

Managing Devices

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

The topics covered in this chapter are:

- [Devices Tab Functions, page 3-2](#)
- [Getting Started with Device Management, page 3-3](#)
- [Setting Up Devices, page 3-5](#)
- [Specifying Device Credentials, page 3-27](#)
- [Managing AAA Servers, page 3-37](#)
- [Managing Device Discovery, page 3-41](#)
- [Managing and Unmanaging Devices, page 3-75](#)
- [Managing Device Inventories, page 3-79](#)
- [Exporting Devices, page 3-93](#)
- [Managing Groups, page 3-96](#)

Devices Tab Functions

The Devices tab provides the facilities for 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 a detailed guide to using these options, see [Getting Started with Device Management, page 3-3](#).

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 your login.

The options under the Devices tab are:

- Discover subtab:
 - Manage Devices—See [Managing and Unmanaging Devices, page 3-75](#)
 - Discover—See [Managing Device Discovery, page 3-41](#)
 - Device Credentials—See [Specifying Device Credentials, page 3-27](#)
 - Inventory—See [Managing Device Inventories, page 3-79](#)
 - Export Devices—See [Exporting Devices, page 3-93](#)
 - AAA Server—See [Managing AAA Servers, page 3-37](#)
- Group Management subtab—See [Managing Groups, page 3-96](#)

Getting Started with Device Management

Before you can use the WLSE to manage newly added devices, you must set up the devices, configure the WLSE, discover the devices, and move the devices to the managed state. Optionally, you can set up your own device groupings to make management easier. To get started, follow the steps listed in the following illustration and 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.

- The alternatives for setting up access points and bridges are:
 - Configure each device manually—see [Set Up Non-IOS Access Points and Bridges](#), page 3-6 and [Set Up IOS Access Points](#), page 3-8.
 - Use automatic startup configuration—see [Assigning a Startup Configuration](#), page 4-300.
- To set up routers and switches, see [Set Up Routers and Switches](#), page 3-24.
- To set up AAA servers, see [Set Up AAA Servers](#), page 3-25.

Step 2: Enter device credentials

Enter device credentials on the WLSE:

- Enter community strings for all managed devices—see [Enter SNMP Community Strings for All Devices](#), page 3-28.
- Enter HTTP usernames and passwords for non-IOS access points—see [Enter HTTP Usernames and Passwords—Non-IOS Access Points](#), page 3-32.
- Enter Telnet credentials for IOS access points—see [Enter Telnet and SSH Usernames and Passwords—IOS Access Points](#), page 3-33.
- Enter HTTP ports for IOS access points—see [Enter HTTP Port Settings—IOS Access Points](#), page 3-35.
- Enter information about setting up AAA servers—see [Managing AAA Servers](#), page 3-37.

Step 3: Discover Devices

Initiate discovery from the WLSE or import devices:

- Add seed devices and run discovery—see [Managing Device Discovery](#), page 3-41.
- Import devices—see [Importing Devices from a File](#), page 3-59 and [Importing Devices from a CiscoWorks Server](#), page 3-61.

Step 4: Verify discovery

Verify that devices were discovered—see [Viewing Discovery Logs](#), page 3-69.

Step 5: Move devices to managed state

Before you can use configuration, reporting, and monitoring features, you must either move devices to the managed state on the WLSE, or specify that all discovered devices be automatically managed—see [Managing and Unmanaging Devices](#), page 3-75.

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 Inventories](#), page 3-79.

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 the on-demand inventory to populate these reports before the next inventory cycle starts. You can also use on-demand polling 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, upgrade, and view reports for a set of access points as a single operation—see [Managing Groups, page 3-96](#).

Step 8: Use all WLSE 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.

Setting Up Devices

You must set up devices before the WLSE can discover and manage them and before you can use the WLSE for the following tasks: discovery, monitoring, reporting, configuration, and firmware upgrade. In addition, IOS access points must be configured for radio management. This section describes both required and optional setup tasks for the following devices:

- Non-IOS access points—see [Set Up Non-IOS Access Points and Bridges, page 3-6](#)
- IOS access points—See [Set Up IOS Access Points, page 3-8](#)
- Routers and switches—See [Set Up Routers and Switches, page 3-24](#)
- AAA servers—[Set Up AAA Servers, page 3-25](#)

Set Up Non-IOS Access Points and Bridges

You can set up access points and bridges in two ways:

- By using the WLSE's automatic configuration option for first-time device configuration and applying a configuration template to a number of access points. For more information, see [Automating Configurations, page 4-300](#).
- By opening a web browser session on each access point and performing the tasks in the following table. To use this method, you must first configure each access point or bridge for web browsing.

Table 3-1 Set Up Procedures for Non-IOS Access Points and Bridges

Tasks	Procedure	Notes
1. Enable Cisco Discovery Protocol (CDP).	<ol style="list-style-type: none"> 1. In the Summary Status page, click Setup. 2. Under Services: Cisco Services, click Cisco Discovery Protocol. 3. Select Enabled. Click Apply or OK. 	Required for the WLSE to use CDP to discover the device.
2. Enable SNMP. (Optional) Set the location. (Optional) Set the system name and system contact.	<ol style="list-style-type: none"> 1. In the Summary Status page, click Setup. 2. Under Services, click SNMP. 3. Select Enabled. 4. Enter a System Name, System Location, and System Contact. 5. Click Apply or OK. 	SNMP is required for the WLSE to discover devices, populate reports, transfer configuration information to devices, and upgrade device firmware. Setting the system name, system contact, and system location ensures that this information is included in device detail displays.

Table 3-1 Set Up Procedures for Non-IOS Access Points and Bridges (continued)

Tasks	Procedure	Notes
3. Set the read community string.	<ol style="list-style-type: none"> 1. In the Summary Status page, click Setup. 2. Under Services, click Security. 3. Click User Information; then click Add New User. 4. Create a user with all privileges, including SNMP, Firmware, Write, and Admin privileges. In addition, for access points that are running a firmware version earlier than 12.01(T), assign Ident privileges. 5. Click Apply or OK. 	The read community string is required for device discovery and populating reports.
4. Set the read-write community string.	<ol style="list-style-type: none"> 1. In the Summary Status page, click Setup. 2. Under Services, click Security. 3. Click User Information; then click Add New User. 4. To create a user with SNMP read/write privileges, enter a username and password and select the Write, SNMP, Firmware, and Admin privileges. 5. Click Apply or OK. 	The read-write community string is required for configuration and firmware jobs.
<p>5. Add an HTTP user with the ability to modify firmware, and enable the User Manager.</p> <p>You can use the same user that you created in Task 4, if the user has firmware privileges.</p>	<ol style="list-style-type: none"> 1. In the Summary Status page, click Setup. 2. Click Security. 3. Click User Information; then click Add New User. 4. Enter a username and password and select Firmware; then click Apply. 5. Navigate back to the Security Setup page and click User Manager. 6. Select Enabled; then click Apply or OK. 	<p>This allows configuration uploads from the WLSE to access points.</p> <p>You must also enter HTTP users and passwords on the WLSE (see Enter HTTP Usernames and Passwords—Non-IOS Access Points, page 3-32).</p>

Table 3-1 Set Up Procedures for Non-IOS Access Points and Bridges (continued)

Tasks	Procedure	Notes
6. Set up TFTP as the transfer protocol between the WLSE and access points.	<ol style="list-style-type: none"> 1. In the Summary Status page, click Setup. 2. Under Services, click FTP. 3. Use the pulldown menu to select TFTP as the file transfer protocol. 4. In the Default File Server text box, enter the IP address of the WLSE. 5. Click Apply or OK. 	TFTP is used for transferring configuration changes to access points.

Set Up IOS Access Points

This section provides:

- Procedures to prepare IOS access points for basic network management by the WLSE—See [Basic Network Management Setup—IOS Access Points, page 3-8](#).
- Procedures to prepare IOS access points and the WLSE for participation in the Cisco Structured Wireless-Aware Network (SWAN)—See [Radio Management Setup—IOS Devices, page 3-13](#).

Basic Network Management Setup—IOS Access Points

You can set up access points and bridges in the following ways:

- Use the WLSE's automatic configuration option for first-time device configuration and applying a configuration template to a number of access points—See [Automating Configurations, page 4-300](#).
- Log into each device by using Telnet or SSH and use the device's CLI commands—See [Set Up IOS Access Points by Using the Device CLI, page 3-9](#).
- Log into each device's Web interface—See [Set Up IOS Access Points by Using the Device Web Interface, page 3-11](#).

After you set up a device, all of its MIB variables can be accessed and the device can be discovered by the WLSE.



Note VLAN information for IOS access points might not be collected by the WLSE if WEP keys are not configured in each VLAN. This affects VLAN reports, grouping, and faults. VLAN information becomes accessible through SNMP as soon as WEP keys are configured.



Note If you are using Wireless Domain Service (WDS), you must configure both the WLSE and an IOS access point that supports WDS (currently, Cisco Aironet 1100 or 1200). In addition, an AAA server is required. For procedures, see [Enter WLCCP Credentials for Wireless Domain Services, page 3-36](#).

Set Up IOS Access Points by Using the Device CLI

Procedure

- Step 1** Use Telnet or SSH to log into the AP 1100 or AP 1210.
- Step 2** Enter enable mode.
- Step 3** Enter global configuration mode.
- Step 4** Enable CDP by entering the following command:

```
cdp run
```



Note You can find out whether CDP has been enabled by using the **show cdp** command in enable mode.



Note If you do not wish to use CDP, you can add all access points as seeds or import devices. For more information, see [Managing Device Discovery, page 3-41](#).

- Step 5** Enter the following commands in the sequence shown. The first two commands set the read-only SNMP community string and create an ISO view, which enables discovery and the fault and report features on the WLSE. The third command sets a read/write community string, which allows you to use the WLSE to update access point firmware and configuration.

```
snmp-server view iso iso included
snmp-server community community_string view iso RO
snmp-server community community_string RW
```



Note These community strings must be entered on the WLSE. See [Enter SNMP Community Strings for All Devices, page 3-28](#).



Note IOS access points that do not have an ISO view will be placed in the Misconfigured Devices system group after discovery and fault will be generated. The fault refers to a “dot 11 MIB” problem.

- Step 6** You can use either Telnet or SSH to push configuration templates to IOS access points. To use templates to configure IOS access points, you must configure either Telnet or SSH or both. See Steps 7 and 8 to enable and configure SSH and Telnet.
- Step 7** To enable and configure SSH, enter the following commands. In these commands, *hostname* is the hostname of the access point, and *domain_name* is your network’s domain name (for example, cisco.com). At the prompt for the number of bits in the modulus, press **Return** to accept the default or enter a value.

```
hostname hostname
ip domain-name domain_name
crypto key generate rsa
How many bits in the modulus [512]:
```

The following commands are recommended, but optional:

```
ip ssh time-out 120
ip ssh authentication-retries 3
```

- Step 8** To configure Telnet, enter the following commands:

```
line 0 4
no access-class 111 in
```

The following commands are recommended, but optional:

```
width 80
length 24
```

Step 9 Exit global configuration mode, then enter the following command:

```
write memory
```

Set Up IOS Access Points by Using the Device Web Interface

Procedure

Step 1 Log into the Web interface of the AP 1100 or AP 1210 device.

Step 2 Select **SERVICES** from the menu, then click **CDP**:

- a. After Cisco Discovery Protocol (CDP), select **Enabled**.
- b. Click **Apply**.



Note If you do not wish to use CDP, you can add all access points as seeds or import devices. For more information, see [Managing Device Discovery, page 3-41](#).

Step 3 You can use either Telnet or SSH (secure shell protocol) to push configuration templates to IOS access points. To use templates to configure IOS access points, you must configure either Telnet or SSH or both. See Steps 4 and 5 to enable SSH and Telnet.

Step 4 To enable and configure SSH (secure shell protocol), enter the following:

- a. Select **SERVICES > Telnet/SSH**.
- b. Enable **Secure Shell**.
- c. Enter a System Name.
- d. Enter a Domain Name (for example, cisco.com).
- e. (Optional) Enter the RSA key size.
- f. (Optional) Enter the Authentication Timeout.

- g. (Optional) Enter Authentication Retries.
- h. Click **Apply**.

Step 5 To enable and configure Telnet:

- a. Select **SERVICES > Telnet/SSH**.
- b. Enable **Telnet**.
- c. (Optional) Enable **Teletype**.
- d. Enter the number of Columns.
- e. Enter the number of Lines.
- f. Click **Apply**.

Step 6 Select **SNMP** from the menu.

- a. After Simple Network Management Protocol (SNMP), select **Enabled**.
- a. Click **Apply**.

Step 7 In the SNMP Request Communities section, enter a community string for the ISO view. This community string is required for discovery and to enable the fault and report features of the WLSE.

- a. Enter the community string in the SNMP Community field.
- b. Enter **iso** in the Object Identifier field.



Note

IOS access points that do not have an ISO view will be placed in the Misconfigured Devices system group after discovery, and a fault will be generated. The fault message refers to a “dot11 MIB problem.”

- c. Click **Read-Only**.
- d. Click **Apply**.

Step 8 In the SNMP Request Communities section, enter a community string to enable firmware and configuration updates on the access point.

- a. Enter the community string in the SNMP Community field.
- b. Click **Read-Write**.
- c. Click **Apply**.

- Step 9** The community strings created in Steps 7 and 8 must be entered on the WLSE before the device can be discovered and other WLSE features can be used. For more information, see [Enter SNMP Community Strings for All Devices, page 3-28](#).
-

Radio Management Setup—IOS Devices



Note

The basic network configuration must first be done on all of the access points. See [Basic Network Management Setup—IOS Access Points, page 3-8](#).

Setting up access points for radio management involves configuring all access points to register with Wireless Domain Services (WDS). WDS provides wireless client roaming and radio management aggregation.

Only Cisco Aironet 1100 and 1200 access points support WDS. For information about the supported access points and IOS firmware versions, see the WLSE 2.7 Supported Devices Table on [cisco.com](#).

Each WDS access point supports one subnet and up to 30 infrastructure access points. You can add additional WDS access points for redundancy. The priorities you set on the WDS access points determine which one is the primary, and which ones are backups.

The requirements for radio management are:

- Configure the WDS devices that will provide services to the infrastructure access points—See [Configure WDS Access Points, page 3-14](#).
- Configure the infrastructure access points to authenticate to the WDS—See [Configure Infrastructure Access Points, page 3-20](#).
- Configure the WLSE with WLCCP credentials—See [Configuring the WLSE, page 3-21](#).
- Define authentication server(s)—See [Configuring Authentication, page 3-14](#).
- Confirm the configuration—See [Confirming the Configuration, page 3-22](#).

Configuring Authentication

To use WDS, both the infrastructure APs and the WLSE must use LEAP to authenticate to the WDS devices. For this purpose, you can use:

- Local authentication on a WDS device. See [Configure WDS Access Points, page 3-14](#).
- AAA servers that you have already configured, or configure servers as described in [Set Up AAA Servers, page 3-25](#).

Configure WDS Access Points



Note

Before making changes to device configuration, you should back up the current configuration, and test the new configuration on non-production devices.

WDS must be active on an access point in each layer-2 domain; backup WDS access point(s) can also be defined in each layer-2 domain.

Configuring WDS involves the following. See the rest of this section for detailed instructions.

- Define the AAA servers and server groups that the WDS will use to LEAP authenticate infrastructure access points and/or wireless clients.
- Enable WDS and set WDS priorities.
- Enter the WMN IP address.

There are three ways to configure WDS access points:

- Using the access point web interface—See [Using the Access Point Web Interface, page 3-15](#).
- Using the access point CLI interface—See [Using the Access Point CLI Interface, page 3-16](#).
- Using a WLSE configuration template—[Using a WLSE Configuration Template, page 3-18](#).

Using the Access Point Web Interface

To configure WDS access points by using the web interface:

-
- Step 1** Log in to an AP that will serve as a WDS device.
- Step 2** Select **Wireless Services > WDS**.
- Step 3** Select the Settings tab.
- Step 4** To enable WDS, select **Use this AP as Wireless Domain Services**.
- Step 5** Enter a value between 1 and 255 in the **Wireless Domain Services** priority field.
The priority value is used to determine which AP will be the active WDS AP when multiple APs are configured to run WDS. The highest priority is 255.
- Step 6** Configure the Wireless Network Manager (WNM) options:
- Select **Configure Wireless Network Manager**.
 - Enter the IP address of your WLSE in the **Wireless Network Manager IP Address** field.
 - Click **Apply**.
- Step 7** Define the AAA server(s) that will be used to LEAP authenticate infrastructure access points participating in SWAN:
- Select the Server Groups tab.
 - Enter a server group name.
 - From the **Priority** lists, select the appropriate AAA servers.
If no AAA servers have been entered into the AP, click **Define Servers** to add the servers, then select the appropriate servers. Consult the AP online help for assistance in entering AAA servers into the AP.
 - Under **Use Group For**, select **Infrastructure Authentication**.
- Step 8** The WDS takes over 802.1x authenticator responsibilities for all access points in the subnet that are registered and authenticated with the WDS. If you are using any EAP type for authentication, *you must define a separate server group for client authentication*. The server group for client authentication may contain the same servers defined in the group for infrastructure authentication.
- Select the Server Groups tab.
 - Enter a server group name.
 - From the **Priority** lists, select the appropriate AAA servers.

d. Under **Use Group For**, select **Client Authentication**.

e. Select the appropriate **Authentication Settings**.

See the access point documentation for more details on wireless client authentication through WDS.

Step 9 Configure the WDS AP to authenticate itself to the WDS so that it can participate in the SWAN hierarchy:

a. Select **Wireless Services > AP**.

b. Select **Enable**.

c. Enter a username and password that can be LEAP authenticated by the AAA servers in the infrastructure server group.

Step 10 To commit the configuration, click **Apply**.

Using the Access Point CLI Interface



Tip

Consult the IOS and access point documentation for details on the subtleties of IOS commands.

The key steps in configuring the WDS are:

- Configure AAA servers to authenticate SWAN infrastructure access points and/or wireless clients.
- Configure WDS.
- Configure the WNM.

To configure the WDS access points using the IOS command line interface:

Step 1 Log in to an access point that will be a WDS device.

Step 2 Turn on AAA services:

```
aaa new-model
```

Step 3 Define the RADIUS servers that you will use for infrastructure authentication and/or client authentication. Consult your RADIUS server documentation for the correct port numbers. CiscoSecure ACS uses port 1645 for authorization and port 1646 for accounting.

```
radius-server host [ ip_address | hostname ] auth-port port
acct-port port key shared_secret_key
```

Step 4 Define a server group for infrastructure authentication:

```
aaa group server radius server_group_name server radius_server
```

Step 5 Define at least one additional server group for wireless client authentication.

Step 6 Configure the AP to run WDS:

```
wlccp wds priority priority interface BVI1
```

where *priority* is a value from 1 to 255. Priority determines which AP will be the active WDS AP when multiple APs are configured to run WDS. The highest priority is 255.

Step 7 Configure the Wireless Network Manager (WNM) component:

```
wlccp wnm ip address wlse_ip_address
```

where *wlse_ip_address* is the address of the WLSE.

Step 8 Configure the server group the WDS will use to LEAP authenticate SWAN infrastructure access points:

```
aaa authentication login named_authentication_list group
infrastructure_authentication_server_group_name
```

```
wlccp authentication-server infrastructure named_authentication_list
```

Step 9 The WDS takes over 802.1x authenticator responsibilities for all access points in the subnet that are registered and authenticated with the WDS. If you are using any EAP type for authentication, *you must configure another server group for client authentication*. The server group for client authentication may contain the same servers defined in the group for infrastructure authentication.

Use the following commands:

```
aaa authentication login named_authentication_list group
client_authentication_server_group_name
```

```
wlccp authentication-server client [ any | eap | leap | mac ]
named_authentication_list
```

Step 10 The WDS access point must also register and authenticate itself to the WDS to participate in the SWAN hierarchy, so the WDS AP is also an infrastructure AP. Configure the WDS access point as an infrastructure access point:

```
wlccp ap username username password password
```

Using a WLSE Configuration Template

You can use the WLSE to configure one or more WDS access points.

The major configuration steps are:

- Create a configuration template to set up AAA servers and the WDS.
- Apply the configuration template to the appropriate access points by running a configuration job.



Note

Your login determines whether you can use this option.

To configure WDS access points by using a WLSE configuration template:

-
- Step 1** Log in to the WLSE web interface.
- Step 2** Select **Configure > Templates**.
- a. Enter a template name, selecting IOS as the template type.
 - b. Click **Create New**.
- Step 3** Enter the AAA servers that will be used to LEAP authenticate the infrastructure access points and the WLSE to the WDS, and the AAA servers that will be used to authenticate wireless client devices:
- a. Select **Security > Server Manager**.
 - b. In the Corporate Servers section, for each server, enter the IP address, select RADIUS, and enter the shared secret.
 - c. Click **Save**.
- Step 4** Select **Wireless Services > WDS** to configure the WDS parameters.
- In the Global Properties section:
- a. Select **Enable**.
 - b. Enter the Wireless Domain Services priority. This value determines which access point will serve as the active WDS when multiple access points are configured to run WDS on the same subnet. Valid priority values are 1-255, with 255 being the highest.

- c. Enter the WLSE's IP address in the WNM IP Address field.
 - Step 5** Configure a server group for authenticating the SWAN infrastructure components.
In the Server Groups section:
 - a. Enter one or more server names or server IP addresses.
 - b. Under Use Group For, select Infrastructure Authentication.
 - c. Click **Save**.
 - Step 6** The WDS takes over 802.1x authenticator responsibilities for all access points in the subnet that are registered and authenticated with the WDS. This means that if you are using any EAP type for authentication, *you must also define a separate server group for client authentication.*

The server group for client authentication may contain the same servers defined in the group for infrastructure authentication.

In the Server Groups section:
 - a. Enter one or more server names or server IP addresses.
 - b. Under Use Group For, select Client Authentication.
 - c. Select the appropriate client Authentication Settings.
 - d. Click **Save**.
 - Step 7** The WDS access point must also register and authenticate itself to the WDS to participate in the SWAN hierarchy, so the WDS AP is also an infrastructure AP. To authenticate and register the WDS AP as an infrastructure AP:
 - a. Select **Wireless Services > AP Configuration**.
 - b. Select **Enabled** as the Wireless Services option.
 - c. Enter a username and password that can be LEAP authenticated by the AAA servers in the infrastructure server group.
 - Step 8** (Optional) Select **Preview** to see a preview of the configuration template.
 - Step 9** Select **Save**, then click the **Save** button.
 - Step 10** Select **Yes** to apply the template immediately or select **No** to save the template. For information on configuration jobs, see [Managing Jobs, page 4-267](#).
-

Configure Infrastructure Access Points

The infrastructure access points initiate participation in SWAN by registering and LEAP authenticating with the WDS.

The only required configuration for infrastructure access points is the username and password used to register with the WDS.

There are three ways to configure infrastructure access points:

- Using the access point web interface—See [Using the Web Interface to Configure Infrastructure APs, page 3-20](#).
- Using the access point CLI interface—See [Using the Command Line Interface to Configure Infrastructure APs, page 3-20](#).
- Using a WLSE configuration template—See [Using a WLSE Configuration Job to Configure Infrastructure APs, page 3-21](#).

Using the Web Interface to Configure Infrastructure APs

To use the web-based interface to configure infrastructure APs:

-
- Step 1** Log in to the AP's web interface.
 - Step 2** Select **Wireless Services > AP**.
 - Step 3** Select **Enabled**.
 - Step 4** Enter the username and password for authenticating the infrastructure AP to the WDS.
 - Step 5** Click **Apply**.
-

Using the Command Line Interface to Configure Infrastructure APs

To use the command line interface to configure infrastructure APs:

-
- Step 1** Log in to the AP's CLI.
 - Step 2** Enter the following command:


```
wlccp ap username username password password
```

where *username* and *password* are the credentials for authenticating the infrastructure access point to the WDS.

Using a WLSE Configuration Job to Configure Infrastructure APs

The WLSE can be used to configure multiple infrastructure APs in a single job. To configure infrastructure APs using the WLSE, create a configuration template using the template creation wizard, then apply the template in a configuration job. For more information about using the template creation wizard and the configuration job interface, see [Chapter 5, “Using IOS Templates.”](#)

**Note**

Your login determines whether you can use this option.

To configure the username and password used to authenticate the AP to the WDS:

- Step 1** Log in to the WLSE web interface.
 - Step 2** Select **Configure > Templates**.
 - Step 3** Select **Wireless Services > AP Configuration**.
 - Step 4** Select **Enabled**.
 - Step 5** Enter the username and password for LEAP authenticating infrastructure APs to the WDS.
 - Step 6** Create a configuration job to apply the template to the appropriate devices. For information on configuration jobs, see [Managing Jobs, page 4-267](#).
-

Configuring the WLSE

The WLSE is the Wireless Network Manager (WNM) component of SWAN. The WLSE polls and aggregates radio management data from WDS devices and processes this data. The following configuration is required on the WLSE for radio management:

- SWAN components communicate via a Cisco proprietary technology called [WLCCP](#). You must enter the WLCCP username and password in the WLSE. This username and password is used to LEAP authenticate the WLSE to the WDS APs in the network. See [Enter WLCCP Credentials for Wireless Domain Services](#), page 3-36.
- Enter the SNMP read-only and read/write communities for all managed IOS access points. See [Enter SNMP Community Strings for All Devices](#), page 3-28.
- Enter Telnet/SSH credentials for IOS access points. See [Enter Telnet and SSH Usernames and Passwords—IOS Access Points](#), page 3-33.

Confirming the Configuration

After the configuration is complete, there are two ways to confirm that they are correct and that the SWAN components are properly communicating:

- Using the Web interface—See [Using the Web-based Interface to Validate the Configuration](#), page 3-22.
- Using the command-line interface—See [Using the Command-Line Interface to Validate the Configuration](#), page 3-23.

Using the Web-based Interface to Validate the Configuration

To confirm the configurations using the web-based interface on WDS APs:

Step 1 Log in to the web interface on each WDS AP.

Step 2 Select **Wireless Services > WDS > WDS Status**.

Check for the following:

- The WDS Information section should display the device WDS state as ACTIVE.
- The WDS Registration and AP Information sections should show the correct number of APs (all of the infrastructure APs and the WDS AP).
- The Mobile Node Information section should display the wireless clients participating in SWAN.

- The Wireless Network Manager section should contain the WLSE IP address. If the WLSE authentication status is SECURITY KEYS SETUP, the WLSE is properly registered.
-

Using the Command-Line Interface to Validate the Configuration

To use the CLI on the WDS APs to validate the configuration:

Step 1 Log in to the CLI on each WDS AP.

Step 2 To validate the WDS configuration, enter:

```
show wlccp wds ap
```

This command lists all of the infrastructure APs and the WDS AP.

Step 3 To verify that the WLSE is correctly registered, enter:

```
show wlccp wnm status
```

This command should display the WLSE IP address. If the WLSE authentication status is SECURITY KEYS SETUP, the WLSE is properly registered.

Set Up Routers and Switches



Note

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

On each router and switch, configure the following:

Table 3-2 Setup Procedures for Routers and Switches

Task	Procedure	Notes
1. Enable CDP and verify that access points and bridges are visible from the router or switch.	<ol style="list-style-type: none"> In enable mode, verify that CDP is running on the device by using one of the following commands: <ul style="list-style-type: none"> On IOS-based devices—show cdp run. On Hybrid OS-based Catalyst switches—show cdp. If CDP is not running, in global configuration mode, enter cdp run to enable CDP. To verify that access points or bridges are visible in the device's CDP table, enter show cdp neighbors. 	CDP is required for the WLSE to discover the device.
2. Enable SNMP and set up community strings.	<p>On IOS-based devices, enter configuration mode and use the snmp community community_string ro command.</p> <p>On Hybrid OS-based Catalyst devices, enter enable mode and use the set snmp community read-only community_string command.</p>	SNMP is required for the WLSE to discover and manage the device.

Table 3-2 Setup Procedures for Routers and Switches (continued)

Task	Procedure	Notes
3. (Optional) Set the system name, contact, and location variables.	<p>On IOS-based devices, enter configuration mode and use the following commands.</p> <ul style="list-style-type: none"> Set system name—hostname <i>name</i> Set system contact—snmp contact <i>contact</i> Set location—snmp location <i>location</i> <p>On Hybrid OS-based Catalyst switches, enter enable mode and use the following commands:</p> <ul style="list-style-type: none"> Set system name—set system name <i>name</i> command. Set system contact—set system contact <i>contact</i> Set location—set system location <i>location</i> 	<p>These variables make the device more manageable.</p> <p>The system name, system contact, and location will appear in the device detail displays.</p>

Set Up AAA Servers

The WLSE can monitor the performance of AAA (Authentication, Authorization, and Accounting) services provided by CiscoSecure ACS server. The WLSE can also monitor a Cisco Access Registrar (CAR) RADIUS server. The services supported are LEAP, RADIUS, EAP-MD5, and PEAP (EAP-GTC only).

To enable monitoring, you must:

- Configure CiscoSecure ACS server to recognize the WLSE as a client. Follow the procedure in this section on each server.



Note

For PEAP, besides the procedure in this section, you must set up a certificate and private key on the ACS server and then enable PEAP. For more information, see the CiscoSecure ACS documentation.

- Configure the WLSE to add information about servers. For more information, see [Managing AAA Servers, page 3-37](#).

In addition to monitoring AAA servers, the WLSE uses an AAA server to authenticate to a Wireless Domain Services (WDS) access point. To enable this authentication, make sure an AAA server is configured as described in this section. You must also configure the WDS access point and the WLSE. For more information, see [Enter WLCCP Credentials for Wireless Domain Services, page 3-36](#).

Procedure

Step 1 Log into the CiscoSecure ACS Server that will provide authentication services to the wireless network.



Note You will need the IP address or name of the system on which CiscoSecure ACS Server is running when you configure the WLSE.

Step 2 Click **User Setup** on the left side of the initial page.

Step 3 Enter a username for the user the WLSE will use for synthetic transactions and click **Add/Edit**.

Step 4 Enter a password in the first set of Password and Confirm Password fields. Click **Submit**.



Note You will need this name and password when configuring the WLSE.

Step 5 Click **Network Configuration** on the left side of the page.

Step 6 Click **Add Entry**. In the Add AAA Client area, enter the WLSE information in the following text boxes:

- Client Hostname—enter the WLSE hostname (or IP address)
- Client IP—enter the WLSE IP address
- Key—enter a secret key



Note You will need this key when configuring the WLSE.

Step 7 Select RADIUS (Cisco Aironet) from the Authenticate Using list.

- Step 8** Click **Submit** or **Submit+Restart**. A restart is required for the changes to take effect.
-

Specifying Device Credentials

Before the WLSE device discovery or device polling can successfully communicate with the network devices, the WLSE must be aware of the appropriate device SNMP credentials to use.

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

- For all managed devices, you must enter SNMP credentials.
- For access points, the following additional credentials are required:
 - For IOS-based access points, you must enter Telnet or SSH credentials and IOS HTTP port settings.
 - For non-IOS access points, you must enter HTTP credentials.
- If you are using Wireless Domain Services (WDS), you must enter RADIUS credentials and configure the WDS access point.

The Device Credentials options are:

- **SNMP Communities**—Specify community strings for managed devices. Using this option, you can specify device [community strings](#), other required device credentials, and ports. Community strings are required for discovery, and community strings and other credentials are required for other WLSE functions. See [Enter SNMP Community Strings for All Devices, page 3-28](#).
- **HTTP User/Password**—Specify the HTTP usernames and passwords for configuring non-IOS access points. See [Enter HTTP Usernames and Passwords—Non-IOS Access Points, page 3-32](#).
- **Telnet/SSH User/Password**—Specify the Telnet usernames and passwords for IOS access points. See [Enter Telnet and SSH Usernames and Passwords—IOS Access Points, page 3-33](#).
- **IOS HTTP Port Settings**—Specify the HTTP ports for IOS access points. See [Enter HTTP Port Settings—IOS Access Points, page 3-35](#).

- **WLCCP Credentials**—Specify the RADIUS credentials for Wireless Domain Service (WDS). See [Enter WLCCP Credentials for Wireless Domain Services](#), page 3-36.

Enter SNMP Community Strings for All Devices

The Wireless LAN Solution Engine uses a device's read-only [SNMP](#) community string to discover the device and populate reports and uses the read/write community string to configure the device and update firmware. 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 is *public* for both the read-only string and the read-write string. If the community strings on your devices differ from the defaults, you must specify the community strings on the WLSE before the discovery process can begin and before you can configure the devices.

If you are importing devices from a file or CiscoWorks, 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 3-59 and [Importing Devices from a CiscoWorks Server](#), page 3-61.

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 3-54.



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > Device Credentials > SNMP Communities**. The SNMP Communities dialog box contains a default entry that covers all devices, provided device community strings are set to the default (*public*).

Step 2 To add community strings, use either of the following methods to enter the community strings you created during initial device setup. For more information, see [Setting Up Devices, page 3-5](#).

- Use the individual text boxes and list for the variables: Hostname (IP address), Read Community, SNMP Timeout, SNMP Retries, and Write Community. Then click **Add**. The community string appears in the large text box.
- Enter the data directly in the large text box. Use the following syntax:

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



Note

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

[Table 3-3](#) describes the community string variables.

Table 3-3 Community String Variables

Variable	Description	Notes
target	The IP address of a device or range of devices that use these community strings.	If you do not specify a target, the default community strings apply to all devices in the network.
read_community	A password allowing read-only access to the target devices.	You must specify the read community string. Otherwise, the default value of <i>public</i> is used.
timeout	The length of time (seconds) the server waits for a response from the device before performing the first retry.	The default is 10 seconds. If you increase the timeout period, discovery could take significantly longer to complete. The minimum value is one and the maximum value is 60.

Table 3-3 Community String Variables (continued)

Variable	Description	Notes
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	The password that allows write access to the target devices.	You must specify the write community string. Otherwise, the default value of <i>public</i> is used.

Step 3 To modify a community string, make your changes directly in the large text box.

Step 4 Click **Save** to apply your changes.

Related Topics

- [Community String Guidelines, page 3-30](#)
- [Recommendations For Configuring SNMP Credentials, page 3-31](#)

Community String Guidelines

Use these guidelines when adding or modifying community strings:

- You can assign community strings to any of the following:
 - Complete IP address; for example, 172.20.4.9
 - Any wild cards (based on IP addresses); for example:
 - *.*.*.*
 - 172.*.*.*
 - Address ranges, which can include wild cards; for example:
 - 27.20.[4-55].*
 - 172.[21-30].[44-88].*
 - 172.*.*.[121-255]

- You can add a combination of general and specific entries, but the WLSE reads the community strings from most specific to least specific.
- If you enter duplicate community strings for a device, the most specific community string is used.
- All printable characters, except for colons (:), are allowed in community strings.
- Spaces are not allowed in community strings.
- Comments are not allowed.

Recommendations For Configuring SNMP Credentials

This section contains information about setting the SNMP credentials on the WLSE.

Community Strings

When there are multiple potential entries, the WLSE will use the most specific SNMP community entry for a device IP. In the case of equally specific entries, the WLSE will select the first entry in the list, which may not be the correct community.

SNMP Timeouts and Retries

Exercise 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. To do this:

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 8-36](#)) 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 Guidelines, page 3-30](#)

Enter HTTP Usernames and Passwords—Non-IOS Access Points

HTTP usernames and passwords are required for downloading configuration files to non-IOS access points. The password must be set on each access point, and you can enter as many usernames and passwords as necessary on the WLSE. For more information about setting passwords on access points, see [Setting Up Devices, page 3-5](#).



Note

Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > Device Credentials > HTTP User/Password**.
- Step 2** To add a username and password:
 - a. Enter the access point IP address or range of IP addresses that will use this username and password.

For information on using ranges and wildcards in IP addresses, click **Learn More** or see [Entering IP Addresses, page 3-35](#).

- b. Enter the username.
- c. Enter the password.
- d. Click **Save**. The IP address and username are added to the Current Entries text box.

Step 3 To modify an entry:

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

Step 4 To delete an entry, select it from the Current Entries text box and click **Delete**.

Related Topics

[Chapter 4, “Configuring Devices”](#)

Enter Telnet and SSH Usernames and Passwords—IOS Access Points

Telnet or SSH (SSH1 only) usernames and passwords are required for applying configuration templates to IOS access points and for upgrading firmware on IOS 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 [Setting Up Devices, page 3-5](#).

The Telnet/SSH credentials you enter in this dialog must match the login sequence on the IOS access points. For example, if the device prompts for an enable password only, enter the Enable Password only. Do not enter a User Name or User Password. Otherwise the WLSE will not be able to open a login session on the device.



Note

Your login determines whether you can use this option.

Procedure

Step 1 Select **Devices > Discover > Device Credentials > Telnet/SSH User/Password**.

Step 2 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 3-35 .
Username	Telnet username. Note If the device is configured for a Telnet password only, enter a user password but leave the Username field blank.
User Password	Telnet password.
Confirm Password	
Enable Password	Telnet enable password.
Confirm Enable Password	

Step 3 To add more entries, repeat Step 2.

Step 4 To modify an entry:

- a. Select the entry from the Current Entries text box.
- b. 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**.

Related Topics

[Chapter 4, “Configuring Devices”](#)

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 Port Settings—IOS Access Points

HTTP port settings are required for reports on IOS 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.



Note

For non-IOS access points, there is no need to specify HTTP ports. Port information is collected during inventory.

Procedure

-
- Step 1** Select **Devices > Discover > Device Credentials > IOS HTTP Port Settings**.

- Step 2** To add a port:
- 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 3-35](#).
 - Enter the port number.
 - 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 configure an AAA server, enter [WLCCP](#) credentials on the WLSE, and configure the WDS access point. The steps in setting up WDS on the network are:

- [1. Configure an AAA Server, page 3-36](#)
- [2. Configure the WLSE, page 3-36](#)
- [3. Configure the WDS Access Points, page 3-37](#)

1. Configure an AAA Server

Use an AAA server that you have already configured, or configure a server as described in [Set Up AAA Servers, page 3-25](#).

2. Configure the WLSE

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 that you set for the WLSE on the AAA server.
- Step 3** To modify the WLCCP credentials, modify the fields as needed.
- Step 4** To save the credentials, click **Save**.

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

3. Configure the WDS Access Points

WDS is currently supported on two types of IOS-based access points: Cisco Aironet 1100 and Cisco Aironet 1200. The WDS access points must be managed by the WLSE.

To configure an access point to provide WDS:

Step 1 Log in to the access point's CLI interface.

Step 2 In configure mode, enter the following command:

```
# wlccp wnm ip address x.x.x.x
```

where *x.x.x.x* is the WLSE's IP address.

Step 3 In enable mode, verify that authentication is working by entering the following command:

```
# show wlccp wnm status
```

If the command returns a status of SECURITY KEYS SETUP, the WLSE has authenticated successfully with the WDS.

Related Topics

[Viewing the WDS Summary Report, page 6-4](#)

Managing AAA Servers

The options in this screen allow you to:

- Add AAA servers—See [Adding an AAA Server, page 3-39](#).
- Remove AAA servers—See [Removing an AAA Server, page 3-40](#).
- Edit AAA server entries—See [Modifying an AAA Server, page 3-40](#).

**Note**

Before the WLSE can monitor your AAA servers, you must configure the servers to add the WLSE as a client. For information on adding the WLSE as a client on AAA servers, see [Set Up AAA Servers, page 3-25](#).

Related Topics

- [About AAA Servers, page 3-38](#)
- [Set Up AAA Servers, page 3-25](#)

About AAA Servers

Before adding Authentication, Authorization, and Accounting (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 AAA servers, see [Set Up AAA Servers, page 3-25](#).

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**. The WLSE can monitor AAA services provided by Cisco Secure ACS.

If you are using Wireless Domain Services (WDS), you will also use an AAA server to allow the WLSE to authenticate with the WDS access point. For more information, see [Enter WLCCP Credentials for Wireless Domain Services, page 3-36](#).

- The services supported by the WLSE are
- EAP-MD5
- LEAP
- PEAP (EAP-GTC only)
- RADIUS

For information about changing the polling interval and response time fault thresholds for AAA server monitoring, see [Specifying Fault Thresholds, page 2-37](#).

Adding an AAA Server



Note

Before the WLSE can monitor your AAA servers, you must configure the servers to add the WLSE as a client. For information on adding the WLSE as a client on AAA servers, see [Set Up AAA Servers, page 3-25](#).

Procedure

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

Step 2 Enter the following data:

Field	Description
Show List	Select server type from the pulldown list: <ul style="list-style-type: none"> • EAP-MD5 • LEAP • PEAP (EAP-GTC only) • RADIUS
Server Name	Hostname or IP address of the AAA server.
Server Port	Port on the server that is used for authentication; this should always be 1645.
Username	Client username that you entered on the LEAP server.
Password	Client password that you entered on the LEAP server.
Secret	Shared secret key that you entered on the LEAP server.

Step 3 Click **Save**.

Step 4 To discard your entries, click **Cancel**.

Removing an AAA Server

Procedure

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

Modifying an AAA Server

Procedure

-
- Step 1** Select **Devices > Discover > AAA Server**.
 - Step 2** Select the server type from Show List; all servers of that type are displayed.
 - Step 3** Select the server to be modified.
 - Step 4** Modify any of the following characteristics of the server:

Field	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 LEAP server.
Password	Client password that you entered on the LEAP server.
Secret	Shared secret key that you entered on the LEAP server.

- Step 5** Click **Save**.
 - Step 6** To discard your entries, click **Cancel**.
-

Managing Device Discovery

By default, the WLSE runs Cisco Discovery Protocol (CDP) discovery every 24 hours. You can use the options under **Devices > Discover > DISCOVER** to:

- Run additional CDP discoveries and modify the default schedule.
 - For more information, see [About Discovery, page 3-41](#).
 - To run CDP discoveries, see [Using the Discovery Wizard, page 3-54](#).
- Discover devices by importing them from a file or from a CiscoWorks server.
 - For more information, see [About Discovery, page 3-41](#).
 - To run device imports, see [Using the Discovery Wizard, page 3-54](#).



Note After devices are discovered, they must be put under management—see [Managing and Unmanaging Devices, page 3-75](#). Unmanaged devices do not appear in WLSE displays.

- Set advanced options that modify the behavior of discovery and device management—See [Setting Advanced Options, page 3-63](#).
- Set up IP address filtering for discovery—See [Using Discovery IP Address Filtering, page 3-67](#).
- View discovery job details—See [Viewing Discovery Logs, page 3-69](#).

About Discovery

The topics covered in this section are:

- [Understanding Discovery and Management, page 3-42](#)
- [Understanding WLSE Discovery Methods, page 3-43](#)
- [About CDP-Based Discovery, page 3-44](#)
- [About Individual Device Seeding, page 3-46](#)
- [About Device Import From a File, page 3-47](#)
- [About Device Import From CiscoWorks, page 3-51](#)
- [About CSV Files, page 3-49](#)

Understanding Discovery and Management

Network devices are interrogated by the WLSE by multiple processes: discovery and inventory polling.

Device discovery is a periodic process that finds new devices and possibly topology and network changes. The WLSE can discover Cisco wireless access points and bridges, and Cisco switches or routers that have Cisco wireless devices attached to them. The discovery process can be run at scheduled intervals or on-demand.

Discovered devices can exist in one of two states: managed and unmanaged. By default, newly-discovered devices are in the unmanaged state and will not be polled until manually moved 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 3-1](#) illustrates the managed/unmanaged state machine.

Figure 3-1 *Device Management 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.

Understanding WLSE Discovery Methods

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

- CDP-based discovery
- Individual device seeding
- Device import from a file
- Device import from CiscoWorks Resource Manager Essentials (RME)

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



Note AAA servers must be input individually regardless of discovery method. See [About AAA Servers, page 3-38](#).

Table 3-4 *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 3-44 .

Table 3-4 *Discovery Options (continued)*

Discovery Method	Use This Method When...
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 This method forces the user to input each device IP address, so it may not scale.</p> <p>For more information, see About Individual Device Seeding, page 3-46.</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 3-47.</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 3-51.</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.



Note To configure a scheduled or recurring CDP-based discovery process, or to run a CDP-based discovery on-demand, see [Using the Discovery Wizard, page 3-54](#).

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
- Change the default CDP schedule

Devices must be properly configured for access by the WLSE before they can be discovered and managed (see [Setting Up Devices, page 3-5](#)).

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 3-46](#).

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 3-46](#)
- [About Device Import From a File, page 3-47](#)
- [About Device Import From CiscoWorks, page 3-51](#)

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 or the scheduled discovery options 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 Options, page 3-63](#).
- IP Filter Rules—See [Using Discovery IP Address Filtering, page 3-67](#).

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 3-56](#)) for each device during the import process. The WLSE will do this even if there are already entries that qualify for the devices configured.

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 3-69](#)), the name of the import from file is shown as `CDPDiscovery_Import_Devices_number`.

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 also 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 > 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 Options, page 3-63](#).
- IP Filter Rules—See [Using Discovery IP Address Filtering, page 3-67](#).

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:
 - **RMEDiscovery**—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_number**—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.

Pre-Discovery Checklist

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



Note This list is only the requirements for successful device discovery. To use other WLSE features, other configuration requirements exist. For details about how to configure the specific device parameters, see [Chapter 4, Configuring Devices](#).

- CDP enabled on network devices (for CDP-based discovery).
- SNMP communities configured on network devices.
 - Read-only SNMP community on switches and routers.
 - Correct access capabilities for SNMP communities on non-IOS-based wireless access points and bridges.
 - Read-only SNMP community strings configured for IOS-based wireless access points.
- SNMP communities entered into WLSE device credentials fields.
- WLSE configured as network access server (NAS) for CiscoSecure Access Control Server (ACS) (for RADIUS, LEAP, EAP-MD5 server monitoring) or equivalent in other AAA servers.
- WLSE synthetic transaction user created on AAA server.

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 3-54](#). The discovery methods are:

- CDP discovery—see [Running CDP Discovery, page 3-54](#)
- Device import from a file—see [Importing Devices from a File, page 3-59](#)
- Device import from a CiscoWorks server [Importing Devices from a CiscoWorks Server, page 3-61](#)

Using the Discovery Wizard

The discovery wizard provides the following choices for discovering devices.

Procedure

Step 1 Select a discovery option:

Option	Description	Reference Information
CDP Discovery	Runs immediate or scheduled discovery by using Cisco Discovery Protocol (CDP).	About Discovery, page 3-41
Import from File	Imports devices from a file.	
Import from CiscoWorks	Runs immediate or scheduled imports from a CiscoWorks server (uses Resource Manager Essentials).	

Step 2 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 > CDP Discovery**.

The tasks for running CDP discovery are:

Table 3-5 Tasks for CDP Discovery

Type Discovery	Task	Reference
Run Now	Select Run Now.	Select the Type of CDP Discovery, page 3-55
	Specify SNMP communities	Enter SNMP Communities, page 3-56
	Specify initiating IP addresses (seeds)	Enter Initiating IP Addresses, page 3-57
	Verify your settings and finish	Verify Your Settings and Finish—Run Now, page 3-58
	View discovery run details	
Modify Schedule	Select Modify Schedule	Select the Type of CDP Discovery, page 3-55
	Modify the schedule	Specify the Schedule, page 3-56
	Specify SNMP communities	Enter SNMP Communities, page 3-56
	Specify initiating IP addresses (seeds)	Enter Initiating IP Addresses, page 3-57
	Verify your settings and finish	Verify Your Settings and Finish—Modify Schedule, page 3-58
	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 3-44](#)

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**.

You can also find details on entering community strings and the community string requirements for discovery in [Enter SNMP Community Strings for All Devices, page 3-28](#).

Step 4 Click **Next**.

Enter Initiating IP Addresses

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

Procedure

Step 1 Add seed devices by entering comma-separated IP addresses or device names 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.

Device names must resolve to your local [DNS](#) in order to translate device names to IP addresses during discovery. The requirements for entering device names are:

- Blank spaces are not allowed.
- The first character in a name must be alphanumeric.
- The only valid characters are the alphanumeric characters, the minus sign (-), and the period (.).
- The last character cannot be a minus or a period.

- 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**.
-

Verify Your Settings and Finish—Run Now

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 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 3-69](#).

Related Topics

[Viewing Discovery Logs, page 3-69](#)

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.
-

Related Topics

[Viewing Discovery Logs, page 3-69](#)

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**.

The tasks for importing devices from a file are:

Table 3-6 *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 3-59
Verify your settings and finish	Finish the Import, page 3-60
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 3-49](#).

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 3-69](#)

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 3-7 *Tasks for Import from CiscoWorks*

Task	Description
Specify the CiscoWorks server	Schedule the Import and Finish, page 3-61
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. For more information about importing devices from a CiscoWorks server, see [About Device Import From CiscoWorks, page 3-51](#).

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	The CiscoWorks server IP address.
Port	The 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	The 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. If you want 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.

Step 4 To view the status of the last import from CiscoWorks, click **Check Last Status**. Details on the latest import (if any) are shown. Click **Refresh** to update the display. You might see the following error messages:

Table 3-8 Device Import Status Messages

Message	Meaning

Related Topics

[Viewing Discovery Logs, page 3-69](#)

Setting Advanced Options

This window provides the following options for discovery and device management:

- Reverse DNS lookup—See [Enable Reverse DNS Lookup, page 3-63](#).
- Automatic management of newly discovered devices—See [Enable Auto-Management, page 3-64](#).
- Filtering for time-based access point management—See [Enable MAC Address Auto-Management Filtering for Access Points, page 3-65](#).

**Note**

Your login determines whether you can use these options.

Enable Reverse DNS Lookup

Enabling reverse DNS lookup affects hostname (device name) display on the WLSE as follows:

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.
	If the sysName is not set, the device IP address is displayed.



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

[Understanding WLSE Discovery Methods, page 3-43](#)

Enable Auto-Management

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

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 4-300](#).

- 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 3-65](#).
- Step 4** Click **Save** to save all of your settings in the Advanced Options screen.

Related Topics

- [Understanding WLSE Discovery Methods, page 3-43](#)
- [Managing and Unmanaging Devices, page 3-75](#)

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.

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

Table 3-9 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 time interval expires, newly discovered access points will not be auto-managed. Any access points that you have manually placed in the Managed folder will still be managed.

You can specify the access points to 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 3-67](#).

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:
 - a.** Remove the default * entry before beginning. Otherwise, all access points will be auto-managed regardless of the MAC addresses you enter.
 - b.** 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.
 - c.** Repeat Step b to add more addresses.
 - Step 6** To import a list of Ethernet MAC addresses from a file:
 - a.** Create an ASCII file consisting of one address per line or a comma-separated list (.txt file). For sample files, see [Example MAC Address Files, page 3-67](#).
 - b.** Enter the path to the file in the **Import From File** text box or click **Browse** to find the file.
 - c.** 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.



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 the following table.



Note Exclude rules take precedence over include rules.

Table 3-10 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 3-43](#)

Viewing Discovery Logs

This option displays details on the results of discoveries and imports.

Procedure

- Step 1** Select **Devices > Discover > DISCOVER > Logs**.
- A list of the last 15 jobs is displayed.
- Step 2** To filter the list of jobs, select All, Running, or Scheduled from the Discovery Job State list.
- Step 3** The names of the jobs indicate the type of discovery that was run, as explained in the following table:

Table 3-11 Discovery Job Names

Folder Name	Discovery Name	Discovery Type
Scheduled	CDPDiscovery	Scheduled discoveries
Run Now	CDPDiscovery_Run_Now_number	On-demand discoveries
Import	CDPDiscovery_Import_Devices_number	Imported from a file or from a CiscoWorks server
	RMEDiscovery	Imported from a CiscoWorks server ¹

1. Two items are listed in the discovery log for each import from a CiscoWorks server: CDPDiscovery_Import_Devices_number and RMEDiscovery.

- Step 4** 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 3-70](#).

If the log files show that problems occurred while running discovery, see [Diagnosing Common Discovery Problems, page 3-73](#).

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

Discovery Run Details Display

A typical, healthy discovery process 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 Inventories, page 3-79](#).

The following messages may appear in the Discovery Run Details display.

Table 3-12 Error Messages—Discovery Run Log

Message	Meaning
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 3-54 .
Device being updated	The device was previously discovered and information is being updated.
Inventory collection does not run for updated devices, run on-demand or wait for the next polling cycle	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.
New device discovered.	The device was discovered for the first time.
Inventory collection will run immediately for auto-managed devices.	Auto-management is enabled; therefore, inventory collection will run immediately for the auto-managed devices.
x.x.x.x is SNMP unreachable, unable to read CDP cache.	The community strings may be set up incorrectly. See Setting Up Devices, page 3-5 . 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. For more information on troubleshooting SNMP problems, see Diagnosing Common Discovery Problems, page 3-73 .
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.

Table 3-12 Error Messages—Discovery Run Log (continued)

Message	Meaning
x.x.x.x does not respond to ieee802.11 attributes.	<p>Make sure the SNMP community has a proper view associated.</p> <p>The IOS access point has not been configured with an IOS view. To correct this, you can configure the device manually (see Set Up IOS Access Points, page 3-8) or create a configuration job to correct it (see Managing Configuration Jobs, page 4-267). Affected devices are placed in the Misconfigured Devices system group. After the device is properly configured, you can run discovery or wait for the next scheduled discovery. After discovery, the device will be placed in the proper group(s). See Managing Device Discovery, page 3-41.</p>
IP conflict for <i>ip_address (hostname)</i> . Identifier or ethernet MAC is <i>identifier or 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 3-41.</p>
Unable to auto-manage device: x.x.x.x due to MAC filter values or time period for auto-management has expired.	<p>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-Management Filtering for Access Points, page 3-65.</p>
172.19.12.39,public,private,14,1.3.6.1.4.1.9.1.507,!{[NOVALUE]}!,...	<p>Messages similar to this are informational and show data obtained during device import from CiscoWorks:</p>

Related Topics

- [Running CDP Discovery, page 3-54](#)
- [Diagnosing Common Discovery Problems, page 3-73](#)

Diagnosing Common Discovery Problems

This section contains information on:

- [Troubleshooting SNMP Connectivity Problems, page 3-73](#)
- [Obtaining Detailed Discovery Logs, page 3-75](#)

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 8-36](#)). 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 a `-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 TAC web-site at <http://www.cisco.com/tac> for more information.

2. After IP connectivity has been confirmed, use the SNMP Connectivity Tool (see [Using Network Tools, page 8-36](#)) 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 3-31](#).

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 8-37](#)) 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 and Unmanaging Devices

Discovered devices can exist in one of two states: managed and unmanaged. By default, newly-discovered devices are in the unmanaged state and will not be polled until manually moved to the managed state.

The Manage/Unmanage window provides a view of newly discovered devices, managed devices, and unmanaged devices, allows you to manually change the management status of devices, and provides details about all devices. You can also delete devices from this window. Devices must be placed under management before you can use the WLSE to monitor and configure them.



Note There is a limitation on the number of access points and bridges that can be managed by a single Wireless LAN Solution Engine. For more information, see [Limitation on the Number of Managed Devices, page 3-78](#).

- To manually place devices under management or unmanage them, use the following procedure.
- To delete devices, see the following procedure.
- To arrange for devices to be automatically managed, see [Setting Advanced Options, page 3-63](#).
- To filter access point auto-management, see [Setting Advanced Options, page 3-63](#).



Note Your login determines whether you can use this option.

Procedure

- Step 1** Select **Devices > Discover > Managed Devices > Manage/Unmanage**. The following folders are displayed:
- Newly discovered devices (New folder).
 - Managed devices (Managed folder)
 - Unmanaged devices (Unmanaged folder).
- Step 2** To modify the status of devices in a folder:
- a. Click the folder name. You can search for devices; for information on how to search, see [Using the Device Selector and Search, page 1-9](#).
 - b. Select the devices you want to change.
 - c. To manage devices, click **Manage**. Devices will be moved into the Managed folders.
 - Only managed devices appear in WLSE displays.

- After you move devices to the managed state, an immediate inventory is run for those devices. This ensures that device attributes appear in displays, such as reports and system-defined groups without waiting for the next scheduled inventory.
- d. To unmanage devices, click **Unmanage**. Devices will be moved into the Unmanaged folder.
- e. To delete devices, click **Delete**.

Step 3 To view details about an individual device or modify its status, select the device from the device selector. You can search for devices; for information about searching, see [Using the Device Selector and Search, page 1-9](#).

- For information on the device details displayed, see [Understanding Device Details, page 3-78](#).



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

- To change a device's status:
 - To manage a device, click **Manage**.
 - To unmanage, click **Unmanage**.
 - To delete a device, click **Delete**.

Related Topics

- [Managing Device Discovery, page 3-41](#)
- [Device Name and IP Address Display, page 1-8](#)

Understanding Device Details

The details shown in the Device Details panel are:

Table 3-13 Device Details Pane

Field	Description
Device Name	Hostname, IP address, or SNMP sysname.
State	Whether the device is new, managed, or unmanaged.
Description	Detailed device description.
Version	Software version installed on the device.
Device Family	Device type.
SysName	The system name.
SysObjectId	Unique identifier that identifies the device type.
Location	Where the device is located.
IP Address	Device IP address.
Subnet	Subnet in which the device is located.
Network Segment	The network segment in which the device is located.
Contact	The person to contact for this device.
Profile	Name of the profile that contains threshold values and policy settings for fault management.

Limitation on the Number of Managed Devices

Limits on the number of managed devices are enforced according to the type of WLSE hardware you have.



Note

The following numbers are based on the number of radios in a device. Therefore, the number of managed devices must be reduced for dual-radio devices.

- The WLSE 1130 can manage 2500 access points and wireless bridges. After you have placed 2500 of these devices under management, warning messages are displayed each time you place more devices in the folder. After 2550 devices are under management, no additional devices can be placed in the Managed folder.
- The WLSE 1105 can manage 500 access points and wireless bridges. After you have placed 500 of these devices under management, warning messages are displayed each time you place more devices in the folder. After 525 devices are under management, no more devices can be placed in the Managed folder. Installing WLSE 2.0 software on a WLSE 1105 does not increase the number of devices you can manage.

**Note**

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

Managing Device Inventories

During inventory, the WLSE retrieves device attributes in order 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 3-80](#).

You can use the inventory options to:

- Run immediate or scheduled inventories of specified devices—See [Running Immediate and Scheduled Inventories, page 3-83](#).
- Reset the polling intervals for automatic inventories, job retention, and report data retention—See [Changing the Polling Intervals for Automatic Inventories, page 3-81](#).
- View details on all types of inventory jobs—See [Viewing Inventory Logs, page 3-90](#).

Related Topics

[About Inventories, page 3-80](#)

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 populate WLSE trending reports.
- Inventory polling is typically run at regular intervals, but can also be run on-demand. You can also run on-demand polling per device or per device group.
- Other polled data are processed and compared against fault, performance, and configuration policy thresholds.
- Device polling and data aggregation intervals are configurable.

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

- **Basic** inventories of all devices that 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 appear in the Scheduled folder.



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

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

In the inventory log, these inventories appear in the Periodic - All Devices folder under the name *ClientInventory*.

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

In the inventory log, these inventories appear in the Periodic - All Devices folder under the name *PerformanceInventory*.

You can reset the polling intervals for automatic inventories. See [Changing the Polling Intervals for Automatic Inventories, page 3-81](#). You can run immediate or scheduled inventories. See [Running Immediate and Scheduled Inventories, page 3-83](#).

You can run immediate and schedule inventories to run one time or at a specified interval. You select the devices for these inventories.

**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 3-82](#).

Procedure

- Step 1** Select **Devices > Discover > Inventory > Polling** option.
- 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 3-86](#)
- [Guidelines For Choosing Inventory Intervals, page 3-82](#)

Guidelines For Choosing Inventory Intervals

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

Setting Different Intervals For Different Device Groups

The scheduled inventory feature (see [Running Immediate and Scheduled Inventories, page 3-83](#)) lets you define more frequent inventory polling for a set of devices. This feature allows you to set general polling system parameters at a less frequent interval than the scheduled inventory parameters.

For example, you might decide to set the inventory intervals based on connection speeds. Suppose Site B and Site C are connected via 256 KB frame relay links back to the Site A corporate headquarters network. Assuming the headquarters network is minimally a high-speed Ethernet network, there is obviously a higher tolerance for inventory polling for Site A than for Sites B and C. So in this case, you might want to set the global inventory intervals for Sites B and C to less frequent values than those of Site A.

Setting the Recurring Interval Size

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.

Running Immediate and Scheduled Inventories

This section provides procedures for running immediate and scheduled 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.

To get started, select **Devices > Discover > Inventory**. Then refer to [Table 3-14 on page 3-83](#).


Note

Your login determines whether you can use this option.

The tasks for running inventories are:

Table 3-14 Tasks for Running Inventories

Type of Inventory	Task	Reference
All	Select inventory type.	Select Inventory Type, page 3-83
Run Now	Select devices, run inventory, and verify results.	Run Now—Select Devices and Run Inventory, page 3-84
Scheduled	Select devices.	Scheduled Inventory—Select Devices, page 3-85
	Schedule and run inventory and verify results.	Scheduled Inventory—Specify the Schedule, page 3-85

Select Inventory Type


Note

Your login determines whether you can use this option.

Procedure

Step 1 Select the inventory type:

- Run Now allows you to run an immediate inventory. You can only select one group or the individual devices in one group.

- Scheduled allows you to schedule inventory. There is also an option for scheduling repeated inventories. You can select multiple groups and individual devices from multiple groups.

Use this option to run scheduled inventories of selected devices. You can use this option when you need to inventory certain devices more frequently than the inventories provided by the automatic inventory feature.

Step 2 Click **Next**.

Related Topics

- [Managing Device Inventories, page 3-79](#)
- [Guidelines For Choosing Inventory Intervals, page 3-82](#)

Run Now—Select Devices and Run Inventory

You can 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 the on-demand inventory 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 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 and Search, page 1-9](#).
- Step 2** 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 3** Click **Run Inventory**. The inventory job starts immediately. Managed devices are polled and information is collected. WLSE displays are updated accordingly.

- Step 4** In the Tasks list, expand the Inventory folder and the Run Now folder to see the results of the inventory collection.
- Immediate inventories of selected devices are named InventoryRunNow_ *number*. The *number* increments each time you run an inventory.
- Step 5** To view details on an inventory, click the inventory name. The Run Log shows the start and end times of the inventory and the type of data that was collected for the devices you selected. For more information on inventory logs, see [Viewing Inventory Logs, page 3-90](#).
-

Scheduled Inventory—Select Devices

Procedure

- Step 1** 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 and Search, page 1-9](#).
- Step 2** Select the entire group or individual devices and click >>. The devices are moved to the Selected Devices list.
- Step 3** Repeat Steps 1 and 2 to select more devices.
- Step 4** Click **Next**.
-

Scheduled Inventory—Specify the Schedule

Procedure

- Step 1** Select a Start Date and Time. Do not schedule an inventory within 5 minutes of the current time; the first inventory might not run. Use the Run Now option instead.
- Step 2** If you want the job to repeat at regular intervals, select **Enable Repeat**. Enter an interval and select Minutes, Hours, Days, Weeks or Months.



Note The minimum interval is 30 minutes.

Step 3 Click **Finish** to schedule the inventory.

To return to the previous screen, click **Back**.

To cancel the inventory, click **Cancel**.

Step 4 In the Tasks list, expand the Inventory folder and the Scheduled folder to see the results of the inventory collection.

Step 5 To view details on an inventory, click the inventory name. The Run Log shows the start and end times of the inventory and the type of data that was collected for the devices you selected. For more information on inventory logs, see [Viewing Inventory Logs, page 3-90](#).

Related Topics

- [Guidelines For Choosing Inventory Intervals, page 3-82](#)

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.



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 3-87](#) are displayed.

Step 2 To change parameter values, select new values from the pulldown lists.

Step 3 To reset parameters to their previous values, click **Reset** *before* clicking **Apply**.

- Step 4** To save your changes, click **Apply**. To return to the System Parameters window, click **Back**.

Related Topics

[About Trending and Aggregation Data, page 3-89](#)

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 3-15 on page 3-87](#)).
- [Fault and Job Truncation Parameters](#)—Control the amount of data displayed in fault history tables and job history tables (see [Table 3-16 on page 3-88](#)).
- [Data Retention Parameters](#)—Control how long to retain the raw and aggregated data used in trend reports (see [Table 3-17 on page 3-89](#)).

For general information about polling intervals and data retention parameters and guidelines for choosing the appropriate settings, see [About Inventories, page 3-80](#).

Table 3-15 *Polling Interval Parameters*

Parameter	Description	Values
Inventory Poll Interval	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. Tip For more accurate trending, set this parameter at a lower interval than the Performance Attributes Poll Interval .	Default: 12 hours Minimum: 1 hour Maximum: 7 days

Table 3-15 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 and Scheduled Inventories, page 3-83.</p>	<p>Default: 51 minutes</p> <p>Minimum: 17 minutes</p> <p>Maximum: 7 days</p>
Performance Attributes Poll Interval	<p>Interval during which performance and utilization data are collected from the devices for the performance inventory.</p> <p>To set the aggregation period of this data, change the Raw Trend Data parameter.</p>	<p>Default: 13 minutes</p> <p>Minimum: 13 minutes</p> <p>Maximum: 7 days</p>

Table 3-16 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. This is the data shown in Configure > Jobs, Firmware > Jobs, and Reports > Scheduled Email Jobs.</p> <p>Note Recurring jobs are truncated every day to retain the last 30 runs.</p>	<p>Default: 30 days</p> <p>Minimum: 15 days</p> <p>Maximum: 60 days</p>

Table 3-17 Data Retention Parameters

Parameter	Description	Values
Raw Trend Data	How long the raw (unaggregated) trend data is retained.	Default: 2 days Minimum: 1 day Maximum: 5 days
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: 48 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 3-87](#).

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 To view a list of jobs, expand the Inventory folder. Then expand the folder that contains the type of inventory you want to see:

- The Scheduled folder contains the last 15 scheduled inventories.
- The Periodic- All Devices folder contains the last 15 performance and client inventories.
- The Run Now folder contains the last 15 immediate inventories.

In each subfolder, the latest job is listed first and earliest is listed last.

Step 3 The names of inventory jobs indicate the type of inventory that was run, as explained in the following table.

Table 3-18 Inventory Folders and Job Names

Folder Name	Inventory Name	Inventory Type
Periodic—All Devices	Inventory	Automatic inventories of all devices
	ClientInventory	Automatic inventories of client associations with access points
	PerformanceInventory	Automatic inventories of performance attributes for trend reports
Run Now	InventoryRunNow_ <i>number</i>	On-demand inventories of selected devices, run by users and generated by the radio management module.
Scheduled	ScheduledInventory	Inventories of all devices, scheduled by users

- Step 4** 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 3-91.

Related Topics

[Diagnosing Common Inventory Problems](#), page 3-92

Run Log Details—Inventory

Most inventory run log messages show the type of data collected and the devices you selected for inventory.

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 3-92](#)

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 **Administration > 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 for any task. 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 3-93.
- A comma-separated values (CSV) file—see [Exporting Devices to a CSV File](#), page 3-95.

**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 > 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 3-19 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 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 3-49](#).

Procedure

-
- Step 1** Select **Devices > Discover > Export Devices > To CSV File**.
- Step 2** Device credentials are exported to the file in plain text. For added security during the transmission of credentials, you can switch your browser to HTTPS so that HTTPS is used for the downloading the file. To switch to HTTPS, enter the following URL in the browser:
- `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 a message appears about the HTTPS certificate, follow the directions for installing the certificate.
- Step 3** Click **Download CSV File**, then click **Save**. Specify the filename and location.



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 3-97](#).

The group management window allows you to:

- Select a group and view details about it—See [Using the Group Details Window, page 3-100](#).
- Create a new static or rule-based group:
 - [Creating a Static Group, page 3-102](#)
 - [Creating a Rule-Based Group, page 3-104](#)
- Create a new group by copying an existing group:
 - [Creating a Static Group by Copying a Static or Rule-Based Group, page 3-106](#)
 - [Copying a Rule-Based Group, page 3-107](#)
- Edit a group:
 - [Editing a Static Group, page 3-109](#)
 - [Editing a Rule-Based Group, page 3-110](#)
- Delete a group—See [Deleting a Static or Rule-Based Group, page 3-111](#).

Related Topics

- [Managing Device Discovery, page 3-41](#)
- [Managing Device Inventories, page 3-79](#)

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 3-97](#).
- User-defined groups—See [User-Defined Groups, page 3-99](#).

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.

**Tip**

A complete listing of supported devices can be found on Cisco.com.

[Table 3-20](#) lists the system-defined groups, dynamic groups and subgroups.

Table 3-20 System-Defined Groups

System-Defined Groups	Contained in Folder	Subgroups
Device Type	Device Type	<ul style="list-style-type: none"> • AAA servers—LEAP, RADIUS, EAP-MD5, and PEAP groups. Groups appear and servers are added to groups after you add the servers to the WLSE (see Managing AAA Servers, page 3-37). • AP 1100, AP 1200, AP 1210 • AP 340, AP 350, AP 350-IOS <p>Note Cisco Aironet 4800 access points being managed by the WLSE will appear in the AP350 group.</p> <ul style="list-style-type: none"> • Bridge 350 • Routers • Switches
SSID	More System Groups	Contains a group for each radio service set ID (SSID) that is configured on access points. For information about configuring SSIDs on access points, see Setting Up Devices, page 3-5 .
Software Version	More System Groups	Contains a group for each software version that is installed on the devices.
Subnet	More System Groups	Contains a group for each subnet that is configured in the network.

Table 3-20 System-Defined Groups (continued)

System-Defined Groups	Contained in Folder	Subgroups
VLAN	More System Groups	<p>Contains a group for each VLAN that is configured on the access points.</p> <p>Note VLAN groups for IOS access points might not be populated if the WEP keys are not configured in each VLAN. VLAN information becomes accessible through SNMP as soon as WEP keys are configured.</p>
Wireless Domain Services (WDS)	WDS	<p>Contains WDS access points:</p> <ul style="list-style-type: none"> • Active WDS—Contains the access point that is actively providing WDS services. • Backup WDS—Contains the backup WDS access points.
Misconfigured Devices	Misconfigured Devices	<p>Contains IOS access points that do not have an ISO view configured.</p> <ul style="list-style-type: none"> • To manually correct this problem on an access point, see Set Up IOS Access Points, page 3-8. • To correct the problem by creating a configuration job, see Managing Configuration Jobs, page 4-267. <p>Note Devices that receive a dot11 mib view fault are automatically placed in this group.</p>

User-Defined Groups

You can define any number of groups, and set up hierarchies of groups which can contain subgroups and devices.



Tip

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.

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.
- 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.

Useful user-created groups in a WLAN greatly depend on the structure of the network and the application demands. [Table 3-21](#) contains examples of groups that might be worthwhile in a typical wireless LAN environment.

Table 3-21 Sample Useful 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
Department	Accounting, Marketing, Sales, Manufacturing
Operating System	non-IOS, IOS
Special Features	Proxy Mobile IP, Wireless Domain Services
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 3-22 Group Details Window Fields

Field		Description
Description		Description entered when the group was created or edited (if any)
Created by		Username of the creator of the group
Type		System Group, Static Group, or Rules-Based Group
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 summary report and links to the device's fault status and history. 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 3-23 Group Details Window Buttons

Button Name	Function	Reference
Create Static Group	Create a static group.	Creating a Static Group, page 3-102.
Create Rule-Based Group	Create a rule-based group.	Creating a Rule-Based Group, page 3-104.
Copy	Copy a static or rule-based group.	Creating a Static Group by Copying a Static or Rule-Based Group, page 3-106 Copying a Rule-Based Group, page 3-107
Copy Static	Make a static copy of a rule-based group.	Copying a Rule-Based Group, page 3-107
Edit	Edit a static or rule-based group.	Editing a Static Group, page 3-109 or Editing a Rule-Based Group, page 3-110
Delete	Delete a static or rule-based group.	Click Delete to delete the group.

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.

- Enter a description in the Description text box (optional).

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

Step 3 The new group is placed at the top (root) level or becomes a subgroup of another static group as follows:

- If another static group was selected when you created the new group, the new group becomes a subgroup of that group.
- If no static group was selected, the new group becomes a subgroup of root.

To change the subgroup designation:

- To make your new group a subgroup of any existing static group, select 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 and Search, page 1-9](#).

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 3-106](#)

[Copying a Rule-Based Group, page 3-107](#)

Creating a Rule-Based Group

To create a new rule-based group:

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.
 - (Optional) enter a description in the Description text box.



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

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

- Step 3** 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. The sysLocation <i>null</i> matches all devices that do not have this variable set.
WDS State	The WDS state of the access points in the group: <ul style="list-style-type: none"> • Active WDS—the active WDS access point. • Backup WDS—the backup WDS access point. • Candidate WDS—any other access points that are configured for WDS.
Registration State with WDS	Whether the access points in the group are registered with a WDS access point.
Device Type	Select an access point type from the list, if this group contains access points. If you select AP350, BR 350 devices will be included in the group as well.
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 4** To preview the group, click **Preview**. The rule(s) you defined and any currently managed devices that match the rule(s) are displayed.
- Step 5** To reset the window to its contents before this session, click **Reset**.
- Step 6** 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 3-107](#)

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.
- Group names can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).
- Step 4** The devices in the group you copied appear in the Devices in Group list.
- Step 5** 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 and Search, page 1-9](#).
- 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 6** To remove devices from the group, select them from the Devices in Group list and click <<.
- Step 7** 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 3-109](#)
- [Deleting a Static or Rule-Based Group, page 3-111](#)
- [About Groups, page 3-97](#)

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 3-106](#).

- 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.

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

Step 4 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. The sysLocation <i>null</i> 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. If you select AP350, BR 350 devices will be included in the group as well.
Subnet	A subnet, in decimal-dot format; for example 172.10.10.10, or 172.*.
WDS State	The WDS state of the access points in the group: <ul style="list-style-type: none"> • Active WDS—the currently active WDS access point. • Backup WDS—the backup WDS access point. • Candidate WDS—any other access points configured for WDS.
Registration State with WDS	Whether the access points in the group are registered with a WDS access point.
SSID	An SSID defined on devices.
VLAN ID	An existing VLAN configured on managed access points.

Step 5 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.
Group names can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).
 - Step 4** To make the group a subgroup of another group, select a group from the Subgroup Of list. The group you are editing will become a subgroup of the group you select.
 - 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 and Search, page 1-9](#).
 - 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 3-102](#)
- [Deleting a Static or Rule-Based Group, page 3-111](#)
- [About Groups, page 3-97](#)

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.
- Group names can be up to 64 characters in length. For information about the characters allowed in group names and descriptions, see [Naming Guidelines, page A-1](#).
- Step 4** 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. The sysLocation <i>null</i> 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. If you select AP350, BR 350 devices will be included in the group as well.

Rule Name	Data to Select or Enter
Subnet	A subnet, in decimal-dot format; for example, 172.10.10.10, or 172.*.
WDS State	The WDS state of the access points in the group: <ul style="list-style-type: none"> Active WDS—the active WDS access point. Backup WDS—the backup WDS access point. Candidate WDS—other access points configured for WDS.
Registration State with WDS	Whether the access points in the group are registered with a WDS access point.
SSID	An SSID defined on devices.
VLAN ID	The existing VLANs configured on managed access points.

- Step 5** 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 3-97](#)
- [Editing a Static Group, page 3-109](#)
- [Creating a Static Group, page 3-102](#)

