To view details, click any process name. The [Daemon Information](#) window opens.
- To view process status, click any process state. The [System Log](#) window opens.
- To stop a process, select the check box next to the process name and click **Stop**. The Process Status table displays the new status and other process information. The [WebServer](#) and [Tomcat](#) processes cannot be stopped.

- To start a stopped process, select the check box next to that process name and click **Start**. The Process Status table displays the new status and other process information.
- To update the Process Status table with the latest data, click **Refresh**. The table does not automatically update.
- To see a complete report of all processes running on the WLSE, click **Complete Report**.

## Processes Displayed

The Process Status table displays the status of the following major WLSE-specific processes:

Process Name	Description
WLSEjobvm	The job virtual machine.
WLSEFaults	The fault manager.
WebServer	The Web Server.
Tomcat	The Java servlet engine.
ExcepReporter	The process that forwards traps.
CDPbrdcast	The CDP daemon that identifies Cisco devices to their immediate neighbors.
PerfMon	The process that monitors performance.

## Daemon Information

The Daemon Information dialog box displays the following:

Field	Description
Process	The process name.
Path	The file location.
Flags	The flags used to register the process with the Daemon Manager.

Field	Description
Startup	The method used to start the process.
Dependencies	The other processes that must be running for this process to run.

## System Log

The system log, which describes the status of the processes running in the system, displays the following:

Field	Description
Timestamp	The date and time the message is logged.
Process	The process that logged the message.
Type	The message type, such as INFO, WARNING, CRITICAL.
Information	The process status as known by the Daemon Manager.

## Setting Up the Splash Screen Message

The Splash Screen Message window allows you to set up a message that is displayed when a user logs in. After viewing the message, the user must click **Agree** to continue logging in, or click **Disagree** to log out.

### Procedure

- Step 1 Select **Administration > Appliance > Splash Screen**. The Splash Screen Message window appears.
- Step 2 Enter the message to be displayed.
- Step 3 Check the **Enable** check box, then click **Apply**. The splash screen message is enabled.



**Note** You *must* check **Enable** for the message to appear.

# Managing System Parameters

The System Parameters window allows you to set global parameters. For example, to set the interval at which the Wireless Clients reports will be updated, change the [Wireless Client Polling Interval](#) parameters.



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

## Procedure

- Step 1** Select **Administration > System Parameters**. The following parameters are displayed in the System Parameters window:

Parameter	Description
Inventory Polling Interval	<p>Interval at which the configuration data will be collected from the devices. (This is the data shown in any GUI device detail table.)</p> <p><b>Tip</b> For more accurate trending, set this parameter at a lower interval than <a href="#">Inventory Performance Attributes Polling Interval</a>.</p> <p>Default: 1 hour</p>
Inventory Performance Attributes Polling Interval	<p>Interval at which the performance and utilization data will be collected from the devices.</p> <p>To set the aggregation period of this data, change the <a href="#">Aggregation Interval</a> parameter.</p> <p>Default: 5 minutes</p>
Wireless Client Polling Interval	<p>Interval at which the device data is collected for client information and the Wireless Clients reports are updated.</p> <p>Default: 5 minutes</p>

Parameter	Description
Aggregation Interval	<p>Interval at which the performance data (from <a href="#">Inventory Performance Attributes Polling Interval</a>) is aggregated. (This is the data shown in Report Trends.)</p> <p><b>Note</b> For reports it is necessary to compute some attributes over longer periods (average, percentages, changes). This interval determines how often these computations are performed.</p> <p>Default: 3 hours</p>
Short Term Trending Inventory Truncation Interval	<p>Duration for which the performance data (from <a href="#">Inventory Performance Attributes Polling Interval</a>) is retained by the WLSE.</p> <p>Default: 1 day</p>
Aggregation Truncation Interval	<p>Duration for which the aggregated (historical) data is retained by the WLSE.</p> <p>Default: 15 days</p>
Fault History Truncation Interval	<p>Duration for which the fault data is retained. (This is the data shown in Fault Description.)</p> <p>Default: 30 days</p>
Job History Truncation Interval	<p>Duration for which job data is retained. (This is the data shown in Configure Jobs, Discovery History, Email Jobs.)</p> <p><b>Note</b> Recurring jobs are truncated every day to retain the last 30 runs.</p> <p>Default: 30 days</p>

- Step 2** To change any of the parameters, select new values from the pulldown lists and click **Apply** to save the changes. To reset the system parameters to the previous values, click **Reset**.



**Note** To reset the parameters to previous values, click **Reset** before saving.

A confirmation dialog appears. To return to the System Parameters window, click **Back**.

---

## Administering Users

The User Admin options allow you to manage user roles and logins:

- **Manage Roles**—Add, modify, and delete roles (see [Managing Roles, page 6-61](#)).
- **Manage Users**—Add, modify, and delete user accounts (see [Managing Users, page 6-63](#)).

### Related Topic

[Modifying Your Profile, page 6-66](#)

## Managing Roles

Use this option to add, modify, and delete user-defined roles and to modify predefined roles. A user's role determines the tabs and subtabs the user can access. Users who have access to a subtab can perform all of the tasks under the subtab.

Although you cannot delete predefined roles, you can modify them. The predefined roles and their default privileges are:

- **System administrator**—Superuser access to the Wireless LAN Solution Engine (can perform any task). The password is the password assigned during initial WLSE setup (using the console). You can change the password using the console or the WLSE's Manage Users option (see [Managing Users, page 6-63](#)).
- **Network administrator**—Monitoring authority, device configuration authority, and discovery configuration authority.
- **Network operator**—Monitoring and device configuration authority.
- **Help desk**—Monitoring authority only.

You can create other roles, which can be modified or deleted.



---

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

---

### Procedure

---

**Step 1** To access the role management window, select **Administration > User Admin > Manage Roles**. Role names are displayed in the center pane. To view the subtabs to which the role has access, select the role.

- The admin user can view all existing roles.
- Other users can only view the roles assigned to them and any roles that they have created.

**Step 2** To add a role:

- a. Replace the text *New Role* with the name you have chosen for the new role.
- b. Select the check boxes next to the features the role will access. Click **Add**.



---

**Note** When you select a feature (for example, Display Faults), the role is granted access to the corresponding subtab (for example, **Faults > Display Faults**).

---

- c. The new role appears in the list of roles in the middle pane.

**Step 3** To modify a role, select the role. Select the check boxes for the features you want to add to the role and deselect the check boxes next to the features you want to remove from the role. Then click **Modify** to save the changes.

**Step 4** To delete a user-defined role, select the role, then click **Delete**.

---

### Related Topics

- [Naming Guidelines, page A-1](#)
- [Managing Users, page 6-63](#)

# Managing Users

Use this option to:

- [Add Users, page 6-63](#)
- [Modify Users, page 6-64](#)
- [Delete Users, page 6-66](#)

## Add Users



### Note

Your login determines whether you can use this option.

### Procedure

- Step 1** Select **Administration > User Admin > Manage Users**. The Add/Modify/Delete dialog appears. The Users list displays the current users.
- The admin user can view and modify all existing users.
  - Other users can view their own logins and any users they have created.
- Step 2** Enter the following information, in the order shown:



### Note

To clear your entries and start over, click **Clear**.

Field	Information to Enter
User Name	Enter the name of the new user.
User Password	Enter a password for new user.
Confirm Password	Reenter the password.
Email	Enter the email address of the user (optional).

Field	Information to Enter
CLI Access	Select the user's access to the WLSE CLI: None, Level 0, or Level 15. By default, Level 15 is selected for System Administrator, and None is selected for other users. Users with privilege level 15 can use all commands, and users with privilege level 0 can use a subset.
Roles	Select one or more roles for the user. To add a role, select it from the pulldown list. To view a role, select it and click <b>show role</b> . To remove a role, select it and click <b>remove</b> .

- Step 3** To add the new user, click **Add**. The new username appears in the Users list. To discard your changes, click **Clear**.

## Modify Users



### Note

Your login determines whether you can use these options.

### Procedure

To modify a user:

- Step 1** Select **Administration > User Admin > Add/Modify/Delete**. The Add/Modify/Delete dialog appears. The Users list displays the current users.



### Note

Only the logins created by you are displayed. If logins were created by another user, they are not visible; only their creator can display them. The admin user can view all logins.

**Step 2** Select the user from the Users list and make the desired changes:

Field	Information to Enter
User Name	Enter the user's name.
User Password	Enter a new password for new user.
Confirm Password	Reenter the new password.
Email	Enter or change the user's email address.
CLI Access	Change the user's access to the WLSE CLI: None, Level 0, or Level 15. By default, Level 15 is selected for System Administrator, and None is selected for others. Users with privilege level 15 can use all commands, and users with privilege level 0 can use a subset. For information on commands available for each privilege level, see the <i>User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine</i> —From the online help, click <b>View PDF</b> .
Roles	Change the user's roles. To add a role, select it from the pulldown list. To view a role, select it and click <b>show role</b> . To remove a role, select it and click <b>remove</b> .

**Step 3** Click **Modify** to save your changes or **Clear** to discard your changes.

#### Related Topics

- [Naming Guidelines, page A-1](#)
- [Managing Roles, page 6-61](#)

## Delete Users



---

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

---

### Procedure

---

- Step 1** Select **Administration > User Admin > Manage Users**. The Manage Users dialog appears.
- Step 2** Select the username from the Users list, then click **Delete**. A confirmation dialog appears. After you click **OK**, the user is deleted.
- 

## Modifying Your Profile

Use the My Profile tab to change your password.



---

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

---

### Procedure

---

- Step 1** Select **Administration > My Profile > Change password**.
- Step 2** To change your password, enter a new password in the New Password and Re-enter New Password fields. For information on allowable characters, see [Naming Guidelines, page A-1](#).
- Step 3** Click **Apply** to save your changes or **Reset** to discard your changes.
- 

### Related Topic

- [Modify Users, page 6-64](#)
- [Naming Guidelines, page A-1](#)

# Using Connectivity Tools

The options in the Connectivity Tools window allow you to perform connectivity tests and find information about devices.

**Note**

---

Your login determines whether you can use this option.

---

**Procedure**

- 
- Step 1** Select **Administration > Connectivity Tools**. The Network Connectivity and Security Test dialog box appears.
- Step 2** Enter a device name or IP address in the Device text box.
- Step 3** Click an option button:

**Note**

---

Pressing **Enter** will not work. You *must* click a button.

---

- Ping—Test device reachability.
- Traceroute—Detect routing errors between the Wireless LAN Solution Engine and the target device.
- NSLookup—Look up device or host information via the name server. The information displayed includes server name, server IP address, device name, and the device IP address.
- TCP Port Scan—Find the active ports on the device.

A results window appears.

- Step 4** Click **Close** to close the results window.
-

