



Device Discovery and Management

The Devices tab provides options for basic device management on the WLSE. The options in this tab allow you to discover and manage devices and organize devices into easily manageable groups.

The topics covered in this chapter are:

- [Getting Started with Device Management, page 4-2](#)
- [How the WLSE Communicates with Devices, page 4-4](#)
- [Overview: Devices Tab Functions, page 4-5](#)
- [Entering Device Credentials, page 4-7](#)
- [Monitoring AAA Servers, page 4-21](#)
- [Managing Device Discovery, page 4-33](#)
- [Managing Devices, page 4-77](#)
- [Managing Device Inventory, page 4-89](#)
- [Using Enhanced \(WDS\) Client Tracking, page 4-27](#)
- [Exporting Devices, page 4-101](#)
- [Managing Groups, page 4-105](#)

Getting Started with Device Management

This section describes two methods for deploying devices in a wireless network:

- The Deployment Wizard for devices used in a [SWAN](#) framework—See [Using the Deployment Wizard, page 4-2](#).
- Manual configuration—See [Using Manual Methods, page 4-2](#).

Using the Deployment Wizard

For IOS access points used within a Cisco [SWAN](#) framework, you can use Wireless Domain Services ([WDS](#)) and the WLSE's Deployment Wizard for device configuration and deployment, instead of using manual deployment procedures. The Deployment Wizard is the preferred method for SWAN deployments. If you are using the Deployment Wizard, see [Chapter 2, "Using the Deployment Wizard."](#)

The Deployment Wizard handles device configuration and discover. You can also set up device groupings to make management easier, if desired. See [Managing Groups, page 4-105](#).

Using Manual Methods

If you do not use the Deployment Wizard, you can use the configuration methods methods described in the following paragraphs.

Before you can use the WLSE to manage newly added devices, the following tasks must be performed.

- Configure the devices
- Configure the WLSE
- Discover the devices
- Move the devices to the managed state
- (Optional) set up your own device groupings to make management easier.

To get started, follow the steps explained in the following paragraphs.

Step 1: Set up devices

Before devices can be discovered and managed by the WLSE, they must be properly configured. In addition, if you are using WLSE radio management, access points must be configured for Wireless Domain Service (WDS) and for LEAP authentication. You can:

- Configure devices manually. For information on setting up devices manually, see *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.12* on Cisco.com at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.
- Use auto-config. See [Automating Configurations](#), page 8-47.

Step 2: Enter device credentials

Enter device credentials on the WLSE as follows:

- Community strings for all managed devices—see [Enter or Modify SNMP Community Strings for All Devices](#), page 4-9.
- Telnet/SSH credentials for access points—see [Enter Telnet/SSH Usernames and Passwords—Access Points](#), page 4-15.
- HTTP ports for access points—see [Enter HTTP/HTTPS Port Settings—Access Points](#), page 4-18.
- WLCCP credentials—see [Enter WLCCP Credentials for Wireless Domain Services](#), page 4-20.
- Information about AAA servers that you want to monitor—see [Monitoring AAA Servers](#), page 4-21.

Step 3: Discover devices

Initiate discovery from the WLSE or import devices:

- Add seed devices and run discovery—see [Managing Device Discovery](#), page 4-33.
- Import devices—see [Importing Devices from a File](#), page 4-54 and [Importing Devices from a CiscoWorks Server](#), page 4-56.

Step 4: Verify discovery

Verify that devices were discovered—see [Viewing Discovery Logs](#), page 4-69.

Step 5: Move devices to managed state

Before you can use configuration, reporting, and monitoring features, devices must be managed by the WLSE. You must either manually move devices to the managed state on the WLSE after discovery, or specify that all discovered devices be automatically managed—see [Managing Devices, page 4-77](#).

Step 6: Run inventory

After the devices are in the managed state, an immediate inventory runs automatically to obtain device information needed to use such WLSE features as reports and automatic grouping—see [Managing Device Inventory, page 4-89](#).

You can also run inventory polling on demand for one or more devices. When new devices are discovered and managed, basic inventory and client reports are not populated until the next inventory polling occurs. However, you can use on-demand inventory to populate these reports before the next inventory cycle starts. You can also use on-demand inventory when configuration changes are made on network devices and you want the changes quickly reflected in the basic and client inventory reports.

Step 7: Create device groups

The WLSE grouping feature lets you organize managed devices into logical subsets and hierarchies. Using device grouping, you can quickly configure and upgrade a set of access points, and view reports for a set of access points as a single operation—see [Managing Groups, page 4-105](#).

Step 8: Use All WLSE Management Features

Now you can use fault monitoring, reports, firmware upgrade, and configuration, and radio management. You can also export devices, monitor AAA servers, and use Wireless Domain Services.

How the WLSE Communicates with Devices

The WLSE communicates directly with devices through SNMP and through the device CLI. For status analysis, communication takes place through most of the MIBs supported on access points. To configure IOS-based access points, the

access point CLI is used. To check device configuration, the WLSE can be configured to inventory all managed access points at user-defined intervals. For status analysis, polling intervals can be configured.

For radio management, the WLSE communicates directly with access points through Wireless Domain Service (WDS) and, for some operations, directly through SNMP. This communication takes place via Cisco's Wireless LAN Context Control Protocol (WLCCP). For this communication to occur, the access points and the WLSE authenticate with the WDS through LEAP-over-WLCCP. The frequency of radio management operations can be specified through the job scheduling interface for radio management.

From the WLSE's viewpoint, all communication is through its Ethernet interfaces. For some radio management operations, the access points communicate with each by using their radios.

Overview: Devices Tab Functions

The Devices tab covers basic device management on the WLSE. The options under this tab allow you to discover and manage devices, inventory devices, and organize devices into easily manageable groups. After devices are discovered and managed, you can use all of the other WLSE management features. For more explanation of these options, see [Getting Started with Device Management, page 4-2](#).

Managed devices can be exported to a file and to CiscoWorks Resource Manager Essentials.



Note

These subtabs may not be visible to some users; what you see under the Devices tab depends on the roles assigned to your login.

The Devices tab leads to two subtabs:

- Discover—Discovery, inventory, and device management options. The subtabs and options are briefly described in [Table 4-1 on page 4-6](#).
- Group Management—Allows you to view system groups and to create your own custom static and dynamic groups—See [Managing Groups, page 4-105](#) for information on system groups and procedures for using custom groups.

Table 4-1 **Functions of the Discover Subtab**

Subtab	Option	Reference
Managed Devices	Managed Devices—View details about a device, manage and unmanage devices, delete devices, add descriptions.	Managing Devices, page 4-77
Discover	Discovery Wizard—Run CDP discoveries or import devices.	Using the Discovery Wizard, page 4-48
	Advanced Options—Specify how devices are named, use reverse DNS lookup, auto-manage devices (with or without filtering), set discovery filtering.	Setting Advanced Discovery Options, page 4-59
	IP Filter Rules—Specify the rules for discovery filtering.	Using Discovery IP Address Filtering, page 4-67
	Logs—View discovery run logs.	Viewing Discovery Logs, page 4-69
Device Credentials	SNMP Communities	Enter or Modify SNMP Community Strings for All Devices, page 4-9
	Telnet/SSH User/Password	Enter Telnet/SSH Usernames and Passwords—Access Points, page 4-15
	IOS HTTP/HTTPS Port Settings	Enter HTTP/HTTPS Port Settings—Access Points, page 4-18
	WLCCP Credentials	Enter WLCCP Credentials for Wireless Domain Services, page 4-20

Table 4-1 **Functions of the Discover Subtab (continued)**

Subtab	Option	Reference
Inventory	Run Inventory	Running Immediate Inventories, page 4-93
	Polling—Specify polling intervals, how long to retain fault and job history data, and how long to retain aggregated data. Delete discovery and inventory logs.	Managing Polling Parameters, page 4-94
	Logs—View inventory logs.	Viewing Inventory Logs, page 4-98
Export Devices	To CiscoWorks—Export devices to CiscoWorks RME.	Exporting Devices, page 4-101
	To CSV File—Export devices to a file.	
AAA Server	Enter AAA servers to be monitored by the WLSE.	Monitoring AAA Servers, page 4-21
Client Tracking	Enable enhanced client tracking on WDS devices.	Using Enhanced (WDS) Client Tracking, page 4-27

Entering Device Credentials

The Device Credentials options allow you to enter the various credentials required for WLSE management and other features to work. These options are listed in [Table 4-2 on page 4-8](#).



Note

If you are using the WLSE Deployment Wizard to deploy IOS access points used within a Cisco [SWAN](#) framework, you can enter credentials in the Wizard instead of using the screens described in this section. For information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

The Device Credentials option lets you enter the following required device credentials:

- All managed devices must have SNMP credentials entered on the WLSE. Before the WLSE device discovery or device polling can successfully communicate with devices, the WLSE must be aware of the appropriate device SNMP credentials to use.
- For IOS-based access points, you must enter Telnet or SSH credentials and IOS HTTP port settings.
- If you are using Wireless Domain Services (WDS), you must enter RADIUS credentials and configure the WDS access point.

The Device Credentials options are:

Table 4-2 **Device Credential Options**

Option	Function	Reference
SNMP Communities	All devices—Enter community strings. Required for discovery. Note Community strings can also be entered in the Discovery Wizard and the Deployment Wizard.	Enter or Modify SNMP Community Strings for All Devices, page 4-9
Telnet/SSH User/Password	IOS APs—Enter the Telnet or SSH usernames and passwords. Note Telnet/SSH credentials can also be entered in the Deployment Wizard.	Enter Telnet/SSH Usernames and Passwords—Access Points, page 4-15
IOS HTTP Port Settings	IOS APs—Enter HTTP port numbers.	Enter HTTP/HTTPS Port Settings—Access Points, page 4-18
WLCCP Credentials	WDS—Enter RADIUS credentials for WDS.	Enter WLCCP Credentials for Wireless Domain Services, page 4-20

Enter or Modify SNMP Community Strings for All Devices

The WLSE uses **SNMP** community strings to discover devices and enable other WLSE options, such as firmware updates, configuration, and radio management. If community strings are not entered correctly, the WLSE cannot communicate with the device. Both read-only and read/write community strings are required.

The default community string covers all devices and uses *public* for both the read-only string and the read-write string. If the community strings on your devices differ from the default, you must specify the community strings on the WLSE before devices can be discovered and managed. For guidelines on configuring community strings on your devices, see the document *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine* at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

If you are importing devices from a file or CiscoWorks (instead of using the discovery mechanism), the community strings will also be imported. You do not need to enter the community strings here; however, if you import the strings and want to edit them, you can use this screen to do so. Also, if you imported devices and you want to customize the timeouts and retries, you can use this screen. For information about importing devices, see [Importing Devices from a File, page 4-54](#) and [Importing Devices from a CiscoWorks Server, page 4-56](#).

If you are using the Discovery Wizard to run CDP discovery, you can enter community strings in the wizard. For more information, see [Using the Discovery Wizard, page 4-48](#).

If you are using the Deployment Wizard to deploy access points in a WDS environment, you can enter community strings in the Wizard. For more information, see [Chapter 2, “Using the Deployment Wizard.”](#)



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Device Credentials > SNMP Communities**.



Note The SNMP Communities dialog box contains a default entry that covers all devices, provided that device community strings are set to the default (*public*). This entry is also used when none of the specified rules match a given IP address.



Note For information on guidelines for entering community strings, click **Learn more about community strings guidelines**.

Step 2 To add an entry:

- a. Enter data in the individual text boxes: IP address, Read Community, SNMP Timeout, SNMP Retries, and Write Community. [Table 4-3](#) describes the community string variables. For more guidelines, see [Recommendations For Configuring SNMP Credentials, page 4-12](#).
- b. Click **Add**.

Result: The community string appears in the list of entries.

Table 4-3 **Community String Variables**

Variable	Description	Notes
IP Address	IP address of a device or range of devices that use these community strings.	If you do not specify an IP address, the default community strings apply to all devices in the network.
Read Community	Password allowing read-only access to the devices.	You must specify the read community string. Otherwise, the default value of <i>public</i> is used.
SNMP Timeout	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 is one and the maximum is 60.

Table 4-3 Community String Variables (continued)

Variable	Description	Notes
SNMP Retries	Number of attempts the server makes 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	Password that allows write access to the devices.	You must specify the write community string. Otherwise, the default value of <i>public</i> is used.

Step 3 To modify an entry:

- a. Select the entry in the list of entries.
- b. Change the desired fields in the individual text boxes.
- c. Click **Modify**.



Note The IP Address field of an existing entry cannot be changed.

Step 4 To delete an entry:

- a. Select the entry in the list of entries. To select a number of community strings, hold down the Ctrl key while dragging the mouse down the list.
- b. Click **Delete**.



Note The default entry cannot be deleted.

Step 5 Click **Save** to apply your changes.

Related Topics

- [Community String Format, page 4-12](#)
- [Recommendations For Configuring SNMP Credentials, page 4-12](#)

Recommendations For Configuring SNMP Credentials

This section contains the following information:

- [Unsupported Characters](#), page 4-12
- [Community String Format](#), page 4-12
- [Multiple Entries and Order of Use](#), page 4-13
- [Example of Matching](#), page 4-13
- [SNMP Timeouts and Retries](#), page 4-14

Unsupported Characters

You cannot enter the <> sequence of characters in the Read Community and Write Community textboxes; for example <abc> is not allowed. The sequence >< is allowed, and the single characters < and > are allowed.

Spaces not allowed.

The following characters are not recommended for community strings: question mark (?), double-quotes (“”), dollar sign (\$), plus (+), left square bracket ([), pound sign at the beginning of the string (#), exclamation mark (!), and semi-colon (;).

Community String Format

Use these guidelines when constructing entries:

- You can assign community strings to any of the following:
 - Complete IP address; for example, 172.20.4.9
 - Wild cards based on IP addresses; for example:
*. *.*.*
172.*.*.*
 - Address ranges, which can be combined with wild cards; for example:
27.20.[4-55].*
172.[21-30].[44-88].*
172.*.*.[121-255]
- All printable characters, except for colons (:), are allowed in community strings.

- Spaces are not allowed in community strings.
- Comments are not allowed.

Multiple Entries and Order of Use

The default entry (*.*. *.*.*) is used when none of the specified rules match a given IP address. The default entry cannot be removed.

When there are multiple entries that are potential matches for an IP address:

- The WLSE will use the best (longest) matching community string. So, a fully formed IP address always takes the highest precedence.
- Matching is done from left to right on the IP address field.
- In case of conflicts caused by overlapping address specifications, the entry listed first will be used.

It is strongly recommended that you remove any ambiguity by breaking address specifications into non-overlapping sets.

The order in which you add entries does not matter.

Example of Matching

For example, assume that the user specifies community strings in the following order:

Row	Community String
1	172.20.[20-40].*
2	*.*.*.*
3	172.*.[20-40].*
4	172.20.30.44
5	172.[20-30].[20-50].*
6	172.[20-30].[30-40].*

The following device IP addresses match the user's community string specifications as follows:

- 172.20.30.40 matches row 1
- 172.20.50.40 matches row 5

- 172.50.30.40 matches row 3
- 192.168.98.98 matches row 2
- 172.20.30.44 matches row 4 (fully formed IP address)
- 172.30.40.44 matches row 6 (higher precedence than row 5)

Internally, the WLSE reorders the user specifications as follows:

```
172.20.30.44
172.20.[20-40].*
172.[20-30].[30-40].*
172.[20-30].[20-50].*
172.*.[20-40].*
*.*.*.*
```

SNMP Timeouts and Retries

Use caution in configuring the SNMP timeouts and retries because the timeout/retry mechanism uses an exponential back-off algorithm. Follow these guidelines:

- In almost all circumstances, the default timeout of 10 seconds should not be changed.
- Because SNMP is UDP-based and UDP packets can easily be lost in normal network conditions, it is usually advisable to increase the number of retries to two.

However, if you are managing devices across high latency links (for example, thin or congested WAN links) or you encounter problems with SNMP timeouts, you might need to increase the timeouts or retries. If you need to change the default timeout and retries settings, the only way to arrive at optimal settings is through experimentation. One recommended procedure is to incrementally increase the timeout settings without increasing the retries until SNMP timeouts cease:

1. Validate that the devices have the proper SNMP configuration and that the correct SNMP credentials are entered into the WLSE.
2. Increase the timeout by a small amount of time, perhaps 5 seconds.
3. Use the SNMP connectivity tool (see [Using Network Tools, page 15-65](#)) to check if SNMP requests time out. If they do, increase the timeout and test reachability again.

Continue the process until SNMP requests no longer time out. Then leave the timeout setting in place, allowing the WLSE to operate normally with these settings. If you continue to see SNMP timeouts, you might need to increase the timeout setting or increase the retries settings again.

Related Topics

[Community String Format, page 4-12](#)

Enter Telnet/SSH Usernames and Passwords—Access Points

Telnet or SSH (SSH1 only) usernames and passwords are required for applying configuration templates to access points and for upgrading firmware on access points. You can enter as many usernames and passwords as necessary on the WLSE. For more information about setting passwords on IOS access points, see *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.12* at

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

The Telnet/SSH credentials you enter in this dialog must match the login sequence on the IOS access points. If the credentials and login sequence do not match the device, the WLSE will not be able to access the device. For more information on supported login sequences, see [Supported Telnet/SSH Login Sequences for APs, page 4-17](#).

If you are using the Deployment Wizard for setting up a wireless network using WDS, you can enter these usernames and passwords in the Wizard. For more information, see [Chapter 2, “Using the Deployment Wizard.”](#)



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > Device Credentials > Telnet/SSH User/Password**.
- Step 2** Enter the credentials that match the login sequence on devices, as shown in the following table.

When adding credentials:

- Always enter the IP address information.
- Enter only the username and password information that matches the credentials requested by the access points that use the IP address or range of IP addresses.

Field	Description
IP address	IP address or range of IP addresses for access points using this username and password. For details on entering address ranges and using wildcards, see Entering IP Addresses, page 4-18 .
Username	Telnet/SSH username. Note The following characters are not supported and cannot be entered in this field: double quote, single quote, and angle brackets (< >).
User Password	Telnet/SSH password.
Confirm Password	
Enable User	Telnet/SSH enable username. Note The following characters are not supported and cannot be entered in this field: double quote, single quote, and angle brackets (< >).
Enable Password	Telnet/SSH enable password.
Confirm Enable Password	

Step 3 To add more entries, repeat Step 2.

Step 4 To modify an entry:

- Select the entry from the Current Entries text box.
- Modify fields as needed and click **Save**.

Step 5 To clear the current entry, click **Clear Fields**.

Step 6 To delete an entry, select it from the Current Entries text box and click **Delete**.

Supported Telnet/SSH Login Sequences for APs

The Telnet/SSH credentials you enter on the WLSE must match the login sequence on the access points.

For example:

- If the device prompts for a password but not a username, do not provide a username.
- If the device prompts for a username and password and logs you directly into enable mode without asking for an enable password, do not provide an enable password.
- If the device prompts for an enable password only, enter the enable password only. Do not enter a username or user password.

If the credentials and login sequence do not match the device, the WLSE will not be able to open a session on the device. Match the credentials and login sequence as shown in the following table.

Device Login Sequence	Telnet Credential Fields Required
Username: Password: prompt> enable Password: enable prompt #	User Name User Password Enable Password
Password: prompt> enable Password: enable prompt#	User Password Enable Password
Username: Password: enable prompt#	User Name User Password
enable prompt#	(no credentials required)
Username: prompt> enable Password: enable prompt#	User Name Enable Password
prompt> enable Password: enable prompt#	Enable Password

Device Login Sequence	Telnet Credential Fields Required
Username: prompt#	User Name
Username: Password: prompt> enable	User Name User Password
Username: Password: enable prompt#	Enable User Name Enable Password

Entering IP Addresses

IP addresses can consist of the following:

- A complete IP address; for example, 172.20.4.9.
- An IP address with * wildcards; for example:
 - *.*.*.*
 - 172.*.*.*
- An IP address with ranges [x - y], where x is less than y, and wildcards; for example:
 - 27.20.[4-55].*
 - 172.[21-30].[44-88].*
 - 172.*.*.[121-255]



Note

When two or more entries match the IP address of a device, the most specific entry will be used.

Enter HTTP/HTTPS Port Settings—Access Points

HTTP or HTTPS port settings are required for reports on access points; the port settings are used for the links from reports to the Web interfaces of access points. The port you should supply for each device is the port for accessing the access point's Web interface.

Access points with version 12.3 and later firmware use HTTPS.



Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Device Credentials > IOS HTTP/HTTPS Port Configuration**.

Step 2 To add a port:

- a. Enter the IP address or range of IP addresses that use this port number.

For information on using ranges and wildcards in IP addresses, click **Learn More**, or see [Entering IP Addresses, page 4-18](#).

- b. Select HTTP or HTTPS.
- c. Enter the port number.



Note The port numbers allowed for HTTPS are 443 (the default) and port numbers above 1024.

- d. Click **Save**.

Step 3 Repeat Step 2 to add more IP addresses and ports.

Enter WLCCP Credentials for Wireless Domain Services

If you are using the WLSE to monitor Wireless Domain Services (WDS) on your network, you must enter **WLCCP** credentials on the WLSE for the WDS devices or an AAA server providing LEAP authentication services.

The purpose of entering the RADIUS username and password in this screen is to allow the WLSE to authenticate with the WDS device.

The WLSE authenticates to each WDS device using the same credentials.

For more information about WDS devices, see [What is WDS and Why Do I Need It?](#), page 11-11.


Note

WLCCP credentials are required for WDS discovery. For more information about this method of discovery, see [About WLCCP/WDS Discovery](#), page 4-39.


Note

The WLSE uses UDP port 2887 for WLCCP.

To enter WLCCP credentials on the WLSE:

-
- Step 1** Select **Devices > Discover > Device Credentials > WLCCP Credentials**.
- Step 2** In the Radius Username and Radius Password fields, enter the username and password for LEAP authentication that you set for the WLSE on the WDS device or the AAA server.


Note

The following characters are not supported for the Radius Username and cannot be entered in this field: double quote (“), single quote (’), and angle brackets (< >).

Step 3 To modify the WLCCP credentials, change the fields as needed.

Step 4 To save the credentials, click **Save**.

To clear all fields and remove the WLCCP credentials, click **Clear Fields**.

Monitoring AAA Servers

The options in this screen allow you to:

- Add AAA servers—See [Adding an AAA Server, page 4-23](#).
- Remove AAA servers—See [Removing an AAA Server, page 4-25](#).
- Edit AAA server entries—See [Modifying an AAA Server, page 4-25](#).

Related Topics

- [About AAA Servers, page 4-21](#)

About AAA Servers

The WLSE can monitor AAA services provided by supported AAA (authentication, authorization, accounting) servers, Cisco Aironet 1100 or 1210 access points configured as AAA servers, and the WLSE's internal AAA server. The internal server is available on the [WLSE Express](#) only. The WLSE monitoring functionality is intended primarily to monitor AAA servers for availability and response time. Therefore, monitoring multiple protocols on the same AAA server is not supported.

For information on the external AAA servers supported by the WLSE, see the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.12* at

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

Once an AAA server's credentials are added, the WLSE can monitor the availability, authentication, and response time for the server.

The AAA services supported by the WLSE are:

- EAP-MD5
- LEAP
- PEAP (EAP-GTC only)
- RADIUS
- [EAP-FAST](#)



Note The WLSE does not monitor EAP-FAST on the internal AAA server.

Before adding AAA servers to the WLSE, configure the servers to add the WLSE as a client. For information on adding the WLSE as a client on an ACS server, see *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine*, 2.12 at

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

There are additional prerequisites for using an EAP-FAST server; see [Prerequisites for Adding an EAP-FAST Server](#), page 4-22.

After you add AAA servers to the WLSE, the WLSE automatically performs periodic logins on each server to monitor the server's response time and availability and displays this information under **Reports > Trends**.

If authentication fails, a fault will be generated and displayed by the WLSE fault monitoring system.

If an AP 1100 or AP 1210 is registered with the WLSE as an AAA server, it cannot be managed by the WLSE as an access point that also provides wireless services. An access point can either be monitored as an AAA server *or* managed as an access point that provides wireless services.

For information about changing the polling interval and response time fault thresholds for AAA server monitoring, see [Setting AAA Server Response Time](#), page 3-69.

Prerequisites for Adding an EAP-FAST Server

Before the WLSE can monitor an EAP-FAST server, the PAC (protected access credentials) must be provisioned. Use the following procedure to issue the PAC and import it to the desktop.

Procedure

-
- Step 1** On the Cisco Secure ACS server, use the **csutil** command to provision a PAC for each user. If more than one PAC is generated, ACS will generate a CAB file containing the PAC files. The PACs are exported one per file and have the naming format *username.pac*. For information on this command, see the documentation for Cisco Secure ACS server on Cisco.com.

- Step 2** FTP the .pac files to your desktop (WLSE browser client machine).
- Step 3** Configure EAP-FAST server monitoring on the WLSE by following the procedures in [Adding an AAA Server, page 4-23](#).
-

Adding an AAA Server

**Note**

For information about other requirements for AAA servers, see [About AAA Servers, page 4-21](#). In addition, for EAP-FAST servers, see [Prerequisites for Adding an EAP-FAST Server, page 4-22](#).

If you add an AP as an AAA server, it can no longer be managed by the WLSE as an access point providing wireless services.

You can monitor only one protocol on a given AAA server. For example, if you have added an AAA server and specified the PEAP protocol, you cannot add the same server a second time and specify the RADIUS protocol. When you try to add the server the second time, an error message is displayed.

There is no limitation on the number of AAA servers you can add.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > AAA Server**.
- Step 2** Enter the following data.

Table 4-4 AAA Server Parameters

Field	Description
Show List	Select the protocol type from the pulldown list: ¹ <ul style="list-style-type: none"> • EAP-MD5 • LEAP • PEAP (EAP-GTC only) • RADIUS • EAP-FAST
Server Name	Hostname or IP address of the AAA server. In WLSE displays, the server is identified by this name.
Server Port	Port on the server that is used for authentication; this should always be 1645.
Username	Client username that you entered on the AAA server.
Password	Client password that you entered on the AAA server.
Secret	Shared secret key that you entered on the AAA server.
PAC File Password (EAP-FAST only)	Password for decrypting the .pac file and the filename of the .pac file to be uploaded from the desktop.
PAC Filename (EAP-FAST only)	Note If you have not created a .pac file for this EAP-FAST server, see Prerequisites for Adding an EAP-FAST Server, page 4-22 .

1. The WLSE monitors only one protocol for a given AAA server.

- Step 3** Click **Save**. To discard your entries, click **Cancel**.
- Step 4** Edit the default faults profile to enable polling for the AAA protocol you selected. See [Managing Fault Settings, page 3-14](#) for procedures.
- Step 5** If authentication fails, a fault will be generated.
For EAP-FAST, check the user credentials and make sure that the valid PAC file has been imported. If the PAC has expired or is invalid, re-import the PAC file from the desktop.
- Step 6** After a few polling cycles, you can view the trend data for the server response time in the Server Response Time Graph.
- a. Select **Reports > Trends**.

- b. Choose the protocol type from the **Device Type > AAA Servers > protocol** folder.

**Note**

For EAP-FAST, choose EAP.

- c. Select the server's IP address.
-

Removing an AAA Server

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > AAA Server**.
 - Step 2** Select the server type from Show List
Result: All servers of that type are displayed.
 - Step 3** Select the server to be removed.
 - Step 4** Click **Remove**.
-

Modifying an AAA Server

The WLSE monitors only one protocol for a given AAA server.

**Note**

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > AAA Server**.

Step 2 Select the server type from Show List.

Result: All servers of that type are displayed.

Step 3 Select the server to be modified.

Step 4 You can modify only the following characteristics of an existing AAA server entry.

Modifying the hostname or IP address of an existing AAA server entry requires removing the existing server and adding it back with the new IP address or hostname.

Characteristic to Modify	Description
Server Port	Port on the server that is used for authentication; this should always be 1645.
Username	Client username that you entered on the server.
Password	Client password that you entered on the server.
Secret	Shared secret key that you entered on the server.
PAC File Password (EAP-FAST only)	Password for decrypting the .pac file and the filename of the .pac file to be uploaded from the desktop.
PAC Filename (EAP-FAST only)	

Step 5 Click **Save**.

Step 6 To discard your entries, click **Cancel**.

Related Topics

- [Removing an AAA Server, page 4-25](#)
- [Adding an AAA Server, page 4-23](#)

Using Enhanced (WDS) Client Tracking

The WLSE can track clients of access points by querying Wireless Domain Service (WDS) for all client associations. You can use the following procedure to enable or disable this type of client tracking globally or enable it on selected WDS devices (access points or WLSM). By default, client tracking is globally disabled.

In addition to enabling client tracking, you must configure access points and the WLSE. See [Prerequisites for Enhanced Client Tracking, page 4-29](#) for more information.

For more information on client tracking and client polling, see [About WDS Client Tracking, page 4-29](#).

For information on the IOS firmware versions that support enhanced client tracking, see the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.12at*

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

Configuring Enhanced Client Tracking

**Note**

Your login determines whether you can use this option.

Procedure

-
- Step 1** Select **Devices > Discover > Client Tracking**. The client tracking options are displayed.
- Step 2** Select an option:
- **Enable client tracking on all WDS devices**—client tracking will be enabled on all WDS access points.
 - **Disable client tracking on all WDS devices**—this is the default state.
 - **Enable client tracking only on selected WDS devices:**
 - A list of the configured and managed WDS devices appears. The information in the list is described in [Table 4-5](#).

- Select the WDS devices on which you want to enable client tracking.

Table 4-5 Client Tracking Devices

Field	Description
Name	Name and IP address of an active WDS device that is being managed by the WLSE.
IP Address	Note Although only active WDS devices are listed, the configuration settings of an active WDS will be applied automatically to the backup WDS when the backup becomes active.
Subnet	Subnet to which the WDS is assigned.
Version	Firmware image on the WDS device.
Backup Count	Number of WDS devices (in the same subnet) that are acting as backup for this active WDS device.
Registered Node Count	Number of access points registered with this WDS device.
WNM Authentication State	Status of the authentication of the WLSE with the WDS device.
WDS Tracking Status	Current state of client tracking for the WDS device: <ul style="list-style-type: none"> • Enabled—the WLSE is receiving client tracking events from this WDS device. • Disabled—the WLSE is not receiving client tracking events from this WDS device.

Step 3 To reset to the previous setting, click **Reset**. To save your changes, click **Apply**.

Related Topics

- [About WDS Client Tracking, page 4-29](#)
- [About Inventories, page 4-90](#)
- [Displaying Wireless Client Reports, page 10-31](#)

About WDS Client Tracking

This section contains information about the following:

- [Prerequisites for Enhanced Client Tracking, page 4-29](#)
- [Client Tracking vs. Client Polling, page 4-30](#)
- [Wireless Client Reports, page 4-32](#)
- [Display of RADIUS Username in Wireless Client Reports, page 4-32](#)

Prerequisites for Enhanced Client Tracking

In addition to enabling client tracking on the WLSE, you must configure the following for WDS-based client tracking to work.



Note

You can also use the WLSE's Deployment Wizard for configuring access points and the WLSE for WDS.

- Configure the WLSE for WLCCP—See [Enter WLCCP Credentials for Wireless Domain Services, page 4-20](#).
WLCCP messages are required for the WDS to perform client tracking.
- Configure primary and (optional) backup [WDS devices](#)—See *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.12* at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

This feature is not available on all IOS firmware versions. All WDS access points must be upgraded to IOS firmware version 12.2(15)JA or later. For the latest information, see the WLSE 2.11 Supported Device Table at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

If the WDS devices have firmware earlier than 12.2(15)JA, enhanced client tracking is not available. However, client tracking via client polling is available. For more information, see [Client Polling, page 4-30](#).

- Configure [infrastructure access points](#) for WDS—See *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.12* at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

These access points need not necessarily be upgraded.

- (Strongly recommended) Configure Network Time Protocol (NTP) on the network.

Client tracking event reports include a WDS timestamp, which is used to display the order of events at the WDS. If all clocks are not NTP synchronized, events from different WDS devices may not be ordered correctly. You should ensure clock synchronization by configuring NTP service on the WDS and the WLSE. The NTP server should be a network NTP server that is used by all WDS devices. For information on enabling NTP on the WLSE, see [Setting Time, Time Servers, Name Servers, and Web Session Timeout, page 15-59](#). For information on enabling NTP on WDS devices, see the device documentation.

Client Tracking vs. Client Polling

The WLSE obtains client data in two ways:

- Automatic client inventory polling—see [Client Polling, page 4-30](#).
- WDS client tracking—see [Client Tracking, page 4-31](#).

Client Polling

The WLSE automatically collects client data by polling all access points, using a configurable polling interval. Data obtained from client polling is detailed and includes traffic statistics. Polling data is only as timely as the last client polling cycle, which means that the client polling interval greatly affects the accuracy of client reports:

- In environments where clients are highly mobile, such as health care and retail deployments, you should set the client polling interval to the minimum if the network can tolerate the polling traffic.
- In enterprise deployments, most WLAN users have laptops and tend to be stationary for long periods of time, so client polling should be less frequent.

Wireless client polling is a fairly heavyweight process. If you have many access points to poll for client associations, polling should be less frequent. As a result, the client data will not be as accurate. Wireless client reports are updated every 51 minutes by default. To reset the client polling interval, see [Changing the Polling Intervals for Automatic Inventories](#), page 4-91.

**Note**

You can also obtain detailed client information by running on-demand or scheduled inventories on one or more specific access points. See [Running Immediate Inventories](#), page 4-93.

Client Tracking

With client tracking, the WLSE obtains client data from WDS devices, instead of from all of the individual infrastructure access points. Client tracking provides only historical information.

Any clients that have associated with a managed access point are reported and tracked either by a corresponding managed, active WDS device which is serving the same subnet as the managed access point or a WLSM (Wireless LAN Services Module). WLSM-WDS devices can manage multiple access point subnets.

WDS devices send notifications to the WLSE when certain events occur about any client associated with access points that are registered with that WDS. Each WDS maintains an updated active cache of all clients that are associated with each registered access point within the WDS domain. These events are recorded by the WLSE and can be viewed from the Client Historical Association Report and Client Access Failure Report. These events also keep the current client association information up to date. For performance reasons, there is approximately a 2-minute delay between when the event occurs and when the event is available in reports. The reported events are:

- Refresh—Occurs when the WLSE synchronizes with the WDS. This happens when the WLSE reboots and when the WDS-to-WLSE management link is established or restored. During this phase, the WLSE learns about all of the registered clients within a specific WDS domain.
- Registration with WDS—When a client successfully registers with the WDS for the very first time.
- Detachment from WDS—When the WDS cleans up the internal cache of a stale client or the associated access point indicates to the WDS that a client has become inactive.

- Roam—When a client roams to another access point within the same WDS domain.
- Access failure—When a client fails to access an access point during EAP authentication.

Even when client tracking is enabled, the wireless client polling described in [Client Polling, page 4-30](#) is still required to obtain other information about client activity, such as client as client traffic statistics.

If you have a high volume of client roaming or client activity, enabling client tracking will add extra overhead and WLSE performance may be affected. However, client tracking events are optimized to consume very little network traffic and WLSE processing resources.

Although client polling occurs automatically, client tracking must be enabled on [WDS devices](#) by selecting **Devices > Discover > Client Tracking**. To enable client tracking and view the current state of client tracking, see [Using Enhanced \(WDS\) Client Tracking, page 4-27](#).

Wireless Client Reports

Wireless client reports provide information about the type of client that is associating with an access point, how much bandwidth the client is using, which access points the client has associated with, and the kind of client activity.

For information on displaying wireless client reports, see [Displaying Wireless Client Reports, page 10-31](#).

Display of RADIUS Username in Wireless Client Reports

The client RADIUS username is not available for:

- Non-EAP authentication.
- PEAP and EAP-TLS authentication if certain RADIUS servers are used. [Table 4-6 on page 4-33](#) lists username support for various authentication types and AAA servers.

Table 4-6 RADIUS Username in Client Tracking Reports

Authentication Type	RADIUS Server	RADIUS Username Supported?	Configuration Required on RADIUS Server?
non-EAP	Not applicable	No	Not applicable
EAP EAP-MD5 EAP-TLS EAP-SIM	Any server that supports the authentication type	Yes	No
Cisco PEAP Microsoft PEAP EAP-FAST	Cisco ACS server	Yes	No
Cisco PEAP Microsoft PEAP EAP-FAST	Other RADIUS servers that support Cisco PEAP	Unknown	Unknown
EAP-TTLS	Any RADIUS server that supports EAP-TTLS	Unknown	Unknown

Managing Device Discovery



Note

If you are using the WLSE Deployment Wizard to deploy access points used within a Cisco [SWAN](#) framework, you can use the Wizard to discover these devices instead of using the discovery methods described in this section. For information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

By default, the WLSE runs Cisco Discovery Protocol (CDP) discovery every 24 hours. After devices are discovered, they must be put under management—see [Managing Devices, page 4-77](#). Unmanaged devices do not appear in WLSE displays.

The functions under the Discover subtab are described in [Table 4-7 on page 4-34](#). To learn more about discovery, see [About Discovery, page 4-34](#).

Table 4-7 **Discovery Options**

Option'	Description	Reference
Discovery Wizard	Run additional CDP discoveries and modify the default schedule.	Running CDP Discovery, page 4-50
	Discover devices by importing them from a file or from a CiscoWorks server.	Importing Devices from a File, page 4-54 Importing Devices from a CiscoWorks Server, page 4-56
Advanced Options	Set advanced options that modify the behavior of discovery and device management and allow you to specify how devices are identified in displays.	Setting Advanced Discovery Options, page 4-59
IP Filter Rules	Set up IP address filtering for discovery	Using Discovery IP Address Filtering, page 4-67
Logs	View discovery job details	Viewing Discovery Logs, page 4-69

About Discovery

The topics covered in this section are:

- [Understanding Discovery and Management, page 4-35](#)
- [Understanding WLSE Discovery Methods, page 4-36](#)
- [About CDP-Based Discovery, page 4-38](#)
- [About WLCCP/WDS Discovery, page 4-39](#)
- [About Individual Device Seeding, page 4-40](#)
- [About Device Import From a File, page 4-41](#)
- [About Device Import From CiscoWorks, page 4-45](#)
- [About CSV Files, page 4-43](#)

Understanding Discovery and Management

Network devices are interrogated by the WLSE by using discovery and inventory polling.

Device discovery is a periodic process that finds new devices and, possibly, topology and network changes. The discovery process can be run at scheduled intervals or on demand.

The WLSE can discover Cisco wireless access points and bridges, and Cisco switches or routers that have Cisco wireless devices directly connected to them.

Discovered devices are either managed and unmanaged. By default, newly-discovered devices are in the unmanaged state and will not be polled until you manually move them to the managed state.

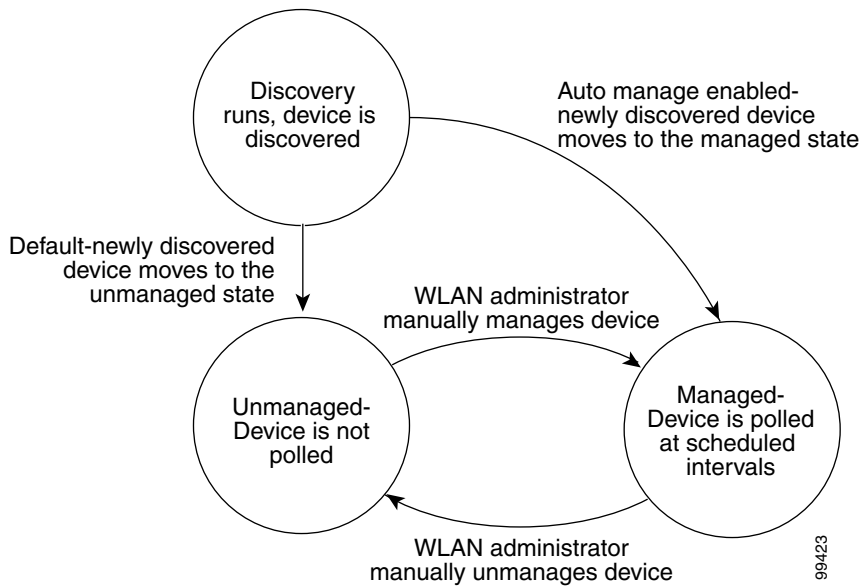
You can enable an auto-manage feature that automatically moves newly discovered devices to the managed state when they are discovered. You can also apply a default device configuration to auto-managed wireless devices. [Figure 4-1](#) illustrates the managed/unmanaged state machine.

Assuming the discovery process is successful, the WLSE discovery footprint is approximately 2500 bytes per device per discovery cycle. *This is just the discovery footprint.* The 2500 bytes represent a single SNMP get-request and a single SNMP get-response. This footprint may be larger if the SNMP get-response needs to be broken up across multiple protocol data units (PDU), which often happens if the device receiving the SNMP get-request has a large CDP neighbor table.

After a device is discovered for the first time and the device is auto-managed, an immediate inventory will run. However, inventory is not run automatically when discovery is run on a device that was already discovered (even if the device is automanaged). You can run an immediate inventory to update device information on the WLSE or wait for the next regular scheduled inventory.

You can view information about discovery jobs in the discovery logs (see [Viewing Discovery Logs, page 4-69](#)) and in the jobvm log. To view or download the jobvm log, select **Admin > Appliance > Status > View Log File** and select the jobvm.log file.

Figure 4-1 Device Management State Machine



Understanding WLSE Discovery Methods

Before the WLSE can manage devices, it must discover them. There are several discovery techniques:

- CDP-based discovery—See [About CDP-Based Discovery, page 4-38](#).
- WLCCP/WDS discovery—See [About WLCCP/WDS Discovery, page 4-39](#).
- Individual device seeding—See [About Individual Device Seeding, page 4-40](#).
- Device import from a file—See [About Device Import From a File, page 4-41](#).
- Device import from CiscoWorks Resource Manager Essentials (RME)—See [About Device Import From CiscoWorks, page 4-45](#).

Use the following table to help you decide which technique to use:



Note AAA servers must be entered individually regardless of discovery method. See [About AAA Servers, page 4-21](#).

Table 4-8 *Discovery Options*

Discovery Method	Use This Method When...
CDP-based discovery	Use this method when wireless devices are attached to Cisco switches or routers running Cisco discovery protocol. For more information, see About CDP-Based Discovery, page 4-38 .
Individual device seeding	<p>If the wireless devices are connected to switches or routers that don't run CDP (for example, non-Cisco switches), this is one option.</p> <p>Note You must enter an IP address for each managed device.</p> <p>For more information, see About Individual Device Seeding, page 4-40.</p>
Device import from a file	<p>If the wireless devices are connected to switches or routers that don't run CDP (for example, non-Cisco switches), this is an option. This technique adds an entry for each device for SNMP credentials.</p> <p>Note Using this method, you might need to create a large CSV file listing each device.</p> <p>For more information, see About Device Import From a File, page 4-41.</p>
Device import from CiscoWorks Resource Manager Essentials (RME)	<p>Use this technique if you have already inventoried the wireless devices using RME. This technique adds an entry for each device for SNMP credentials.</p> <p>For more information, see About Device Import From CiscoWorks, page 4-45.</p>

About CDP-Based Discovery

When the WLSE runs a CDP-based discovery, it begins by using SNMP to retrieve the list of devices in the CDP neighbor table of each seed device. It then retrieves the devices in the CDP neighbor tables from each of the CDP neighbors of the seeds. This process continues until all devices in the network are discovered for the CDP distance is reached.



Note Only Cisco wireless devices and Cisco switches or routers attached to properly configured access points are recognized by the discovery process.

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 can 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 Supported access points, bridges, routers, and switches are all valid seed devices. PCs and workstations are not valid seed devices.

Interesting devices from the perspective of the WLSE are:

- Cisco wireless bridges and access points
- Cisco routers or switches that are CDP neighbors of a Cisco wireless device.

Because the WLSE keeps only interesting devices, try to select seed devices in a way that minimizes unnecessary WLSE discovery traffic on the network by selecting devices so that the discovery process will only touch interesting devices. This is usually not possible, but by selecting seeds wisely, a minimum number of uninteresting devices will be touched by the discovery process.

CDP-based discovery can be run on-demand, at a scheduled time, or at recurring intervals. Typically, you only need to run discovery when you initially deploy the WLSE and when you deploy new wireless devices.

By default, CDP discovery is enabled and runs every 24 hours. The discovery wizard allows you to run additional immediate CDP discoveries and change the default CDP schedule. See [Using the Discovery Wizard](#), page 4-48.

Devices must be properly configured for access by the WLSE before they can be discovered and managed. See *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.12* at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

If CDP is disabled, you can still discover devices by entering their IP addresses as seed values in the discovery dialogs or by importing them. However, the connectivity between access points and switches will not be discovered and switch-related reports will be empty. For more information, see [About Individual Device Seeding](#), page 4-40.

About WLCCP/WDS Discovery



Note

You can also use the Deployment Wizard to deploy access points in a WDS environment. See [Chapter 2, “Using the Deployment Wizard.”](#)

If you use WDS, all of the IOS access points in a subnet register with the WDS, and WDS sends this data to the WLSE via [WLCCP](#). The WLSE checks whether these devices are in the WLSE database. If not, a regular CDP discovery is run, using each device as a seed. So, new devices that register with the WDS will be automatically discovered.

WLCCP-based discovery is the only way to discover a Wireless LAN Services Module (WLSM). CDP-based discovery is not supported for this device.

These WDS discoveries do not appear in the discovery log. WDS discoveries are affected by any discovery filters that you have set. See [Setting Advanced Discovery Options](#), page 4-59 and [Using Discovery IP Address Filtering](#), page 4-67.

For WLCCP discovery to work:

- WDS devices and infrastructure APs must be configured for network management and radio management—See *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.12* at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

**Note**

If the WDS device is configured with the WLSE's address, the WLSE will auto discover the device without waiting for the next scheduled discovery job to run.

- The WDS devices must be in the managed state.

About Alternatives to CDP

Instead of enabling CDP and using it for discovery, you can use the following methods of discovering devices:

- [About Individual Device Seeding, page 4-40](#)
- [About Device Import From a File, page 4-41](#)
- [About Device Import From CiscoWorks, page 4-45](#)

About Individual Device Seeding

Although CDP-based discovery is usually the preferred option, in some network environments a CDP-based discovery is undesirable or impossible. For example, the wired network infrastructure may have non-Cisco switches or hubs that do not support CDP, or IT security policies may prohibit the use of CDP in the network.

As an alternative to using Cisco Discovery Protocol (CDP) to run discovery, you can seed each device IP into the WLSE. The WLSE setup process is similar to the regular CDP-based discovery, and is treated as such by the WLSE discovery process. Rather than using a few, well-chosen seed devices:

1. Enter each device to be managed as a seed device prior to running discovery.
2. Set the [CDP distance](#) to 1.
3. Use either the on-demand discovery option or the scheduled discovery option from **Devices > Discover > DISCOVER**.

**Note**

This technique will not discover switches or routers attached to wireless devices unless the wireless devices and switches and/or routers are CDP-enabled. Because the WLSE cannot establish a neighbor relationship between switches or routers and the wireless devices if the switches or routers are not CDP-enabled, they will not be included as manageable by the WLSE.

**Note**

Because this technique requires that you enter each device as a seed, it may add significant overhead to the WLSE discovery setup time.

About Device Import From a File

When a CDP-based discovery is undesirable or impossible, importing a list of devices from a file is another option in many environments. For example, the wired network infrastructure may have non-Cisco switches or hubs that do not support CDP or IT security policies may prohibit the use of CDP in the network.

Using an import file in comma separated variable (CSV) format is an alternative to individual device seeding. Because the import file may be obtained from another network inventory management application, this technique may be more practical than individual device seeding.

Use the option **Devices > Discover > DISCOVER > Import From File** to import devices from a CSV file. You can choose to discover some devices and import others, however devices not supported by the WLSE are ignored during device import.

A one-time discovery job starts immediately after you import devices from a CSV file. This means the following discovery options affect device import:

- Advanced Options—See [Setting Advanced Discovery Options, page 4-59](#).
- IP Filter Rules—See [Using Discovery IP Address Filtering, page 4-67](#).

When you import the devices from a CSV file, the WLSE:

1. Treats each entry as a seed device and uses a [CDP distance](#) of 1.
2. Attempts to retrieve the CDP neighbor table of each entry, discarding any devices in the CSV file that are not interesting. Interesting devices from the perspective of the WLSE are:
 - Cisco wireless bridges and access points

- Cisco routers or switches that are CDP neighbors of a Cisco wireless device.

If CDP is not enabled on the wireless devices or if there are no CDP neighbors, then the WLSE will only discover the wireless devices and the WLSE cannot be used to manage the neighboring switch or router.



Note Because the WLSE will attempt to determine the device type and CDP neighbors of each device imported from the CSV file, a large number of uninteresting (to the WLSE) devices may add significant time to the discovery process and add unnecessary traffic to the network. To minimize discovery time, you should edit the CSV file to contain only devices of interest.

3. Adds a row in the SNMP device credentials fields (see [Enter SNMP Communities, page 4-52](#)) for each device during the import process. The WLSE will do this even if there are already entries that qualify for the devices configured.

You can choose to delete the specific entries and leave only the general entries. This is not a required step because the WLSE will choose the most specific entry when looking up SNMP credentials for a device, but it is recommended because it will make managing device credentials easier.

4. Imports the following information:
 - IP addresses are accepted as is, and hostnames are resolved to obtain the IP address. Hostnames that cannot be resolved are ignored.
 - Read-only and read/write community strings are inserted into the SNMP Communities table (**Devices > Discover > Device Credentials**).

The community strings that you import will overwrite the information already entered on the WLSE. You can view the information already entered in **Devices > Discover > Device Credentials > SNMP Communities**. Community strings that contain wildcards will not be overwritten unless these entries are exactly matched by entries in the CSV file.

- SNMP timeout and retry settings are not imported but you can specify values, while setting up the discovery job.

The timeouts and retries that you enter will overwrite information already entered on the WLSE.

During the subsequent discovery:

- All WLSE-supported devices in the file are used as seed devices with a [CDP distance](#) of 1. These devices are listed in the Discovery Run Log.
- In the discovery logs (see [Viewing Discovery Logs, page 4-69](#)), the name of the import from file is shown as CDPDiscovery_Import_Devices.

About CSV Files

The file used for imports is an ASCII [CSV](#) (comma-separated values) file with a .txt filename suffix. You can create a CSV file by exporting devices from CiscoWorks or by creating the file with a text editor. You can view a sample CSV file from the Discovery Wizard screens for file import, or see the following example.

A CSV file can contain the following device information:



Note

Only the device name or IP address and the community strings are used by the WLSE.

- Full device name or IP address (required). Include the domain in the device name unless your site has unqualified device names registered in the name service.
- Read-only community string (required).
- Read-write community string (optional).
- Serial number (optional).
- User Fields 1, 2, 3, and 4 (optional).
- Telnet password, enable password, enable secret, TACACS user, TACACS password, TACACS enable user, TACACS enable password, local user, local password, and RCP (remote copy protocol) user.
- RCP password (not used).

An example file follows.

```
;
; The possible columns in the CSV file are listed below.
;
; For importing to WLSE, columns 1,2,3 are required and the
; rest are optional.
;
```

Managing Device Discovery

```

; Col# = 1: Name = Device name (include domain unless your site
;           has unqualified device names registered in
;           the name services)
;           - or -
;           IP Address in dotted decimal notation
;
; Col# = 2: Name = RO community string
; Col# = 3: Name = RW community string
; Col# = 4: Name = Serial Number
; Col# = 5: Name = User Field 1
; Col# = 6: Name = User Field 2
; Col# = 7: Name = User Field 3
; Col# = 8: Name = User Field 4
; Col# = 9; Name = Telnet password
; Col# = 10; Name = Enable password
; Col# = 11; Name = Enable secret
; Col# = 12; Name = Tacacs user
; Col# = 13; Name = Tacacs password
; Col# = 14; Name = Tacacs enable user
; Col# = 15; Name = Tacacs enable password
; Col# = 16; Name = Local user
; Col# = 17; Name = Local password
; Col# = 18; Name = Rcp user
; Col# = 19; Name = Rcp password; Comment = Not used, leave blank
;
; Here are examples of rows of data:
;
1.2.3.4,public,public,,
1.2.2.5,public,public,,,,,telnetpwd
bigrouter.yourcompany.com,public,private,,,,,telnetpwd
dev-2501.yourcompany.com,"Not so, " " public as, thought",private,sn2501,
dev-2502.yourcompany.com,public,"private",sn2502,
dev-2503.yourcompany.com,public,private,sn2503,"
dev-2510.yourcompany.com,public,private,sn2510,
dev-4000.yourcompany.com,public,private,,Big Boys
dev-2517.yourcompany.com,public,private,,nm 25xx
dev-2520.yourcompany.com,public,private,,mylabel2
dev-4700.yourcompany.com,public,private,,yourlabel1,,yourlabel3,yourlabel4
dev-7206.yourcompany.com,public,private,,
dev-7505.yourcompany.com,public,private,,,,,yourlabel4

```

About Device Import From CiscoWorks

If you are using CiscoWorks Resource Manager Essentials (RME) to manage your wireless devices, you can import the devices from RME to the WLSE without configuring, scheduling, or running WLSE discovery. This process is analogous to using a CSV file to import a list of devices. Use the option **Devices > Discover > DISCOVER > Discovery Wizard > Import From CiscoWorks** to import devices from RME.

Immediately after a successful import, the WLSE runs discovery on all of the imported devices. Therefore, the following discovery options affect device import:

- Advanced Options—See [Setting Advanced Discovery Options, page 4-59](#).
- IP Filter Rules—See [Using Discovery IP Address Filtering, page 4-67](#).

You can specify an immediate import, schedule an import for a future time, or schedule recurring imports. The time required to import devices depends on the response from the CiscoWorks server and the number of devices imported. You can check the status of the operation while it is running.

When you import the devices from CiscoWorks, the WLSE:

1. Interrogates the RME server for its device list and credentials, and then treats each device retrieved from RME as a seed device.
2. Attempts to determine the CDP neighbors of each device, discarding devices from RME that are not interesting. Interesting devices from the perspective of the WLSE are:
 - Cisco wireless bridges and access points
 - Cisco routers or switches that are CDP neighbors of a Cisco wireless device.



Note Because the WLSE will attempt to determine the device type and CDP neighbors of each device imported from RME, a large number of uninteresting (to the WLSE) devices may add significant time to the discovery process and add unnecessary traffic to the network.

If CDP is not enabled on the wireless devices or if there are no CDP neighbors, the WLSE will only discover the wireless devices.

3. Adds a row in the SNMP device credentials fields for each device during the import from RME process. This process may result in duplicate entries for SNMP credentials.

You can choose to delete the specific entries and leave the general entries. This is not a required step because the WLSE will choose the most specific entry when looking up SNMP credentials for a device, but it is recommended because it will make managing device credentials easier.



Note Only the device's hostname or IP address and the read and write community strings are imported from a CiscoWorks server. The SNMP timeout and retry settings are not imported (the WLSE default settings are used).

4. During the subsequent discovery, two items are listed in the discovery log for each import from CiscoWorks:
 - Cisco Works Device Import—Click this item to display a run log that shows the information imported for each device found on the CiscoWorks server. The WLSE uses only the hostname or IP address and the community strings.
 - CDPDiscovery_Import_Devices—Click this item to display a run log that shows the results of the discovery that was run by using the information imported from the CiscoWorks server.

The WLSE provides scheduled, automated inventory imports from RME. Many customers prefer keeping a master Cisco device inventory on the RME server. Using the scheduled, automated inventory import allows customers to keep their WLSE device list in sync with the master list.

Most networks have a fairly static inventory. That is, new devices are typically added in planned roll-outs. So there really is no need to have the recurring RME import interval set very frequently. In most cases, once a week is more than frequent enough.

Using the WLSE Discovery Methods

Discovery of devices is a prerequisite to managing and monitoring them. You can discover devices by:

- Enabling CDP on the devices and running a discovery—See [Running CDP Discovery, page 4-50](#).
- Entering all the devices as seeds in the discovery wizard—See [Running CDP Discovery, page 4-50](#).
- Importing devices from a file—See [Importing Devices from a File, page 4-54](#).
- Importing devices from CiscoWorks RME—See [Importing Devices from a CiscoWorks Server, page 4-56](#).

Pre-Discovery Checklist

The following checklist will help you confirm that the prerequisites for successful discovery have been met.

This list is only the requirements for successful device discovery. To use other WLSE features, other configuration requirements exist.

For details on setting up devices for discovery and for other configuration requirements, see *Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.12* at

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.

For information on using the Wizard for setting up devices, see [Chapter 2, “Using the Deployment Wizard.”](#)

Prerequisites for discovery:

- CDP enabled on network devices (for CDP-based discovery).
- SNMP communities configured on network devices.
 - Read-only SNMP community strings configured on switches and routers.
 - Read-only SNMP community strings configured for IOS-based wireless access points.
- SNMP community strings entered into WLSE device credentials fields.

- WLSE configured as network access server (NAS) for CiscoSecure Access Control Server (ACS) (for AAA server monitoring) or equivalent in other AAA servers.

Related Topics

[Managing Device Discovery, page 4-33](#)

About the Discovery Wizard

From **Devices > Discover > DISCOVER > Discovery Wizard**, you can use all of the discovery methods. To start using the wizard, see [Using the Discovery Wizard, page 4-48](#). The discovery methods are:

- [Running CDP Discovery, page 4-50](#)
- [Importing Devices from a File, page 4-54](#)
- [Importing Devices from a CiscoWorks Server, page 4-56](#).

Using the Discovery Wizard

The discovery wizard provides the following choices for discovering devices.

**Note**

Your login determines whether you can use this option.

Procedure**Note**

Before devices can be discovered, they must be properly configured. For more information, see [Pre-Discovery Checklist, page 4-47](#).

Step 1 Select **Devices > Discover > Discover > Discovery Wizard**.

Step 2 Select the type of discovery you want to run:

Option	Description	Reference
Automatic Device Discovery based on Cisco Discovery Protocol	Run immediate or scheduled discovery by using Cisco Discovery Protocol (CDP).	About Discovery, page 4-34
Import from File	Import devices from a file.	
Import from CiscoWorks	Import devices from a CiscoWorks server (using Resource Manager Essentials), on an immediate or scheduled basis.	

Step 3 (Optional) To use discovery advanced options, click **Advanced Options**.

You can use advanced options to:

- Customize the device name format.
- Use reverse DNS lookup.
- Auto manage the discovered devices and use automanagement filtering for access points. For more information on these options, see [Setting Advanced Discovery Options, page 4-59](#).

Step 4 (Optional) To set up discovery filtering by IP address, click **IP Filter Rules**.

Filtering by IP address limits the range of discovery. For more information, see [Using Discovery IP Address Filtering, page 4-67](#).

Step 5 Click **Next**.



Note

In the following screens, you can click **Back** to modify a previous screen or **Cancel** to cancel the discovery or import.

Running CDP Discovery

This section provides procedures for using the Discovery Wizard screens for CDP discovery. To get started, select **Devices > Discover > DISCOVER > Discovery Wizard > Automatic Device Discovery based on Cisco Discovery Protocol**.


Note

Your login determines whether you can use this option.

The tasks for running CDP discovery are described in [Table 4-9 on page 4-50](#).

Table 4-9 **Tasks for CDP Discovery**

Type Discovery	Task	Reference
Run Now	Select Run Now.	Select the Type of CDP Discovery, page 4-51
	Specify SNMP communities.	Enter SNMP Communities, page 4-52
	Specify initiating IP addresses (seeds).	Enter Initiating IP Addresses (Seeds), page 4-52
	Verify your settings and finish.	Verify Your Settings and Finish—Run Now, page 4-53
	View discovery run details.	
Modify Schedule	Select Modify Schedule	Select the Type of CDP Discovery, page 4-51
	Modify the schedule	Specify the Schedule, page 4-51
	Specify SNMP communities	Enter SNMP Communities, page 4-52
	Specify initiating IP addresses (seeds)	Enter Initiating IP Addresses (Seeds), page 4-52
	Verify your settings and finish	Verify Your Settings and Finish—Modify Schedule, page 4-54
	View discovery run details	

Select the Type of CDP Discovery

The Select Type of CDP Discovery screen provides choices for running CDP Discovery.

**Note**

By default, discovery runs once every 24 hours.

Procedure

- Step 1** Choose an option:
- To run a one-time discovery now, select **Run Now**.
 - To modify the default discovery schedule, select **Modify Periodic**.
- Step 2** Click **Next** to continue.
-

Related Topics

[About CDP-Based Discovery, page 4-38](#)

Specify the Schedule

In this screen, you can modify the discovery schedule.

Procedure

- Step 1** Select the Start Date and Start Time from the pulldown lists.
- Do not schedule a discovery to begin within 5 minutes of the current time. Otherwise, the first discovery might not run. Use the **Run Now** option instead.*
- Step 2** To repeat discovery at specified intervals, click **Enable**. Then enter a number in the Every text box and select the interval from the list.
- Step 3** Click **Next**.
-

Enter SNMP Communities

The community strings for all devices to be discovered by using CDP must be entered on the WLSE.

Procedure

Step 1 If you have not yet entered community strings for the devices in this discovery job or you need to change the community strings, you can do it now.

Step 2 There are two methods for entering community strings:

- Enter community strings directly in the large text box.
- Use the individual text boxes and click **Add** after entering the data for each string.



Note The large text box lists all SNMP credentials that have been entered on the WLSE.

Step 3 For guidelines on community string syntax, click **Learn more about community string guidelines**.

Step 4 Click **Next**.

Related Topics

[Recommendations For Configuring SNMP Credentials, page 4-12](#)

Enter Initiating IP Addresses (Seeds)

You must enter at least one initiating IP address (seed device).

Procedure

Step 1 Add seed devices by entering their comma-separated IP addresses in the Add Values text box and click >>.



Note Seed devices entered during **Run Now** are not retained after the discovery. Seed devices added during **Modify Schedule** are retained and you can use them for subsequent discoveries.

Step 2 Set the **CDP distance** by selecting a number from the list.

Set this value appropriately to discover the entire wireless network or the set of devices you are discovering. A CDP distance of 1 only discovers the immediate neighbors of the seed devices.

Routers and switches that do not have access points attached to them are used when computing CDP distance. However, these routers and switches will not be discovered.

Step 3 Click **Next**.

Related Topics

[About CDP-Based Discovery, page 4-38](#)

Verify Your Settings and Finish—Run Now

Procedure

Step 1 Enter a job name, if desired. For guidelines on naming jobs, see [Appendix B, “Naming Guidelines.”](#)



Note Job names must be unique. Do not use the same job name for discovery jobs and other jobs (such as firmware or configuration jobs).

Step 2 Verify that your settings are correct.

Step 3 If settings are not correct, click **Back** to make changes.

Step 4 When settings are correct, click **Finish**.

Discovery will begin immediately and the Discovery Run Details screen will appear, showing the details of the discovery job.

For more information about Discovery Run Details, see [Viewing Discovery Logs](#), page 4-69.

Related Topics

[Viewing Discovery Logs](#), page 4-69

Verify Your Settings and Finish—Modify Schedule

Procedure

- Step 1** Verify that your settings are correct.
- Step 2** If not, click **Back** to make changes.
- Step 3** When settings are correct, click **Finish**.
- Discovery will begin at the Start Time you selected.



Note If a warning message appears saying that WLSE server is ahead of or behind your local time, see [Understanding Time Discrepancy Problems in Job Scheduling](#), page 1-16.

Related Topics

[Viewing Discovery Logs](#), page 4-69

Importing Devices from a File

This section gives procedures for using the Discovery Wizard screens for importing devices from a file.

To get started, select **Devices > Discover > DISCOVER > Discovery Wizard > Import From File**.



Note Your login determines whether you can use this option.

The tasks for importing devices from a file are:

Table 4-10 *Tasks for Import from File*

Task	Reference
Specify the file and set the SNMP retry and timeout (optional)	Select the File and Set SNMP Parameters, page 4-55
Verify your settings and finish	Finish the Import, page 4-56
View import details	

Select the File and Set SNMP Parameters

To import devices from a file, you can create the file by using a text editor or by exporting devices from a CiscoWorks server that is running Resource Manager Essentials.

For information about CSV files, see [About CSV Files, page 4-43](#).

Procedure

-
- Step 1** To see a sample CSV device file, click **See Sample CSV File**.
- Step 2** Enter a pathname for the file in the Select File dialog box or click **Browse** to find the file on the desktop or another network system.
- Step 3** The read and write community strings for the imported devices will be imported and will overwrite existing community strings. Existing entries that use wildcards will not be overwritten unless they are exactly matched by entries in the CSV file.
- To see or edit the existing community strings on the WLSE, select **Devices > Discover > Credentials > SNMP Communities**.
- Step 4** The timeout and retry settings in a CSV file are not imported. If you do not specify timeout and retries, the default settings (10 seconds and 1 retry) will be assigned to the imported devices. The timeouts and retries you enter here will overwrite any timeouts and retries already entered for existing community strings. To specify the timeout and retries for the imported devices:

- Enter the number of seconds in the SNMP Timeouts text box.
 - Enter the number of retries in the SNMP Retries text box.
- Step 5** To view the status of the last import, if any, click **Check Last Status**. Details on the latest import are shown.
- Step 6** To import devices from the file you selected, click **Next**. The file will be imported and a one-time discovery will begin immediately.
-

Finish the Import

Procedure

- Step 1** This screen shows the devices that will be imported.
- Step 2** To view the status of this import, click **Check Last Status**.
- Step 3** Click **Finish**. The Import from File Status screen will appear, showing the job details.
-

Related Topics

[Viewing Discovery Logs, page 4-69](#)

Importing Devices from a CiscoWorks Server

This section provides procedures for using the Discovery Wizard screens for importing devices from CiscoWorks server that is running Resource Manager Essentials.

To get started, select **Devices > Discover > DISCOVER > Discovery Wizard > Import from CiscoWorks**.



Note

Your login determines whether you can use this option.

The tasks for importing devices from CiscoWorks are:

Table 4-11 Tasks for Import from CiscoWorks

Task	Description
Specify the CiscoWorks server	Schedule the Import and Finish, page 4-57
Schedule the import	
View import details	

Schedule the Import and Finish

This screen allows you specify a CiscoWorks server as the source of the devices to be imported. You can run a one-time import or schedule imports.

Procedure

- Step 1** Enter the following information. All fields are required; if any fields are left blank, the display will clear when you try to save your settings.

Field	Description
Host	CiscoWorks server IP address. Note The following characters are unsupported and cannot be entered in this field: double quote, single quote, and angle brackets (< >).
Port	Port number on which the CiscoWorks server listens for HTTP requests. You may need to contact the administrator of the CiscoWorks server to obtain this information.
User	Username and password of any user who has the authority to export and import device credentials on the CiscoWorks server.
Password	
Confirm Password	

- Step 2** To run a one-time import:
- a. Select **Run Now**.
 - b. Click **Finish**. The import will begin immediately.
- Step 3** To schedule a one-time import or repeated imports:
- a. Select the start date from the Start Date pulldown lists.
 - b. Enter the start time from the Start Time pulldown lists.
 - c. To schedule repeated imports, click **Enable Repeat** and set the interval by entering a number after Every and selecting Minutes, Hours, Days, Weeks, or Months from the pulldown list.
 - d. Click **Finish**. A one-time import will begin immediately.



Note If a warning message appears saying that WLSE server is ahead of or behind your local time, see [Understanding Time Discrepancy Problems in Job Scheduling, page 1-16](#).

- Step 4** To view the status of the last import from CiscoWorks, click **Check Last Status**. Details on the latest import are shown. Click **Refresh** to update the display. You might see the error messages listed in [Table 4-12 on page 4-58](#).

Table 4-12 Device Import Status Messages

Message	Meaning
Error: Could not connect to CiscoWorks server: <i>ip_address</i> on port: <i>port_number</i> .	Either the host or the port specified in the WLSE import dialog was wrong.
Error: Connected to CiscoWorks server: <i>ip_address</i> on port: <i>port_number</i> successfully, but server returned error after connection.	Either the user or password specified in the WLSE import dialog was wrong.

Related Topics

- [Viewing Discovery Logs, page 4-69](#)

- [About Device Import From CiscoWorks, page 4-45](#)

Setting Advanced Discovery Options

This option provides the following customizations for discovery and device management:

- Select the name format for the device identifier in WLSE displays—See [Selecting the Device Name Format, page 4-59](#).
- Enable or disable reverse DNS lookup—See [Enabling Reverse DNS Lookup, page 4-63](#).
- Specify automatic management of newly discovered devices—See [Enable Auto-Management, page 4-64](#).
- Specify filtering for time-limited access point management—See [Enable MAC Address Auto-Manage Filtering for Access Points, page 4-65](#).

**Note**

Your login determines whether you can use these options.

Selecting the Device Name Format

The Name Format option lets you define the format of the device name shown in WLSE displays. You can choose from the following formats and you can specify a combination of more than one format:

- DNS name
- Hostname
- IP address
- Description of your choice

If you chose this option, you must enter a description for each device in the Device Details screen under **Devices > Discover > Managed Devices**.

- Ethernet MAC address (APs only)
- Radio interface MAC address (APs only)

Your choice of name format affects the display of all devices, except for AAA servers. For AAA servers, the device name displayed is always the name you specify when adding the AAA server as a device to be monitored by the WLSE.

The name format(s) that you choose are used to make up a device identifier string. This string is computed for each device and shown in all WLSE displays.

The fact that long names will be truncated in some WLSE displays may influence your choice of device identifier string. For example, in device trees, only 30 characters are shown. If you choose the hostname plus IP address as the string and you are using the fully qualified domain name as the hostname, it may be difficult to distinguish between different devices in the tree if the hostname is the first part of the string. As a workaround, you could construct the string so that the IP address is first.

You can search for devices by specifying the device description.

Procedure

To change the device identifier used for managed devices:

-
- Step 1** Select **Devices > Discover > DISCOVER > Advanced Options**.
 - Step 2** To view information about the name formats, click **Learn About Name Format**.
 - Step 3** To specify the device identifier format, compose a string from the list of variables in [Table 4-13 on page 4-61](#), and enter the string in the Name Format field. For examples and rules, see [Examples and Rules for the Name Format Option, page 4-62](#).
 - Step 4** Click **Save** to save all of your settings in the Advanced Options screen.

Result: All device names (except for AAA servers) in WLSE displays will be changed to the new format.



Note If a device is in the unmanaged state and you move it to the managed state, the device name does not immediately change to the currently specified name format. The change occurs after the next inventory is run. To change to the correct name format immediately, you can run an immediate inventory on that device. For more information, see [Running Immediate Inventories, page 4-93](#).

Table 4-13 Name Formats

Name Format String ¹	Result	
%dns%	<p>The device DNS name is displayed,</p> <p>Whether the DNS name is displayed, or a different identifier is displayed, depends on several factors. For details, see Enabling Reverse DNS Lookup, page 4-63.</p> <p>If there is no DNS name, the device name is displayed as %dns%.</p>	
(%ip%)	<p>The device IP address is displayed.</p> <p>Using this string guarantees that the device name display will always be correct.</p>	
%hostname%	<p>The device hostname is displayed. This is the default.</p> <p>If the device has no hostname assigned to it, the device name is displayed as %hostname%.</p>	
%description%	<p>A description of your choice is displayed.</p> <p>You must enter a description for each device in the device detail screen accessible from Devices > Managed Devices.</p> <p>Note If you select %description% as the name format and do not enter a description for a device, the device name is displayed as %description%.</p> <p>Note The following characters are unsupported and cannot be used in a device description: double quote, single quote, and angle brackets (< >).</p>	
%r0MAC%	The MAC address of the radio interface is displayed.	<p>The MAC address formats apply only to access points and bridges, and are not applicable to switches and routers.</p> <p>Only the last 6 characters of the MAC address are used in the device identifier.</p> <p>If you use one of these name formats for devices other than access points, the DNS name, sysName, or IP address will be used instead. Which identifier is used depends upon whether reverse DNS lookup is enabled and the sysName is set on the device; for more information, see Enabling Reverse DNS Lookup, page 4-63.</p>
%e0MAC%	The MAC address of the Ethernet 0 interface is displayed.	

1. Does not affect the display the identifiers of AAA servers.

Related Topics

- [Examples and Rules for the Name Format Option, page 4-62](#)
- [Enabling Reverse DNS Lookup, page 4-63](#)
- [Entering Device Descriptions, page 4-83](#)

Examples and Rules for the Name Format Option

The name format can be any of the types listed when you select **Learn About Name Format** or any combination of these types, for example:

- (%ip)%dns%
- %hostname%
- %dns%%r0MAC%
- %e0MAC%(%ip%)
- %e0MAC%%description%
- (%ip)%e0MAC%%description%
- (%ip)%dns%%description%%r0MAC%%e0MAC%%r1MAC%

If the computed device identifier is longer than 30 characters, the WLSE will display only the first 30 characters in the device tree.

For name formats that include %e0MAC%, %r0MAC%, or %r1MAC%, only the last 6 characters of the MAC address will be used.

Name formats that include %e0MAC%, %r0MAC%, or %r1MAC% are not applicable to switches and routers.

Name formats do not apply to AAA servers; AAA servers are displayed according to the name entered when the server was added to the WLSE.

Enabling Reverse DNS Lookup

Enabling reverse DNS lookup affects hostname display on the WLSE as shown in [Table 4-14 on page 4-63](#). The actual identifier displayed for a device is also affected by the choices you make when specifying a device name format in **Devices > Discover > DISCOVER > Advanced Options** (for more information, see [Selecting the Device Name Format, page 4-59](#)).

Table 4-14 *Effects of Reverse DNS Lookup on Device Name Display*

Reverse DNS lookup enabled?	Effect on Display
Yes	If the lookup succeeds, the device name is displayed.
	If the lookup fails, the device IP address is displayed.
No	If the device's SNMP sysName is set, the sysName is displayed. ¹
	If the sysName is not set, the device IP address is displayed.

1. If a device's sysName contains a single quote (') and DNS is not enabled, the IP address will be displayed instead of the sysName.



Note

The hostname (device name) is not updated during every inventory cycle. This information is updated only after the device is rediscovered.

Procedure

-
- Step 1** Select **Devices > Discover > DISCOVER > Advanced Options**.
 - Step 2** If DNS is configured on devices, you can enable reverse DNS lookup by selecting **Use reverse DNS lookup**.
 - Step 3** Click **Save** to save all of your settings in the Advanced Options screen.
-

Related Topics

[Selecting the Device Name Format, page 4-59](#)

Enable Auto-Management

Enabling this option causes all discovered devices to be automatically managed.

**Note**

The Deployment Wizard enables auto-management. For more information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

Procedure

To enable automatic management for all discovered devices:

Step 1 Select **Devices > Discover > DISCOVER > Advanced Options**.

Step 2 Select **Auto-Manage Devices without Filtering**.

All discovered devices will be automatically placed in the Managed folder.

**Note**

If you are using the automatic device configuration feature, make sure you enable auto-management. Access points and bridges that you add to the network will be automatically configured only if Auto-Manage is enabled. For more information, see [Automating Configurations, page 8-47](#).

Step 3 To use the option for auto-managing selected access points within specified time limits, see [Enable MAC Address Auto-Manage Filtering for Access Points, page 4-65](#).

Step 4 Click **Save** to save all of your settings in the Advanced Options screen.

Related Topics

- [Managing Devices, page 4-77](#)

Enable MAC Address Auto-Manage Filtering for Access Points

This option allows you to specify access points that you want to auto-manage during a specified time interval.

Filtering also affects devices discovered through Wireless Domain Service (WDS). For more information, see [About WLCCP/WDS Discovery, page 4-39](#).

Auto-management affects all discovered devices. Access point filtering affects only access points. See the following table for details on the effects of these two options.



Note

The auto-manage filtering settings that you make here affect the Timer option in the Deployment Wizard and will be reflected in the Deploy Config screen of the Wizard. For more information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

Table 4-15 Access Point Filtering Outcomes

Auto-Manage selected?	MAC Filtering selected?	Result
No	No	All discovered devices must be manually moved to the managed state.
Yes	No	All discovered devices are automatically moved to the managed state.
Yes	Yes	Only access points listed in Access Points to Auto-Manage will be auto-managed and they will be auto-managed only during the specified interval. Note If the interval expires, newly discovered APs will not be auto-managed. However, any APs that you have manually placed in the Managed folder will still be managed.

You can specify the access points to be auto-managed by entering Ethernet MAC addresses in the screen or importing a file containing Ethernet MAC addresses. For example files, see [Example MAC Address Files, page 4-67](#).

To enable MAC address filtering:

-
- Step 1** Select **Devices > Discover > DISCOVER > Advanced Options**.
- Step 2** Select **Auto-Manage Devices without Filtering**.
- Step 3** Select **Enable Filtering for Auto-Manage devices**.
- Step 4** In the **Filters Valid From** and **To** fields, specify the time period for auto-management.



Note When the time period expires, you must deselect **Enable Filtering**. Otherwise, no newly discovered access points will be auto-managed.

- Step 5** To enter Ethernet MAC addresses in the screen:
- Remove the default * entry before beginning. Otherwise, all access points will be auto-managed regardless of the MAC addresses you enter.
 - Enter an Ethernet MAC address in the **Enter MAC Address of access point** text box (in hexadecimal format) and click >>. For example, 000b46fd0286. You can use the asterisk (*) as a wildcard; for example, *b46fd0286.
 - Repeat Step b to add more addresses.
- Step 6** To import a list of Ethernet MAC addresses from a file:
- Create an ASCII file (.txt file) consisting of one address per line or a comma-separated list. For sample files, see [Example MAC Address Files, page 4-67](#).
 - Enter the path to the file in the **Import From File** text box or click **Browse** to find the file.
 - Click **Import**.
- Step 7** To remove an address, select it in the **Valid MAC Addresses** text box and click <<.
- Step 8** Click **Save** to save all of your changes in the Advanced Options screen.
-

Example MAC Address Files

You can use either of the following file formats to import MAC addresses for limited discovery of access points:

- One address per line. For example:

```
0040965b611f
000a41047e3b
0040965b5f75
004096588420
004096543a84
000bbe6d8bd4
000af4fb658a
```

- Comma-separated list. For example:

```
000b466e482,0000bbe8190c2,0040965b611f,000a41047e3b,0040965b5f75,
004096588420,004096543a84,000bbe6d8bd4
```

Using Discovery IP Address Filtering

You can limit discovery to selected devices by setting up filter rules to include or exclude devices. Filter rules consist of device IP addresses with optional wildcards and ranges.

IP address filtering also affects devices discovered through Wireless Domain Service (WDS). For more information, see [About WLCCP/WDS Discovery, page 4-39](#).



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > DISCOVER > IP Filter Rules**. For details on creating rules, click **Learn more about IP filter rules**.
- Step 2** Add IP addresses to the Include Rules or Exclude Rules text boxes, one entry per line. Use standard IP address format (four octets separated by periods) in which any octet can be:

- A value between 0 and 255.
- An asterisk (*) wildcard, denoting any number from 0 to 255; for example, 10.20.*.*.
- A range in which the first number is less than the second; for example, 10.20.30[50-60].

Rules cause discovery to be limited as described in [Table 4-16](#).



Note Exclude rules take precedence over include rules.

Table 4-16 *Effects of Include and Exclude Rules in Discovery Filters*

Include Rules Defined?	Exclude Rules Defined?	Result
No	No	All devices are discovered.
No	Yes	All devices are discovered, but devices that match the Exclude Rules are discarded.
Yes	No	Only devices that match the Include Rules are discovered.
Yes	Yes	Only devices that match the Include Rules are discovered. Devices that match the Exclude Rules are discarded.

For example, assume the IP addresses of the devices in a network are from 10.10.10.1 through 10.10.10.200:

- The include rule is 10.10.10.[40-80]
- The exclude rule is 10.10.10.[60-70]

All of the devices with the IP addresses 10.10.10.[40-80] are discovered, but those with IP addresses 10.10.10.[60-70] are discarded. Therefore, the devices discovered and retained have IP addresses 10.10.10.[40-59] and 10.10.10.[71-80].

Step 3 Click **Save**. Your rules will take effect for all subsequent discoveries.

Related Topics

[Understanding WLSE Discovery Methods, page 4-36](#)

Viewing Discovery Logs

This option displays detailed logs on the results of discoveries and imports.

To delete all discovery logs, see [Deleting Inventory and Discovery Logs, page 4-93](#).

**Note**

WDS discoveries are not logged.

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > DISCOVER > Logs**.

A table of discovery jobs is displayed.

Step 2 The names of the jobs indicate the type of discovery that was run, as explained in the following table:

Table 4-17 *Discovery Job Log*

Field	Description
Name	Type of discovery that was run: <ul style="list-style-type: none"> • Periodic CDP Discovery—scheduled discovery • Run Now CDP Discovery—on-demand discovery • CDPDiscovery_Import_Devices—device import from a file or CiscoWorks server • CiscoWorks Device Import—device import from a CiscoWorks server¹
Start Time	When the discovery started.
Recurring	<ul style="list-style-type: none"> • Yes—scheduled job that repeats at regular intervals. • No—on-demand or scheduled for one time only.

Table 4-17 **Discovery Job Log (continued)**

Field	Description
State	Scheduled—Discovery will occur in the future. Not scheduled—Run Now discoveries
User	User name—Name of the user who ran the job or who was the last user to modify the job. WLSE—Automatic, scheduled discovery that has not been modified by a user.
End Time	When the discovery ended.

- Two items are listed in the discovery log for each import from a CiscoWorks server: CDPDiscovery_Import_Devices and CiscoWorks Device Import.

Step 3 To view details about a job, select the job and click **Discovery Run Detail**. The Discovery Run Detail window shows the start and end times of the job run, whether it succeeded, and other details. For scheduled discoveries, there will be several runs listed.

- To view the next page, click the arrow.
- To view the next 8 rows or all rows, click **8** or **All**.
- To close the window click **Close**.
- To refresh the display click **Refresh**.

For more information on data shown in the Discovery Run Detail window, see [Discovery Run Details Display, page 4-71](#).

If the log files show that problems occurred while running discovery, see [Diagnosing Common Discovery Problems, page 4-74](#).

Step 4 To filter the list of jobs, select All, Running, or Scheduled from the Discovery Job State list.

Step 5 To refresh the display, click **Refresh**.

Related Topics

[Deleting Inventory and Discovery Logs, page 4-93](#)

Discovery Run Details Display

A typical, healthy discovery run produces a log file similar to the following:

```
Seed value entered: 10.2.8.3
Hop count defined: 1
CDP Discovery started at 2003-03-27 22:40:11.437 (UTC)
New device discovered:10.2.8.3 ( AP1200-CHAR-NET )
Number of devices (re)discovered: 1
CDP Discovery completed at 2003-03-27 22:40:11.737 (UTC)
```

The log in the Discovery Run Details window shows the following information:

- Start and end times.
- The hop count (CDP distance) that was specified.
When you import devices, each imported device is listed as a “Seed value entered” in the log, and the “Hop count defined” value is 1.
- The seed devices that were entered or imported.
- Devices that were previously discovered and are being updated.
- Devices that were discovered for the first time.
- Devices that are being auto-managed. An immediate inventory collection will run automatically on auto-managed devices.
- Number of devices discovered or rediscovered.



Note An immediate inventory does not run automatically after a device is rediscovered. You can run an immediate, on-demand inventory or wait for the next regularly scheduled inventory. For more information, see [Managing Device Inventory, page 4-89](#).

The messages listed in [Table 4-18 on page 4-72](#) may appear in the Discovery Run Details display.

Table 4-18 Messages—Discovery Run Log

Message	Meaning
172.19.12.39,public,private,14,1.3.6.1.4.1.9.1.507, !{[NOVALUE]}!,...	Messages similar to this are informational and show data obtained during device import from CiscoWorks.
CDP Discovery completed	Periodic CDP discovery end time.
Number of devices (re)discovered <i>number</i>	Number of devices discovered or rediscovered.
No seeds defined.	Although discovery is initially enabled and runs every 24 hours, it will not run unless you add seed devices. See Using the Discovery Wizard, page 4-48 .
<i>ip_address</i> Device updated (<i>sysname</i>)	Device was previously discovered and information is being updated.
Inventory collection was not run for updated devices, run on-demand inventory or wait for the next scheduled inventory	An automatic inventory does not run for rediscovered devices. Run an on-demand inventory or wait for the next scheduled inventory. This is an informational message.
<i>ip_address</i> New device discovered (<i>sysname</i>)	Device was discovered for the first time.
<i>ip_address</i> Device being auto-managed (<i>sysname</i>)	Auto-management is enabled.
Inventory collection will run immediately for auto-managed devices.	Auto-management is enabled; therefore, inventory collection will run immediately for the auto-managed devices.
<i>ip_address</i> is SNMP unreachable, unable to read CDP cache.	<p>The community strings may be set up incorrectly. See <i>Configuring Devices for Management by the CiscoWorks Wireless LAN Solution Engine, 2.12</i> at http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwparent/cw_1105/wlse/2_12/index.htm.</p> <p>This message might indicate a network problem, or the device might be an invalid seed device (not running CDP and SNMP), such as a PC or workstation.</p> <p>For more information on troubleshooting SNMP problems, see Diagnosing Common Discovery Problems, page 4-74.</p>

Table 4-18 Messages—Discovery Run Log (continued)

Message	Meaning
No logs available. Waiting for resources to start job.	Other running jobs are using all available resources. Information on this job will be displayed when resources are available.
x.x.x.x is reachable but unable to provide the information you requested. For IOS access points, make sure the SNMP community does not have an object identifier associated with it.	<p>The community string associated with the device might not have an SNMP ISO view associated with it, and the WLSE cannot poll some attributes. Configure the community string in the AP as follows:</p> <pre># snmp-server view iso iso included # snmp-server community community_string view iso RO</pre> <p>where <i>community_string</i> is the AP's read-only community string.</p>
IP conflict for <i>ip_address</i> (<i>hostname</i>). Identifier or ethernet MAC is <i>identifier</i> or <i>MAC address</i> . A device already exists under this IP address. If the original device was replaced, please delete it first and run discovery again.	<p>A newly discovered device has the same IP address as a previously discovered device. The new device will not be discovered until the conflict is resolved. The identifier shown is for the previously discovered device. For access points, the identifier shown is the Ethernet MAC address.</p> <p>If you want both devices to be managed, assign a different IP address to the newly discovered device. If you substituted a new device for a previous device and want to retain the IP address, delete the old device. In either case, run discovery again or wait for the next scheduled discovery. See Managing Device Discovery, page 4-33.</p>
Unable to auto-manage device: x.x.x.x due to MAC filter values or time period for auto-management has expired.	A new device is being discovered but could not be auto-managed because the MAC filter values exclude the device or the time period selected for auto-management has expired. See Enable MAC Address Auto-Manage Filtering for Access Points, page 4-65 .

Related Topics

- [Running CDP Discovery, page 4-50](#)
- [Diagnosing Common Discovery Problems, page 4-74](#)

Diagnosing Common Discovery Problems

This section contains information on:

- [Troubleshooting SNMP Connectivity Problems, page 4-74](#)
- [Obtaining Detailed Discovery Logs, page 4-76](#)

**Note**

For more troubleshooting information and FAQs, see the *Troubleshooting Guide for the CiscoWorks Wireless LAN Solution Engine, 2.12*. For help locating this document, see [Finding WLSE Documentation on Cisco.com, page 1-21](#).

Troubleshooting SNMP Connectivity Problems

The most common discovery problems are related to SNMP connectivity. This type of message indicates that the WLSE attempted to retrieve the CDP neighbor table of the device, but was unable to do so because of an SNMP connectivity issue:

```
172.20.98.230 is SNMP unreachable, unable to read CDP cache.
```

Typical causes of SNMP connectivity issues are:

- No IP connectivity to the device
- SNMP community misconfigurations and/or mismatch
- SNMP agent is not running on devices
- SNMP timeouts, retries need to be adjusted

To determine the cause of the problem:

1. Confirm IP connectivity from the WLSE to the unreachable devices with the Ping Connectivity Tool (see [Using Network Tools, page 15-65](#)). Note that the WLSE Ping Connectivity Tool will attempt reverse name resolution on the IP address. If your network does not support reverse name resolution for the devices, you typically see 80% ICMP packet loss using the Ping Connectivity Tool unless you enter the `-n` flag in the Device field. If your network does not support reverse name resolution for your devices, enter `-n dvc_IP_address` in the Device field before clicking on the Ping button.



Note Cisco's Technical Assistance Center (TAC) has published a number of useful hints and documents on network troubleshooting. Visit the Cisco.com TAC web-site for more information.

2. After IP connectivity has been confirmed, use the SNMP Connectivity Tool (see [Using Network Tools, page 15-65](#)) to verify SNMP connectivity to the devices in question. This tool retrieves a single object—the SNMP sysObjectID of the device.

One common problem with both IP and SNMP connectivity is the presence of access control lists (ACLs) or firewalls in the network between the WLSE and the managed devices that might reject management traffic. Verify that management traffic is permitted from the WLSE to each of the managed devices.

3. If SNMP connectivity *can* be confirmed using the SNMP Connectivity Tool and devices cannot be discovered (the log lists the devices as SNMP unreachable), you might need to adjust the SNMP timeout and retries. See [Recommendations For Configuring SNMP Credentials, page 4-12](#).

The SNMP Connectivity Tool retrieves a single object, whereas the discovery retrieves multiple objects. You can use the SNMP Query Tool (see [Using the SNMP Query Tool, page 15-66](#)) to retrieve a larger SNMP table. Then, if you have SNMP connectivity for one variable but not for the larger table, it is likely that the issue is related to the timeout and retry settings. See Step 5.

4. If SNMP connectivity *cannot* be confirmed using the SNMP Connectivity Tool, verify that:
 - The SNMP agent is running on the devices.
 - The SNMP communities are correctly configured on the devices.
 - The SNMP credentials are correctly configured on the WLSE.

If the SNMP configuration is not correct, reconfigure the devices and WLSE as necessary and re-run the discovery.

5. If the SNMP configuration is correct and IP connectivity has been confirmed, you may need to adjust the SNMP timeout and retries (see **Devices > Discover > Device Credentials**). Increase the timeouts and retries in small increments, re-running discovery after each adjustment, until the devices are no longer SNMP unreachable.

Obtaining Detailed Discovery Logs

If the procedures in the preceding section do not solve your discovery problems, open a case with the Cisco TAC. You might be able to assist the Cisco TAC by getting more detailed discovery logs. To increase the level of logging:



Note You must be logged in with admin privileges to use this interface.

1. Navigate to the WLSE interface at http://wlse_ip:1741/debug/logging.jsp.
2. Select **Debug**.
3. Click **Save**.
4. Run the discovery again to get more logging details.

After the discovery runs:

1. Navigate back to WLSE interface at http://wlse_ip:1741/debug/logging.jsp.
2. Select **Default**.
3. Click **Save**.



Note Except for troubleshooting purposes, do not run any logging level other than Default for any task. Running at a level higher than Default might impact the performance of the WLSE.

Managing Devices

**Note**

If you are using the WLSE Deployment Wizard to deploy access points used within a Cisco [SWAN](#) framework, all discovered devices will be automatically managed. For information on the Deployment Wizard, see [Chapter 2, “Using the Deployment Wizard.”](#)

The Managed Devices option under **Devices > Discover > Managed Devices** shows the management state of all discovered devices. Devices must be in the managed state before they can be polled, and before you can use the WLSE to monitor or configure them or use any of the other WLSE network management or radio management features.

By default, newly discovered devices are in the unmanaged state. You can arrange for devices to be automatically managed after they are discovered, or you can manually move devices to the managed state.

From the device tree you can also view details on any device in a folder.

**Note**

The device tree shows the state of the system at the time you select the Managed Devices option. Therefore, if device details change or the device changes to another state after you display the page, these changes not automatically displayed. If you refresh the page from the browser or navigate to another page and then return to Managed Devices, the page will be updated to show changes.

This section contains information on the following device management options:

- The folders under **Devices > Discover > Managed Devices** and how to use the available functions—See [Device Management Folders and Functions, page 4-78](#).
- The number of devices that a WLSE can manage—See [Limitation on the Number of Managed Devices, page 4-86](#).
- What to do when the same IP address is assigned to more than one access point or you replace a managed access point—See [Handling Duplicate IP Addresses on Access Points, page 4-88](#).

Device Management Folders and Functions

The Managed Devices option provides the following functions:

Table 4-19

Function	Reference
View all devices that have been discovered: newly discovered devices that are not yet managed, managed devices, unmanaged devices (devices that were once managed but are no longer managed), and devices with changed IP addresses. Note Only managed devices appear in other WLSE displays, such as groups and reports.	About Managed Devices Folders, page 4-78
Manually change a device's management state. ¹	Manually Changing the State of Devices, page 4-80
View details about a device.	Viewing Device Details, page 4-81
Enter a different description for each device.	Entering Device Descriptions, page 4-83
Delete devices.	Deleting Devices, page 4-85

1. You can also configure the WLSE to automatically manage devices as they are discovered. See [Setting Advanced Discovery Options, page 4-59](#).



Note

The roles assigned to your login determine whether you can use the Managed Devices option.

About Managed Devices Folders

The Managed Devices display contains the following top-level folders. There is a subfolder for each type of device contained in a top-level folder; the subfolders appear only if there is at least one device of that type in the top-level folder.

Table 4-20 *Managed Devices Folders*

Top-Level Folder	Contents	Permitted Actions
Search Results	This folder is populated after you run a successful search for devices. This folder does not contain subfolders. For information on searching for devices, see Using the Device Selector, page 1-17 .	If a device is in any of these folders, you can view details about it, delete it from the database, or change its managed/unmanaged state.
New	Contains all devices that have been discovered but are not in the managed state.	
Managed	Contains all devices that are in the managed state	
Unmanaged	Contains all devices that were once managed but are not longer in the managed state.	
Duplicate IP	<p>Contains access points that are in the <i>pending</i> state. A device becomes pending and is placed in this folder:</p> <ul style="list-style-type: none"> • When the same IP address is assigned to more than one access point. • When an access point's IP address changes. • When you replace a managed access point. <p>The IP address shown for a device in this folder is the last known address for the device, before the address change occurred.</p> <p>For information on how to move devices from the pending state, see Handling Duplicate IP Addresses on Access Points, page 4-88.</p>	If a device is in this folder you can view details about it or delete it from the database.

Manually Changing the State of Devices

Procedure

- Step 1** Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The Discovered Devices tree is displayed.
- For information on the folders and subfolders in the tree, see [About Managed Devices Folders, page 4-78](#).
- Step 2** Select a folder. The Group Change Status window appears and all devices in the folder are displayed.
- Select the devices you want to change, then click **Manage** or **Unmanage**. Devices will be moved into the Managed or Unmanaged folder.



Note After you move devices to the managed state, an immediate inventory is run for those devices. This ensures that device attributes appear in displays immediately, without waiting for the next scheduled inventory.

- Step 3** You can also change the status of a single device from its Device Detail display:
- Expand the folder and select the device.
Result: The Device Detail pane is displayed. For more information on device details, see [Viewing Device Details, page 4-81](#).
 - Click **Manage** or **Unmanage** at the bottom of the pane.
 - The device will be moved into the Managed or Unmanaged folder.



Note After you move a device to the managed state, an immediate inventory is run for that device. This ensures that device attributes appear in displays immediately, without waiting for the next scheduled inventory.

Related Topics

- [Viewing Device Details, page 4-81](#)
- [Entering Device Descriptions, page 4-83](#)

- [Deleting Devices, page 4-85](#)
- [Limitation on the Number of Managed Devices, page 4-86](#)
- [Managing Device Inventory, page 4-89](#)

Viewing Device Details

Procedure

- Step 1** Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The Discovered Devices tree is displayed.
- For information on the folders and subfolders in the tree, see [About Managed Devices Folders, page 4-78](#).
- Step 2** To view details about an individual device:
- Expand the folder and subfolder containing the device.
 - Select the device.
- Result: The Device Details pane appears.
- For information on the device details displayed, see [Understanding Device Details, page 4-82](#).
- For information on entering a description in the Description field, see [Entering Device Descriptions, page 4-83](#).
-

Related Topics

- [Manually Changing the State of Devices, page 4-80](#)
- [Entering Device Descriptions, page 4-83](#)
- [Deleting Devices, page 4-85](#)

Understanding Device Details

Some device details are not displayed unless the corresponding parameters are set on the device; for example, location and contact information.

The details shown in the Device Details pane are described in [Table 4-21 on page 4-82](#).

Table 4-21 **Device Details Pane**

Field	Description
Description	<p>A description to be used as the device identifier in WLSE displays. Only the first 30 characters of the device identifier string will be displayed.</p> <p>For information on entering a description in this field, see Entering Device Descriptions, page 4-83.</p> <p>For details on formatting the device identifier string, see Selecting the Device Name Format, page 4-59.</p> <p>Note If you select description as the name format and do not enter a description in Device Details, the name of the device in WLSE displays will be “%description%.”</p>
Device Name	By default, DNS name, IP address, or sysName. For information on which identifier will be displayed, see Enabling Reverse DNS Lookup, page 4-63 .
State	<p>Current state of the device:</p> <ul style="list-style-type: none"> • New—Device was discovered but is neither managed nor unmanaged. • Unmanaged—Device was discovered but was moved to the unmanaged state. • Managed—Device was discovered and is being managed by the WLSE. • Pending—During discovery, a device was found that has the same IP address as this device. For more information on handling duplicate IP addresses, see Handling Duplicate IP Addresses on Access Points, page 4-88. • Deleted—Someone has deleted the device.
SysDescription	Detailed device description.
Version	Software version installed on the device.
Device Family	Device type; for example, Aironet.

Table 4-21 **Device Details Pane (continued)**

Field	Description
SysName	The system name. Not displayed unless set on the device. Note If a device's sysName contains a single quote (') and DNS is not enabled, the IP address will be displayed instead of the sysName.
SysObjectId	Unique identifier that identifies the device type.
Location	Where the device is located. Not displayed unless set on the device.
Device Identity	MAC address. For access points, this is the FastEthernet MAC address.
Serial Number	Device serial number.
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. Not displayed unless set on the device.
Profile	Name of the fault profile that contains threshold values and policy settings for this device; for example, the Default profile.

Related Topics

- [Manually Changing the State of Devices, page 4-80](#)
- [Viewing Device Details, page 4-81](#)
- [Entering Device Descriptions, page 4-83](#)
- [Limitation on the Number of Managed Devices, page 4-86](#)

Entering Device Descriptions

You can enter a description for each device in the Device Details pane. The description you enter is used in displays in one of the following ways:

- This description can be shown as additional information on the device in device detail displays.

- You can specify that this description be used in place of the normal device name in all WLSE displays. To use the description as the device name, you must select the description type as the name format for all devices. You specify the name format in **Devices > Discover > DISCOVER > Advanced Options**.

**Note**

You can search for devices by specifying the description.

Procedure

-
- Step 1** Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The Discovered Devices tree is displayed.
- Step 2** Expand the folder and subfolder containing the device.
- Step 3** Select the device.
Result: The Device Details pane appears.
- Step 4** Enter a description in the Description field, then click **Save**.

**Note**

For the rules about types and numbers of characters you can enter in this field, see [Appendix B, “Naming Guidelines.”](#)

- Step 5** If you want to use this description as the device name in all displays, make sure to chose %description% as the name format type in **Devices > Discover > DISCOVER > Advanced Options**.

For more information about selecting the name format, see [Selecting the Device Name Format, page 4-59](#).

Result: The Device Name field changes to the new name. The new name appears in device trees and other displays.

**Note**

Only the first 30 characters of the device identifier string will be displayed in the device tree.

Related Topics

- [Manually Changing the State of Devices, page 4-80](#)
- [Viewing Device Details, page 4-81](#)
- [Deleting Devices, page 4-85](#)

Deleting Devices

Procedure

- Step 1** Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The Discovered Devices tree is displayed.
- Step 2** Select a folder.
Result: The Group Change Status window appears and all devices in the folder are displayed.
- Step 3** Select the devices you want to delete, then click **Delete**.
- Step 4** You can also delete a single device from its Device Detail screen:
- a. Select the device from its folder.
Result: The Device Detail pane is displayed.
 - b. Click **Delete** at the bottom of the pane.
Result: Deleted devices are removed from the database and from WLSE displays. Database updates could take some time if many devices are being deleted at the same time.
-

Related Topics

- [Manually Changing the State of Devices, page 4-80](#)
- [Limitation on the Number of Managed Devices, page 4-86](#)

Limitation on the Number of Managed Devices

The number of devices that can be managed by a single WLSE is limited, depending on the hardware platform and (for the [WLSE Express](#)) the installed software.

- [Managed Device Limit on the WLSE 1130 Series, page 4-86](#)
- [Managed Device Limit on the WLSE 1030 Express, page 4-87](#)
- [Finding the Managed Device Limit on Your WLSE, page 4-87](#)

Managed Device Limit on the WLSE 1130 Series

The [WLSE 1130 series](#) can manage 2,500 access points and wireless bridges and up to 5,000 radios if you are using only network management features.

If you are also using radio management features, the WLSE can manage 1,800 access points and 3,600 radios.

When you are using only network management features, after you have placed 2,500 access points under management, warning messages are displayed each time you add more devices to the Managed folder. After 2,550 devices are under management, no additional devices can be placed in the Managed folder. Device discovery continues after the absolute limit (2,550 access points) is reached, but no additional devices can be placed under management.



Caution

If you are also using radio management features, you will not get a warning message when you have exceeded 1,800 access points under management.

Routers, switches, and AAA servers are not included in the 2,500-device limit.

Managed Device Limit on the WLSE 1030 Express

As shipped, the [WLSE Express](#) can manage 50 access points and wireless bridges and up to 100 radios.

After you have placed 45 access points under management, warning messages are displayed each time you add more devices to the Managed folder. After the first warning message appears, you can still add a few more devices. After 50 devices are under management, no additional devices can be placed in the Managed folder.

Device discovery continues after the absolute limit has been reached, but no additional devices can be placed under management.

Routers, switches, and external AAA servers are not included in the device limit.

**Note**

You can upgrade a WLSE Express to manage 100 devices and up to 200 radios.

Finding the Managed Device Limit on Your WLSE

You can display the device management limit on your WLSE by running the **show version** CLI command. For example:

show version

```
(C) Copyright 2005 by Cisco Systems Inc.
WLSE 1030 Release 2.11FCS Mon Mar 7 12:59:06 UTC 2005
Device Limit = 100
Build Version (66) Tue Mar 8 06:47:27 UTC 2005
Uptime: 0 days 1 hour 34 mins
Linux version 2.4.28-5_WLSE (root@app20.cisco.com) (gcc version 2.96
20000731 (Red Hat Linux 7.3 2.96-113)) #1 Mon Jan 31 16:16:56 PST 2005

1030
VIA CPU at 1000.058 Mhz with 1025592K bytes of memory.
1 Ethernet interfaces

18.464Gb on disk
```

For information on accessing and using the CLI, see [Appendix A, “Command Line Interface \(CLI\) Commands.”](#)

Related Topics

[Managing Devices, page 4-77](#)

Handling Duplicate IP Addresses on Access Points

The WLSE uniquely identifies a device in network by its identity, which is the MAC address for an access point and the sysname for routers and switches.

The IP address assigned to a device might change for any of the following reasons:

- An existing AP is replaced by a new AP that has the same IP address.
- Addresses are assigned by DHCP. Either the lease time expires or multiple APs are rebooted, causing the APs to renew their IP addresses. Thus, DHCP might assign different IP addresses.
- A user reorganizes the network.

If the WLSE discovers a device (device A) that has an IP address that was previously assigned to device B, the WLSE will assign the correct IP address to device A. The WLSE will then declare that device B has an IP address conflict, and places device B in the Duplicate IP folder.

When the WLSE finds the correct IP address for device B during discovery, it will automatically assign the IP address to device B and also remove device B from the Duplicate IP folder.

The WLSE raises a single “Duplicate IP Address Detected” fault on IP address 127.0.0.1 regardless of the number of devices in the Duplicate IP folder. The fault will remain until the Duplicate IP folder becomes empty.

Such conflicts within the WLSE might be temporary while discovery is in progress and will likely be resolved at the completion of device discovery. This depends on the discovery seeds and the CDP distance. These parameters should be set so that the WLSE discovers or rediscovers all the affected devices.

The WLSE temporarily treats the devices in the Duplicate IP folder in the same way as unmanaged devices. No active management activity will occur on these devices. The WLSE begins to actively manage such a device as soon as it discovers its correct IP address.

The WLSE can usually automatically detect and handle such IP address changes during device discovery if:

- All devices, including the affected devices, are SNMP reachable.
- Device discovery is configured with the correct seeds and CDP distance so that all affected devices will be accessed.

If any devices still remain in the Duplicate IP folder, you may need to do one of the following to resolve this:

- If the device has been removed from the network, you can delete it from the WLSE.
- Check the network to ensure that the device is SNMP reachable. Then explicitly discover the affected devices using the new IP addresses assigned to them with appropriate CDP distance.

When the WLSE resolves all conflicting devices, the “Duplicate IP Address Detected” fault will be automatically cleared.

Managing Device Inventory

During inventory, the WLSE retrieves device attributes to populate its displays (such as reports) and place devices in groups.

The WLSE automatically runs basic inventories on all managed devices and inventories on client associations and trends for specific types of devices. For information about automatic inventories, see [About Inventories, page 4-90](#).

The inventory options are described in [Table 4-22 on page 4-89](#).

Table 4-22 *Inventory Options*

Option	Description	Reference
Run Inventory	Run immediate inventories of selected devices.	Running Immediate Inventories, page 4-93
Polling	Reset the polling intervals for automatic inventories, job retention, and retention of aggregated data for reports.	Changing the Polling Intervals for Automatic Inventories, page 4-91
	Delete all discovery and inventory logs.	Deleting Inventory and Discovery Logs, page 4-93
Logs	View inventory run details.	Viewing Inventory Logs, page 4-98

Related Topics

[About Inventories, page 4-90](#)

About Inventories

Periodic device inventory polling processes retrieve key data from managed devices. Polling processes support these features:

- Inventory-related polled data populate WLSE current and inventory reports.
- Aggregated inventory polled data populates WLSE trending reports.
- Inventory polling is typically run at regular intervals, but can also be run on-demand.
- Other polled data is processed and compared against fault, performance, and configuration policy thresholds.
- Device polling and data aggregation intervals are configurable.

You can view information about inventory jobs in the logs (see [Viewing Inventory Logs, page 4-98](#)) and in the jobvm log. To view or download the jobvm log, select **Admin > Appliance > Status > View Log File** and select the jobvm.log file.

The WLSE features the following kinds of inventories and polling:

- [Automatic Scheduled Inventories, page 4-90](#)
- [Immediate \(Run Now\) Inventories, page 4-91](#)

Automatic Scheduled Inventories

The WLSE runs 3 types of automatic inventories on a regularly scheduled basis:

- **Basic** inventories of all devices. These inventories collect all the information required by the WLSE to populate displays, such as reports, and to place devices in system-defined groups.

In the inventory log, these inventories are named Periodic Inventory.



Note

An automatic basic inventory runs immediately after a device is discovered for the first time if auto-management is turned on. Inventory does not run immediately after a device is rediscovered.

- **Client** inventories that collect only information about associations of clients to access points.

In the inventory log, these inventories are named Client Inventory.

- **Performance** inventories that collect only the performance attributes used in trend reports for access points, bridges, and [AAA](#) servers.

In the inventory log, these inventories are named Performance Inventory.

You can reset the polling intervals for automatic inventories. See [Changing the Polling Intervals for Automatic Inventories, page 4-91](#). You can run immediate or scheduled inventories. See [Running Immediate Inventories, page 4-93](#).

Immediate (Run Now) Inventories

You can run immediate inventories. You select the devices for these inventories.

These are basic inventories of all devices. These inventories collect all the information required by the WLSE to populate displays, such as reports, and to place devices in system-defined groups.

In the inventory log, these inventories are named Run Now Inventory.



Note

The radio management module of the WLSE runs periodic immediate inventories. These inventories appear in the log as normal immediate inventories.

Changing the Polling Intervals for Automatic Inventories

Use the following procedure to change intervals for automatic inventories. For guidelines on choosing intervals, see [Guidelines For Choosing Inventory Intervals, page 4-92](#).



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Inventory > Polling**.

Step 2 Reset polling intervals as follows:

- To reset the interval for the scheduled complete inventory, use the Inventory Poll Interval parameter.
- To reset the interval for the scheduled client inventory, use the Wireless Client Poll Interval parameter.

- To reset the interval for the scheduled performance inventory, use the Performance Attributes Poll Interval parameter.

Step 3 To save your changes, click **Apply**.

Related Topics

- [Managing Polling Parameters, page 4-94](#)
- [Guidelines For Choosing Inventory Intervals, page 4-92](#)

Guidelines For Choosing Inventory Intervals

Following are some suggestions for deciding how to set the polling intervals.

At each interval, the WLSE runs basic, performance, and client inventory. If the actual inventory data collection time exceeds the interval, the WLSE will skip an inventory polling cycle. The next inventory polling will start at the next expected time.

For example, if the recurring scheduled inventory interval is configured to run every 30 minutes and the inventory polling begins at 10:00AM and runs for 32 minutes, the next polling will not begin until 11:00AM. This means that the data may not be as granular as expected.

A second potential problem occurs when the inventory polling takes just slightly less than the interval. In this case, the WLSE will almost always be running inventory polling processes. For example, suppose the recurring scheduled inventory interval is configured to run every 30 minutes, but inventory polling takes just under 30 minutes. In this case, if an inventory polling cycle begins at, for example, 10:00AM and runs until 10:29AM, the next inventory polling begins almost immediately at 10:30AM. This situation may be completely acceptable if the network can tolerate almost constant management polling from the WLSE and if the WLSE CPU and memory utilization do not become overtaxed.

Deleting Inventory and Discovery Logs

**Note**

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Inventory > Polling**.

Step 2 Click **Delete all Discovery and Inventory Logs**.

Result: All discovery and inventory logs will be deleted. There is no way to delete selected logs.

Running Immediate Inventories

You can run immediate inventories of devices that you specify. The inventories you run are basic inventories that collect all the information required by the WLSE to populate displays, such as reports, and to place devices in defined groups.

**Note**

Your login determines whether you can use this option.

When new devices are discovered and managed, basic inventory and client reports are not populated until the next inventory polling occurs. However, you can use this option to populate these reports before the next inventory cycle starts.

This feature can also be useful when configuration changes are made on network devices and you want the changes quickly reflected in the basic and client inventory reports.

Procedure

Step 1 Select **Devices > Discover > Inventory**.

Step 2 Select a group from the Device Selector in the left pane.

For information on how to use the device selector and search for devices, see [Using the Device Selector, page 1-17](#).

For information on the folders and groups listed in the Device Selector, see [System-Defined Groups, page 4-106](#).

- Step 3** All of the devices in the group are added to the list in the Run Inventory Now window. From the list of devices in the group, select the devices you want to inventory.
- Step 4** Click **Run Inventory**. The inventory job starts immediately. Managed devices are polled and information is collected. WLSE displays are updated accordingly.
- Step 5** To view details of an inventory, see [Viewing Inventory Logs, page 4-98](#).
-

Managing Polling Parameters

The Polling option allows you to:

- Reset global parameters that affect inventory polling intervals, job history retention, and retention of data used in reports.
- Delete all inventory and discovery logs.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > Inventory > Polling**. The parameters described in [Polling Parameter Details, page 4-95](#) are displayed.
- Step 2** To work with parameters:
- a. To change parameter values, select new values from the pulldown lists.
 - b. To reset parameters to their previous values, click **Reset** *before* clicking **Apply**.
 - c. To save your changes, click **Apply**. To return to the System Parameters window, click **Back**.

- Step 3** To delete all inventory and discovery logs, click **Delete All Discovery and Inventory Logs**.

Related Topics

[About Trending and Aggregation Data, page 4-97](#)

Polling Parameter Details

The following tables describe the WLSE's polling parameters.

- **Polling Interval Parameters**—Control the intervals during which inventory, wireless client, and performance data will be collected (see [Table 4-23 on page 4-95](#)).
- **Fault and Job Truncation Parameters**—Control the amount of data displayed in fault history tables and job history tables (see [Table 4-24 on page 4-96](#)).
- **Data Retention Parameters**—Control how long to retain the aggregated data used in trend reports (see [Table 4-25 on page 4-97](#)).

For general information about polling intervals and data retention parameters and guidelines for choosing the appropriate settings, see [About Inventories, page 4-90](#).

Table 4-23 *Polling Interval Parameters*

Parameter	Description	Values
Inventory Poll Interval	<p>Interval during which configuration data will be collected from the devices for inventory. This is the data shown in any Web interface device detail table.</p> <p>Tip For more accurate trending, set this parameter at a lower interval than the Performance Attributes Poll Interval.</p>	<p>Default: 12 hours</p> <p>Minimum: 10 minutes</p> <p>Maximum: 7 days</p>

Table 4-23 *Polling Interval Parameters (continued)*

Parameter	Description	Values
Wireless Client Poll Interval	<p>Interval during which data is collected for client inventory. Also, the interval at which Wireless Client reports are updated. Decreasing the interval provides more data points in reports.</p> <p>Tip When managing more than 1,000 access points, you should increase this parameter. The default polling interval generates too much traffic when large numbers of access points are being managed. To poll a set of clients at frequent intervals, use the Scheduled Inventory feature instead of decreasing this parameter; see Running Immediate Inventories, page 4-93.</p>	<p>Default: 51 minutes</p> <p>Minimum: 17 minutes</p> <p>Maximum: 7 days</p>
Performance Attributes Poll Interval	Interval during which performance and utilization data are collected from the devices for the performance inventory.	<p>Default: 31 minutes</p> <p>Minimum: 13 minutes</p> <p>Maximum: 7 days</p>

Table 4-24 *Fault and Job Truncation Parameters*

Parameter	Description	Values
Fault History Truncation Interval	How long displayed fault data is retained. This is the data shown in Fault displays.	<p>Default: 30 days</p> <p>Minimum: 15 days</p> <p>Maximum: 60 days</p>
Job History Truncation Interval	<p>How long displayed job data is retained.</p> <p>Note Recurring jobs are truncated every day to retain the last 30 runs.</p>	<p>Default: 30 days</p> <p>Minimum: 1 day</p> <p>Maximum: 60 days</p>

Table 4-25 Data Retention Parameters

Parameter	Description	Values
Hourly Aggregated Data	How long to retain the reports data that is aggregated hourly.	Default: 7 days Minimum: 1 day Maximum: 15 days
Daily Aggregated Data	How long to retain the reports data that is aggregated daily.	Default: 30 days Minimum: 8 days Maximum: 30 days
Weekly Aggregated Data	How long to retain the reports data that is aggregated weekly.	Default: 6 months Minimum: 1 month Maximum: 12 months
Monthly Aggregated Data	How long to retain the reports data that is aggregated monthly.	Default: 12 months Minimum: 1 month Maximum: 24 months

About Trending and Aggregation Data

Raw trending data retrieved from inventory polling is placed in database trending tables as follows:

- Every hour, this trending table data is processed into an **hourly** aggregation table.
- Every 24 hours, the first level aggregated data is processed into the **daily** aggregation table.
- The daily aggregation table data is aggregated every seven days into a **weekly** aggregation table.
- The weekly aggregation table is aggregated every 30 days into the **monthly** aggregation table.

The data in the trending and aggregation tables is periodically purged. For the minimum, default, and maximum data retention intervals, see [Polling Parameter Details, page 4-95](#).

Data retention intervals are configurable globally through the system parameters interface. Under almost all circumstances, there is no reason to change the defaults. In some large WLAN deployments, however, the WLSE database may begin to grow so large that it makes sense to purge data more often. Because it may affect the accuracy of the data in the trending reports, be careful when you change the data retention intervals.

Viewing Inventory Logs

This option allows you to view historical information about inventories.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > Inventory > Logs**.
- Step 2** The names of inventory jobs indicate the type of inventory that was run, as explained in the following table.

Table 4-26 *Inventory Job Log*

Field	Description
Name	Type of inventory: <ul style="list-style-type: none"> • Periodic—basic automatic, scheduled inventory of all devices. • Client Inventory—automatic inventory or client associations with access points. • Performance Inventory—automatic inventory of performance attributes for trend reports. • Run Now Inventory—on-demand inventory of selected devices run by a user, or generated by the radio management module.
Start Time	When the inventory started.
Recurring	Yes—automatic scheduled inventory or inventory scheduled by a user. No—on-demand inventory run by a user or the radio management module.

Table 4-26 *Inventory Job Log (continued)*

Field	Description
State	Scheduled—scheduled to run at a later time. Blank field—a Run Now inventory.
User	Username—User who ran the inventory. WLSE—Automatic, scheduled inventory or inventory run by the radio management module.

Step 3 To view details about a job, select the job. The Run Log shows the start and end times of the job and type of data that was collected. The Run Log for immediate inventories shows which devices you selected for inventory. For more information, see [Run Log Details—Inventory, page 4-99](#).

Step 4 You can change the job history retention period. For information, see [Managing Polling Parameters, page 4-94](#).

Related Topics

[Diagnosing Common Inventory Problems, page 4-100](#)

Run Log Details—Inventory

Most inventory run log messages show the start and end time, the type of data collected, and the devices that were inventoried.

You may also see error messages, such as the following:

- No logs available. Waiting for resources to start job—Other jobs are running. Information on your job will be displayed when resources are available.

This message also appears if there are many SNMP timeouts on the network or devices are not reachable through SNMP. In that case, the inventory job will take much longer to finish, and the next scheduled inventory will not run until the current job finishes.

Related Topics

[Diagnosing Common Inventory Problems, page 4-100](#)

Diagnosing Common Inventory Problems

You can view the inventory process log files using the interface in **Devices > Discover > Inventory > Logs**. Open the appropriate folder within the Inventory sub-tree—the tree leaves correspond to the inventory runs. The logs are sorted in each folder by start time, with the most recent runs at the top.

If you have problems with your inventory processes and you open a case with the Cisco TAC, they may ask you for the jobvm log, which you can retrieve by selecting **Admin > Appliance > Status > View Log File**.

You might be able to assist the Cisco TAC by getting more detailed information than what normally appears in the logs. To increase the level of logging:



Note You must be logged in as an administrative user to use this interface.

1. Navigate to the WLSE interface at http://wlse_ip:1741/debug/logging.jsp.
2. Select **Debug**.
3. Click **Save**.
4. Run the inventory again to get more logging details.

After the inventory runs:

1. Navigate back to WLSE interface at http://wlse_ip:1741/debug/logging.jsp.
2. Select **Default**.
3. Click **Save**.



Note Except for troubleshooting purposes, do not run any logging level other than Default. Running at a level higher than Default might impact the performance of the WLSE.

Exporting Devices

You can export all managed devices (access points, routers, switches, and AAA servers) to:

- A CiscoWorks server running Resource Manager Essentials—see [Exporting Devices to a CiscoWorks Server](#), page 4-101.
- A comma-separated values (CSV) file—see [Exporting Devices to a CSV File](#), page 4-103.

**Note**

Unmanaged devices are not exported.

Exporting Devices to a CiscoWorks Server

This option allows you to export all managed devices (access points, switches, and routers) and any AAA servers you have added to a CiscoWorks server. Unmanaged devices are not exported.

The information exported consists of the IP addresses and credentials.

The time required to export devices depends on the number of devices exported and the response from the CiscoWorks 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 **Devices > Discover > Export Devices**, then select **To CiscoWorks**.
- Step 2** Enter the following information:
- The CiscoWorks server IP address.
 - The CiscoWorks server port number. You may need to contact the administrator of the CiscoWorks server.
 - The username and password of any user who has the authority to export and import device credentials on the CiscoWorks server.

Step 3 Click **Export**.

Step 4 To see the export status log, click the **Status** or **Last Status**.

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

The following information is included in the export status log:

Table 4-27 Messages—Export Status Log

Type of Information or Message	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 CiscoWorks server while it was sending a response to the WLSE.
Error: Could not connect to CiscoWorks server: <i>ip_address</i> on port: <i>port_number</i> .	Either the host or the port specified in the WLSE export dialog was wrong.
Error: Connected to CiscoWorks server: <i>ip_address</i> on port: <i>port_number</i> successfully, but server returned error after connection.	Either the username or the password specified in the WLSE export dialog was wrong.

Step 5 To see other information about the export, go to **Admin > Appliance > Log File** and select the cwexport..log file. For more information about viewing logs, see [Using WLSE Log Files, page 15-5](#).

Step 6 After you export devices, you can view them in CiscoWorks Resource Manager Essentials (RME) (see the RME online help for details).

Exporting Devices to a CSV File

This option allows you to export all managed devices (access points, switches, and routers) and any AAA servers you have added to a CSV file. Devices that are unmanaged are not exported.

The information exported for each device is:

- IP address or hostname
- Community strings
- Telnet password
- Enable password

For more information on CSV files, see [About CSV Files, page 4-43](#).



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Export Devices**, then select **To CSV File**.



Note Device credentials are exported to a plain text file.

Step 2 For added security during the transmission of credentials, you can switch your browser to HTTPS and use HTTPS for downloading the file.

To launch an HTTPS session, enter the following URL:

```
https://wlse_ip/
```

where *wlse_ip* is the IP address of the WLSE. Note that you do not append a port number to the IP address when using HTTPS.

- If you did not create an unsigned certificate when you initially configured the WLSE, a Security Client dialog box appears, telling you that there is no valid certificate. For information about creating a certificate, see [Managing SSL \(HTTPS\), page 15-24](#).

- If you created a certificate but have not previously logged in via HTTPS, a Security Client dialog box appears. Enter the following information when prompted:
 - Click **Yes**.
 - Click **View Certificate**.
 - Click **Install Certificate**.
 - Click **Next** on remaining screens, then click **Finish**
 - Click **OK**.
 - Log out of the HTTP session on the browser and log back in to an HTTPS session.
 - Click **Yes** in the Security Client window that appears after you log in.
 - Select **Devices > Discover > Export Devices**, then select **To CSV File**.

Step 3 Click **Download CSV File**, then click **Save**. Specify the filename and location if different from the default.



Note The filename should have a .txt extension.

Result: The file is saved to your desktop.

Managing Groups

When you select **Devices > Group Management**, the Group Details window appears. Both system-defined and user-defined groups appear in the device selector. System-defined groups cannot be edited or deleted. For detailed information on system-defined and user-defined groups, see [About Groups, page 4-105](#).

The group management window allows you to:

Function	Reference
View system and user-defined groups	Using the Group Details Window, page 4-109
Create a new static group	Creating a Static Group, page 4-112
Create a new dynamic (rule-based) group	Creating a Rule-Based Group, page 4-114
Create a new static or rule-based group by copying an existing group	Creating a Static Group by Copying a Static or Rule-Based Group, page 4-116 Copying a Rule-Based Group, page 4-117
Edit a group	Editing a Static Group, page 4-119 Editing a Rule-Based Group, page 4-120
Delete a group	Deleting a Static or Rule-Based Group, page 4-121

Related Topics

- [Managing Device Discovery, page 4-33](#)
- [Managing Device Inventory, page 4-89](#)

About Groups

The WLSE grouping feature lets you organize managed devices into logical subsets and hierarchies. Using device grouping, you can quickly configure, upgrade, and view reports for a set of access points as a single operation.



Note Only managed devices can become members of groups.

The Group Details window allows you to view the existing device groups and categorize devices into named groups. A group is a named entity that can contain devices, other groups, or a combination of devices and groups. There are two types of groups:

- System-defined groups—See [System-Defined Groups, page 4-106](#).
- User-defined groups—See [User-Defined Groups, page 4-108](#).

The device 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 objects it contains (devices and other groups) 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 one or more user-defined groups.

Groups can be dynamic or static:

- In dynamic groups, devices are added as they are discovered or as polling indicates key parameters have changed. Dynamic groups are either the pre-configured, system-defined groups or user-defined groups that have rules assigned to them (rule-based groups).
- Static groups are user-created groups that must have devices added or deleted from them manually.

System-Defined Groups

You cannot edit or delete a system-defined group. The system-defined groups are dynamic (rule-based), and are automatically populated by reading information from the devices during discovery and inventory collection. Any changes to devices are reflected in the system-defined groups only after the next discovery or inventory collection has completed.

System-defined groups are contained in folders; for example, the system-defined groups for device type are contained in the Device Type folder.

If devices are not configured correctly, they may not appear in the system-defined groups. For example, a WDS access point that is not correctly configured will not be included in the Active WDS or Backup WDS system groups.



Tip

A complete listing of supported devices can be found in the *Supported Devices Table for the CiscoWorks Wireless LAN Solution Engine, 2.12*. For help in locating this document, see [Finding WLSE Documentation on Cisco.com, page 1-21](#).

For details on the system defined groups, see [Table 4-28 on page 4-107](#).

Table 4-28 **System-Defined Groups**

Folder Name	Group Name/Description
Device Type	<p>A group for each device type:</p> <ul style="list-style-type: none"> • AAA Servers—EAP and RADIUS. AAA servers include APs configured as AAA servers and the built-in AAA server on the WLSE Express. Servers are added to groups after you add the servers to the WLSE (see Monitoring AAA Servers, page 4-21). • AP 1100 • AP 1130 • AP 1210 (also contains AP 1230 devices) • AP 1240 • AP 350-IOS • Bridge 1300 • Bridge 1400 • Routers • Switches
More System Groups	<ul style="list-style-type: none"> • SSID—Group for each SSID configured on access points. • Software Version—Group for each software version installed on access points. • Subnet—Group for each subnet in the network. For example, 10.10.10.5.
Physical Location	<p>Group for each building defined by users in the Location Manager.</p> <ul style="list-style-type: none"> • To create, modify, and delete Physical Location groups, use the Location Manager. • To add devices to Physical Location groups or remove them from Physical Location groups, use the Location Manager. If you delete devices from the WLSE by using Devices > Discover > Managed Devices, those devices are automatically removed from the Physical Location groups.

Table 4-28 System-Defined Groups (continued)

Folder Name	Group Name/Description
Wireless Domain Services (WDS)	Groups for WDS devices: <ul style="list-style-type: none"> Active WDS—Contains the access point or Wireless LAN Services Module (WLSM) that is actively providing WDS services. Backup WDS—Contains the backup WDS access points or WLSMs.
Scanning AP	Group for access points that are configured for scanning-only mode or that have an interface configured for scanning mode.

User-Defined Groups

You can define any number of groups. User-defined groups can either be static or rule-based:

- You add devices manually to static groups. Static groups can be subgroups of other static groups or can be placed at the top (root) level.

Although there is no limit on the number of levels in a group hierarchy, we recommend that you define no more than four levels. With too many levels, system performance degrades and navigation becomes difficult.

- For rule-based groups, you specify a set of rules that determine which devices are to be included in the group. The membership in rule-based groups is dynamic; when devices that match the defined rules become managed, they automatically become members of the group. All user-defined rule-based groups are placed at the top (root) level. You cannot create a subgroup of a rule-based group.

Useful user-created groups in a WLAN greatly depend on the structure of the network and the application demands. Table 4-29 contains examples of groups that might be worthwhile in a typical wireless LAN environment.

Table 4-29 Examples of User-Defined Groups

Main Group	Sub-Groups
Campus	Main, Library, Dormitory, Athletic Field
RF Power	1mw, 2mw, 5.5mw, 30mw, 100mw
Radio Combinations	802.11a&b, 802.11a&g, 802.11b only

Table 4-29 Examples of User-Defined Groups

Main Group	Sub-Groups
Department	Accounting, Marketing, Sales, Manufacturing
Special Features	Proxy Mobile IP
Antenna Type	Patch, Omni
Channels	1,2,3,4,5,6,7,8,9,10,11

Using the Group Details Window


Note

Your login determines whether you can use this option.

To view details about a group and use group management functions:

Procedure

-
- Step 1** Select **Devices > Group Management**.
- Step 2** Select a group from the device selector. The following details about the group are displayed.

Table 4-30 Group Details Window Fields

Field	Description
Description	Description entered when the group was created or edited (if any). Can be up to 256 characters long.
Created by	Username of the creator of the group.
Type	System Group, Static Group, or Rules-Based Group.

Table 4-30 Group Details Window Fields (continued)

Field		Description
Group Members	Member Type	Device—A device, such as access point or switch. Subgroup—A subgroup of the group you selected.
	Name	Hostname of a member device or name of a subgroup. <ul style="list-style-type: none"> Click a device name to display a window containing links to available reports and (for access points) a link to the AP's web interface. For a list of the items displayed, see Links to Reports from the Group Details Display, page 4-111. Click a subgroup name to see details for the subgroup in a separate window.
	IP Address	IP address of a member device.
	Device Type	Device type of a member device
	Software Version	Software version installed on a member device.

Step 3 Depending on the type of group you selected, the following buttons appear at the bottom of the window.

Table 4-31 Group Details Window Buttons

Button	Function	Reference
Create Static Group	Create static group.	Creating a Static Group, page 4-112.
Create Rule-Based Group	Create rule-based group.	Creating a Rule-Based Group, page 4-114.
Copy	Copy static or rule-based group.	Creating a Static Group by Copying a Static or Rule-Based Group, page 4-116 Copying a Rule-Based Group, page 4-117
Copy Static	Make static copy of a rule-based group.	Copying a Rule-Based Group, page 4-117
Edit	Edit static or rule-based group.	Editing a Static Group, page 4-119 or Editing a Rule-Based Group, page 4-120
Delete	Delete group.	Click Delete to delete the group.

Links to Reports from the Group Details Display

The following reports can be displayed from the Group Details window by clicking the name of a device in the current group. A window opens displaying links to the following reports and a link to the Web interface of the access point.

Table 4-32 Report Types

Device Type	Reports Displayed	Reference
Access point	Summary Report	Displaying an AP Summary Report, page 10-70
	Detailed Report	Displaying a Detailed Report, page 10-74
	Fault Status	Viewing the Fault Status Report, page 10-15
	Device History	Viewing Device History, page 10-15
	Config History	Viewing Config History, page 10-16
	Firmware History	Viewing Firmware History, page 10-17
	AP Web Page	Opens a browser window to AP, displaying Summary Status.
	AP Config	Current configuration of the access point.
Switch	Summary Report	Displaying a Switch Summary Report, page 10-88
	Fault Status	Viewing the Fault Status Report, page 10-15
	Device History	Viewing Device History, page 10-15
Router	Summary Report	Displaying a Router Summary Report, page 10-90
	Fault Status	Viewing the Fault Status Report, page 10-15
	Device History	Viewing Device History, page 10-15
AAA Server	Summary Report	Displaying a Server Summary Report, page 10-92
WDS	Summary Report	Viewing the WDS Summary Report, page 10-12

Creating a Static Group



Note

Your login determines whether you can use this option.

To create a new static group:

Procedure

- Step 1** Select **Devices > Group Management**.
- Step 2** Click **Create Static** and enter the following information:

- Enter a name in the Name text box. Names can be up to 64 characters long.
- Enter a description in the Description text box (optional). Descriptions can be up to 256 characters long.

For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).

- Step 3** The new group becomes the subgroup of whatever choice you make from the **Subgroup Of** list. To place the group at the top level of the tree, select **root**.



Note Your new group will be added to the **Subgroup Of** list.

- Step 4** Select a group or device from the device selector in the left pane. For information on how to use the device selector or search for devices, see [Using the Device Selector, page 1-17](#).

The group or device is added to the Available Devices list in the Create Group dialog.

- Step 5** To add devices to the group, select the group or individual devices from the Available Devices list and click >>.



Note After a device or group is added to the Devices in Group list, it is removed from Available Devices. Clicking on the device or group adds it back to the Available Devices list.

- Step 6** To add more devices, repeat Step 5.

- Step 7** To remove devices from the group, select them from the **Devices in Group** list and click <<.

- Step 8** To save the group, click **Save**. The new group is displayed in alphabetical order in the group list.

To cancel the group creation and discard your changes, click **Cancel**.

Related Topics

[Creating a Static Group by Copying a Static or Rule-Based Group, page 4-116](#)

[Copying a Rule-Based Group, page 4-117](#)

Creating a Rule-Based Group

To create a new rule-based group:



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Group Management**.

Step 2 Click **Create Rule-Based Group** and enter the following:

- Enter a name in the Name text box. Names can be up to 64 characters long.
- (Optional) enter a description in the Description text box. Descriptions can be up to 256 characters long.



Note

New groups are always added at the top level ([root]).

For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).

Step 3 The new group becomes the subgroup of whatever choice you make from the **Subgroup Of** list. To place the group at the top level of the tree, select **root**.



Note

Your new group will be added to the **Subgroup Of** list.

Step 4 Define the rules for determining the devices that will be added to the group.

The available rules are described in the following table. You can use an asterisk (*) as a wildcard to match any number of characters.

- You must select at least one rule. A rule determines which devices are in the group or which devices are excluded from the group:
 - If you select Equals, devices that match the rule definition will be included in the group.
 - If you select Not Equals, devices that match the rule definition will be excluded from the group.

Rule Name	Data to Select or Enter
Software Version	The name of the software version; for example, 12.01T1, 12.2(4)JA1, or 12*
sysLocation	The sysLocation defined on devices, if any. An empty string matches all devices that do not have this variable set.
Device Type	Select an access point type from the list, if this group contains access points.
Subnet	A subnet, in decimal-dot format; for example 172.10.10.10 or 172.*
SSID	An SSID defined on devices.
VLAN ID	The existing VLANs configured on managed access points.

All of the rules you select are added together (logical *and*). For example, if you select the following Equals rules: Device Type AP1100, subnet 171.69.* and Software Version 12.2*, only the AP1100 access points in the specified subnet and running the specified firmware will be part of the group.

If you need to group devices that match more than one parameter in a given rule you can create a group that contains subgroups. For example, a group consisting of the AP1100 access points at two different sysLocations could be constructed by creating a group that contains a subgroup for each sysLocation.

- Step 5** To preview the group, click **Preview**. The rule(s) you defined and any currently managed devices that match the rule(s) are displayed.
- Step 6** To reset the window to its contents before this session, click **Reset**.
- Step 7** To save the group, click **Save**. The new group is added, in alphabetic order, to the list of groups.

All currently managed devices that match the group rules will be added to the group. All devices that become managed later and match the rules will also be added to the group.

Related Topics

[Copying a Rule-Based Group, page 4-117](#)

Creating a Static Group by Copying a Static or Rule-Based Group

**Note**

Your login determines whether you can use this option.

Use this procedure to create a new static group by copying an existing static or rule-based group (including system-defined groups).

Procedure

- Step 1** Select **Devices > Group Management**. The group selector pane and group dialog box are displayed.
- Step 2** Select any group:
 - For system-defined groups and other rule-based groups, click **Copy as Static**.
 - For static groups, click **Copy**.
- Step 3** Edit the name and description. The description is optional.

Names and descriptions can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).
- Step 4** To change the place of the group in the hierarchy, select a group from the **Subgroup Of** list. The group you are editing becomes a subgroup of whatever group you choose. To place the group at the top level of the tree, select **root**.
- Step 5** The devices in the group you copied appear in the Devices in Group list.
- Step 6** To add more devices, you can search for devices or select a group or device from the device selector in the left pane. For information on how to use the device selector or search for devices, see [Using the Device Selector, page 1-17](#).
 - a.** The device or group is added to the Available Devices list in the Create Group dialog.
 - b.** Select the group or individual devices from the **Available Devices** list and click >>.
 - c.** To add more devices, select another group.
- Step 7** To remove devices from the group, select them from the Devices in Group list and click <<.

Step 8 To save the new group, click **Save**. The group is added, in alphabetic order, to the list of groups.

By default, new static groups are placed under the same parent as the group you are copying; you can select another parent from the **Subgroup of** list. New static groups are added to the **Subgroup of** list.

To cancel group creation and discard your changes, click **Cancel**.

Related Topics

- [Editing a Static Group, page 4-119](#)
- [Deleting a Static or Rule-Based Group, page 4-121](#)
- [About Groups, page 4-105](#)

Copying a Rule-Based Group

By copying an existing rule-based group (a user-defined group or a system group), you can create a new rule-based group or a new static group.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Group Management**.
- Step 2** Select the group you want to copy and click **Copy** to create a rule-based group or **Copy Static** to create a static group.
- If you selected **Copy Static** to create a new static group, see [Creating a Static Group by Copying a Static or Rule-Based Group, page 4-116](#).
 - If you are creating a new rule-based group, continue to Step 3. The new group will be placed at the top (root) level.
- Step 3** Edit the group name and description, if desired. A description is optional.

Names and descriptions can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).

- Step 4** To change the place of the group in the hierarchy, select a group from the **Subgroup Of** list. The group you are editing becomes a subgroup of whatever group you choose. To place the group at the top level of the tree, select **root**.
- Step 5** Add rules as follows:

Rule Name	Data to Select or Enter
Software Version	The name of the software version; for example, 12.01T1, 12.2(4)JA1, or 12*.
sysLocation	The sysLocation defined on devices, if any. An empty string matches all devices that do not have this variable set.
Device Type	Select an access point type from the list, if this group contains access points.
Subnet	A subnet, in decimal-dot format; for example 172.10.10.10, or 172.*.
SSID	An SSID defined on devices.
VLAN ID	An existing VLAN configured on managed access points.

- Step 6** To save the group, click **Save**. The new group is displayed and added to the top (root) level in alphabetic order.
- To reset the window to its contents before this session, click **Reset**.
- To cancel group creation and discard your changes, click **Cancel**.

Editing a Static Group

**Note**

Your login determines whether you can use this option.

To edit a static group:

Procedure

-
- Step 1** Select **Devices > Group Management**.
 - Step 2** Select the group and click **Edit**.
 - Step 3** Change the Name or Description by editing the text in the relevant text boxes.
Names can be up to 64 characters long, and descriptions can be up to 256 characters long. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).
 - Step 4** To change the place of the group in the hierarchy, select a group from the **Subgroup Of** list. The group you are editing becomes a subgroup of whatever group you choose. To place the group at the top level of the tree, select **root**.
 - Step 5** To add devices to the group, select a group or device from the device selector in the left pane. For information on how to use the device selector or search for devices, see [Using the Device Selector, page 1-17](#).
 - a. Select the group or individual devices from the list and click **>>**. Devices are placed in the Devices in Group list.
 - b. To add more devices, select another group.
 - Step 6** To delete devices from the group, select one or more devices from the Devices in the Group list and click **<<**.
 - Step 7** To save your changes, click **Save**. The edited group is displayed. To discard your changes, click **Cancel**.
-

Related Topics

- [Creating a Static Group, page 4-112](#)
- [Deleting a Static or Rule-Based Group, page 4-121](#)

- [About Groups, page 4-105](#)

Editing a Rule-Based Group



Note

Your login determines whether you can use this option.

To edit a user-defined rule-based group:

Procedure

- Step 1** Select **Devices > Group Management**.
- Step 2** Select the group and click **Edit**.
- Step 3** Change the Name or Description by editing the text in the relevant text boxes. A description is optional.

Names can be up to 64 characters long, and descriptions can be up to 256 characters long. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page B-1](#).
- Step 4** To change the place of the group in the hierarchy, select a group from the **Subgroup Of** list. The group you are editing becomes a subgroup of whatever group you choose. To place the group at the top level of the tree, select **root**.
- Step 5** Edit rules as follows:

Rule Name	Data to Select or Enter
Software Version	The name of the software version; for example, 12.01T1, 12.2(4)JA1, or 12*
sysLocation	The sysLocation defined on devices, if any. An empty string matches all devices that do not have this variable set.
Device Type	Select an access point type from the list, if this group contains access points.
Subnet	A subnet, in decimal-dot format; for example, 172.10.10.10, or 172.*.

Rule Name	Data to Select or Enter
SSID	An SSID defined on devices.
VLAN ID	The existing VLANs configured on managed access points.

- Step 6** To save your changes, click **Save**. The edited group is displayed.
To reset the window to its contents before this session, click **Reset**.
To discard your changes, click **Cancel**.
-

Deleting a Static or Rule-Based Group



Note

Your login determines whether you can use this option.

To delete a user-defined (static or rule-based) group:

Procedure

- Step 1** Select **Devices > Group Management**.
- Step 2** Select the group from the group selector list.
- Step 3** Click **Delete**.
- Step 4** Click **OK** in the popup window. The group will be deleted.
-

Related Topics

- [About Groups, page 4-105](#)
- [Editing a Static Group, page 4-119](#)
- [Creating a Static Group, page 4-112](#)

