



CHAPTER 2

Using the Deployment Wizard

The Deployment Wizard enables you to configure a wireless LAN (WLAN) using the Cisco Structured Wireless-Aware Network (SWAN) framework.

Using the wizard, you can deploy your network using the Wireless Domain Services (WDS) provided by the following:

- Wireless LAN Services Modules (WLSM)
- WDS access points

About the Deployment Wizard

The Deployment Wizard replaces many of the manual configuration procedures that are normally required to configure infrastructure access points and WDS devices and to configure the WLSE to discover and manage those devices.

Specifically, the Deployment Wizard helps you configure a Wireless LAN (WLAN) using the Cisco Structured Wireless-Aware Network (SWAN) framework. (For additional information on SWAN, see the *Cisco Structured Wireless-Aware Implementation Guide* on Cisco.com.) The wizard creates basic configurations for access points (APs) that can be deployed to existing devices managed by WLSE or deployed to devices that are added later. The wizard also configures WDS devices.

Besides configuring the devices to be managed by the WLSE, the Wizard enters the necessary device credentials on the WLSE and places devices in the managed state.

Newly-installed devices require basic configuration in order to be managed by the WLSE. The basic configurations created by the Wizard can be applied only to devices that are supported by the WLSE. Configurations are downloaded to devices when the devices power up and are deployed according to criteria that you set in the Wizard.

The SWAN framework for WLANs relies on the presence of Wireless Domain Services (WDS). WDS can be supplied by access points or a Wireless LAN Services Module (WLSM).

The Wizard configures WDS devices as follows:

- WDS-WLSM—If you use a WLSM, you must manually configure some parameters on the WLSM. Details on how to configure the WLSM are displayed in the Wizard's Requirements screen. Other parameters are configured by the Wizard.
- WDS-AP—If you use access points for WDS, you can choose manual or automatic configuration.

For configuring the access points, you configure a DHCP server to upload the initial configuration provided by the WLSE to newly-installed devices. Details on how to configure DHCP are displayed in the Deployment Wizard's Requirements screen.

Finally, a RADIUS server is required. You can use a separate AAA server or configure a WDS access point as a RADIUS server.

Related Topics

[Using the Deployment Wizard, page 2-2](#)

Using the Deployment Wizard



Note

The roles and privileges assigned to your login determine whether you can use the Deployment Wizard. Select **Admin > User Admin > Manage Roles**, and make sure that both the **Wizard > WLSE Wizard** and **Configure > Auto Update** options are checked.



Note

If you do not want the wizard to launch at login, deselect the **Launch at login** checkbox. Then, when you want to launch the Wizard, click **Wizard** in the upper right corner of the screen.

The wizard steps you through the following screens:

1. **Description**—See [Description, page 2-2](#).
2. **Deployment Type**—See [Choosing the Deployment Type, page 2-3](#).
3. **Requirements**—See [Satisfying Requirements, page 2-4](#).
4. **Software**—See [Checking Software Versions, page 2-4](#).
5. **Configuration**—See [Creating the Configuration Template, page 2-4](#).
6. **WDS Setup**—See [Setting up the WDS, page 2-8](#).
7. **Deploy**—See [Deploying the Configuration, page 2-10](#).
8. **Finish**—See [Finishing, page 2-12](#).



Note

In all of the screens, click **Next** to move to the next screen, and click **Back** to modify a previous screen.

Related Topics

[About the Deployment Wizard, page 2-1](#)

Description

The Description screen displays general information about the Wizard and allows you to disable automatic launch of the Wizard after login.

Before completing a deployment using the Wizard, you will need to set up a DHCP server with boot file options that specify the IP address of the WLSE and the initial configuration file name (wlsestartup.ini). Details on DHCP requirements are explained in the Requirements screen.

When you finish going through the steps in the Wizard and install a new device in the network, the following occur:

1. The newly powered on device contacts the DHCP server to provide an IP address.
2. The device downloads the `wlsestartup.ini` file, which contains only minimal credentials and a command to Telnet to the WLSE.
3. The WLSE then discovers the device, adds it to inventory, manages it, and downloads a configuration template to it via SSH.

This template contains user-specified credentials (entered in the Wizard Configuration step), which overwrite the existing minimal credentials that were uploaded in the `wlsestartup.ini` file. The template also contains security information.

The Deployment Wizard launches right after you log in. To change this default behavior, so the Wizard does not automatically launch, deselect **Launch at Login** in this screen. To launch the Wizard, click **Wizard** in the upper right corner of any screen.

Related Topics

- [About the Deployment Wizard, page 2-1](#)
- [Using the Deployment Wizard, page 2-2](#)

Choosing the Deployment Type

Use this option to specify the type of deployment:

- **AP**—[infrastructure access points](#) with wireless domain services (WDS) provided by WDS access points (APs).

The WDS provides control path technologies that must be active on an AP in each AP subnet. For more information, see [Understanding WDS Access Points, page 11-8](#).

- **WLSM**—[infrastructure access points](#) with wireless domain services (WDS) provided by a wireless LAN service module (WLSM).

The WLSM is a module for the Cisco Catalyst 6500 series switches that provides WDS to the wireless network. For additional information, see [Understanding WLSM WDS Devices, page 11-9](#).

Procedure

-
- | | |
|---------------|---|
| Step 1 | Select either WLSM or AP , depending on the type of WDS deployment you are using. |
| Step 2 | The screen refreshes and the next screen appears. See Satisfying Requirements, page 2-4 . |
-

Related Topics

- [What is WDS and Why Do I Need It?, page 11-8](#)
- [About the Deployment Wizard, page 2-1](#)

Satisfying Requirements

The Requirements screen provides information about configuration that must be completed outside the Wizard. The displayed requirements provide all the necessary details and are based on the deployment type you chose—WDS-AP or WDS-WLSM.

For either AP or WLSM WDS, you must configure DHCP. Optionally, you can configure [AAA](#) server settings. For WLSM WDS, there are further requirements.

Click **Next** to continue. See [Checking Software Versions, page 2-4](#).

Checking Software Versions

This screen lists the minimum and recommended image versions for different device types. Devices must meet or exceed the minimum image versions in order to be deployed by the Wizard.

- Click **Import Image** to import a new image from the desktop or from Cisco.com—See [Importing Images to the WLSE, page 9-6](#).
- Click **Firmware Upgrade** to schedule a firmware upgrade for managed devices—See [Managing Firmware Jobs, page 9-11](#).
- Click **Compare Known Devices Version** to check the firmware installed on devices that have already been discovered and inventoried. A table of devices is displayed showing:
 - Devices with firmware that does not meet the minimum version (displayed in red). These devices are not supported by the Wizard.
 - Devices that meet the minimum version requirement but do not have the recommended firmware installed (displayed in yellow). These devices are supported by the Wizard.
 - Devices that have the recommended firmware (displayed in green). These devices are supported by the Wizard.

Click **Back** to return to the display of images for all devices.

Click **Next** to continue. See [Creating a General Configuration, page 2-4](#)

Creating the Configuration Template

The Wizard uses two screens to create a configuration template:

- General configuration (credentials)—see [Creating a General Configuration, page 2-4](#).
- Security configuration—see [Creating a Security Configuration, page 2-6](#).

The template created by the Wizard is saved and is listed under **Configuration > Templates** as template type WIZARD. You can use the normal WLSE configuration template features to copy, edit, and delete templates; export templates to your local drive; and import templates from a file or from devices. For more information on managing Wizard templates, see [Chapter 7, “Using Wizard Templates.”](#)

Creating a General Configuration

This option creates a general configuration (set of AP credentials) to be applied to APs and added to the WLSE’s database. You can add as many sets of credentials as you need. The credentials that you enter here are:

- Telnet or SSH username and password and enable password—Required for applying configuration templates and upgrading firmware on APs.
- SNMP community strings (SNMPv1/SNMPv2c) or SNMPv3 user authentication information—Required for discovering devices and enabling other WLSE options, such as firmware upgrades, applying configuration templates, and radio management.



Note WLSE is SNMPv2c-based.



Note You can manage access points using either SNMPv2c or SNMPv3, but not both simultaneously.

Procedure

Step 1 Complete the following:

Table 2-1 General Configuration

Field	Description
Name	Name for the configuration. Note You will use this name in the Wizard's Deploy step to assign the General Configuration to one or more access points.
Protocol	Select Telnet or SSH , and enter the following device credentials. Note Usernames and passwords must match the login sequence on the access points. For more information see Supported Telnet/SSH Login Sequences for Access Points, page 4-12 .
User Name	Telnet or SSH user name. The following characters are not supported and cannot be entered in this field: double quote, single quote, and angle brackets (< >).
Password	Telnet or SSH user password.
Password Confirm	
Enable Secret	Telnet or SSH secret password.
Enable Secret Confirm	
SNMPv2c/SNMPv1	Select SNMPv2c/SNMPv1 to manage access points using SNMPv2c/SNMPv1, and enter the following information for both Read and Write credentials. Both Read and Write community strings are required in order to enable all WLSE management functions. For more information on community strings (including characters that are not supported or not recommended), see Recommendations For Configuring SNMP Credentials, page 4-8 .
Community	The Read or Write community string.
Confirm	

Table 2-1 General Configuration (continued)

Field	Description
SNMPv3	Select SNMPv3 to manage access points using SNMPv3, and enter the following information for both Read and Write credentials. Both Read and Write community strings are required in order to enable all WLSE management functions. For more information on community strings (including characters that are not supported or not recommended), see Recommendations For Configuring SNMP Credentials, page 4-8 .
Username	The SNMPv3 Read or Write username.
Password	The Read or Write user's password.
Confirm	
Auth Algorithm	Select MD5 or SHA as the authentication algorithm for SNMPv3.

Step 2 Click **Add**. The General Configuration is added to the table at the bottom of the screen.



Note The General Configuration template name that you create with the Wizard also appears in the template listings under **Configure > Templates**.

Step 3 Repeat steps 1 and 2 to add more configurations.

Step 4 To remove a configuration, click **Delete** next to the name of the configuration in the table.

Step 5 Click **Next** to continue. See [Creating a Security Configuration, page 2-6](#).

Creating a Security Configuration

This option sets up simple security configurations. This will allow you to enter all the access points' essential settings for basic security.

Procedure

Step 1 Complete the following:

Table 2-2 Security Configuration

Field	Description
SSID Configuration	
Apply to	Select one or both of the following: <ul style="list-style-type: none"> Radio B/G/N—Select this option for radio 802.11b/g/n. Radio A/N—Select this option for radio 802.11a/n.

Table 2-2 Security Configuration (continued)

Field	Description
SSID	<p>Select one of the following:</p> <ul style="list-style-type: none"> Enter any alphanumeric, case-sensitive string, from 1 to 32 characters long. Select Broadcast SSID in Beacon to allow devices without a specified SSID to associate with this access point. Click Broadcast SSID in Beacon for additional information.
VLAN	<p>Note For AP-WDS deployments only.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> No VLAN—Use this setting if there is no VLAN. Enable VLAN ID—Use this setting to indicate there is a VLAN and enter the VLAN identification number. Native VLAN—Select if this is a Native VLAN. Bridge Group ID—Enter the bridge group identification number.
Mobility	<p>Note For WLSM-WDS deployments only.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> No Mobility Network ID—Select this if a mobility network ID is not required. Enable Mobility Network ID—Use this option to require the use of a mobility network ID, then enter the ID number.
Security	<p>Select one of the following:</p> <ul style="list-style-type: none"> No Security—Use this setting if you do not want to specify security options. Click No Security for additional information. Static WEP Key—Use this setting to specify WEP encryption. Click Static WEP Key for additional information. <ul style="list-style-type: none"> For 40-bit WEP keys, enter 10 hexadecimal digits (0-9, a-f, A-F). For 128-bit WEP keys, enter 26 hexadecimal digits (0-9, a-f, A-F). EAP Authentication—Use this setting to specify mandatory WEP, encryption open authentication + EAP, network EAP authentication, and no key management, RADIUS server authentication on port 1645. Click EAP Authentication for additional information. <ul style="list-style-type: none"> RADIUS Server—Enter the hostname or IP address of the RADIUS server you are either adding or deleting. RADIUS Server Secret—Enter the server's shared secret. Authentication Port (optional)—Enter the RADIUS server authentication port number. Accounting Port (optional)—Enter the accounting port number.

Step 2 Click **Add** to add the security configuration to the SSID table at the bottom of the screen.

Step 3 Repeat steps 1 and 2 to add more security configurations.

- Step 4** To remove a configuration, click **Delete** next to the name of the configuration you want to remove from the table.
- Step 5** Click **Next** to continue. See [Setting up the WDS, page 2-8](#).
-

Setting up the WDS

WDS must be set up for WLSE radio management features to work. There are two ways to set up the WDS: automatically and manually. For an explanation of each see: [WDS on an Access Point, page 2-8](#) and [WDS on WLSM, page 2-8](#).

WDS can be provided by either access points or a Wireless LAN Services Module (WLSM). The WDS setup for each is different:

- AP WDS Setup—See [Setting up WDS on Access Points, page 2-8](#).
- WLSM WDS Setup—See [Setting up WDS on WLSMs, page 2-9](#).

WDS on an Access Point

When an access point is discovered and inventoried:

- If the *automatic* configuration option is selected and if this is the first access point discovered in a subnet, the AP-WDS template is pushed to this access point. This access point then becomes the active WDS of the subnet, and the second and third access points discovered in the same subnet become the backup WDS devices.
- If the *manual* configuration option is selected, the MAC address of the AP is compared to the configured MAC address for the subnet. If both match, the AP-WDS template is uploaded to the access point.

If the configuration is manual but the MAC address does not match the configured WDS MAC address for the given subnet, the template, which contains the WLCCP credentials, is uploaded to the access point.

WDS on WLSM

When a WLSM is discovered and inventoried, the WLSM template is uploaded to the WLSM. When a new access point joins the network, the corresponding access point template, which contains the WLCCP credentials, is uploaded to the access point based on the subnet that it is in.

Setting up WDS on Access Points

Use this option to set up WDS on access points.

Procedure

- Step 1** To automatically configure WDS:
- a. Select **Automatic WDS Configuration**.
 - b. Click **Save**.
 - c. Click **Next** to continue. See [Deploying the Configuration, page 2-10](#).

- Step 2** To manually configure WDS:
- a. Select **Manual WDS Configuration**.
 - b. Click **Insert New Row** to add information about a WDS access point. You can enter an active and backup WDS access points for each subnet.
Complete the following:

Table 2-3 AP-WDS Setup

Field	Description
WDS MAC Address	Enter the MAC address of the WDS access point. Use this format: aaaa.bbbb.cccc
Subnet	Enter the IP address and subnet mask separated by a backslash. For example: 172.10.10.0/24
Active/Backup	Select Active or Backup to indicate if this is an active or a backup WDS.

- To add another row, click **Insert New Row**.
 - To delete a row, select it, then click **Delete**.
 - To save the setup, click **Save All**.
- c. Click **Next** to continue. See [Deploying the Configuration, page 2-10](#).

Setting up WDS on WLSMs

Use this option to set up WDS on WLSMs.

Procedure

- Step 1** If you selected WLSM in the Deployment Type screen, complete the following:

Table 2-4 WLSM WDS Configuration

Field	Description
WLSM IP	Enter the IP address of the WLSM. For example: 172.10.10.100
Subnet Details	The subnets the WLSM manages. For each subnet, enter the IP address and subnet mask separated by a backslash. For example: 172.10.10.0/24 Because each WLSM can support more than one subnet, you can enter multiple subnets.

- To add another row, click **Insert New Row**.

- To delete a row, select it, then click **Delete**.
- To save the setup, click **Save All**.

Step 2 Click **Next** to continue. See [Deploying the Configuration, page 2-10](#).

Deploying the Configuration

The Deployment Wizard automatically discovers all deployed access points, uploads configurations, and manages all access points. You can create deployment specifications which include an auto-configuration and a configuration template. The auto-configuration and the configuration template are saved and can be accessed later from the Configuration tab (**Configure > Auto Update > Automanaged Configuration** and **Configure > Templates**).

You can add as many different deployment specifications as you need.

Procedure

Step 1 Complete the following:

Table 2-5 *Deploy Configuration*

Field	Description
Enable Timer for Deploying Configurations	<p>Select to deploy this configuration during a specified time interval.</p> <p>This sets the timer for all configurations.</p> <ul style="list-style-type: none"> • This option has the same effect as enabling filtering for auto-manage devices in Devices > Discover > Discover > Advanced Options > Enable Filtering for Auto-Managed Devices. If you set Enable Timer in the Wizard, these settings will be changed correspondingly under Advanced Options. • If you set the timer under Advanced Options, the settings in the Wizard will be changed correspondingly. <p>Note If you want to enable the timer for certain MAC addresses, you can do so under Devices > Discover > Discover > Advanced Options.</p>
From/To	Specify the time period for deploying this configuration.
Assign Name to the Auto-Managed Configuration	
Name	Enter a name for the auto-configuration.

Table 2-5 *Deploy Configuration (continued)*

Field	Description
Assign matching criteria to the Auto-Managed Configuration	
Description	Enter a description for the auto-managed configuration.
Matching Criteria	
Subnet	Specify the subnets to which this configuration will be deployed by selecting a subnet, then clicking >>. <p>To remove a subnet from the list, select it and then click Remove.</p>
Update device credentials in WLSE	Select this check box to update the device credentials with the credentials defined in this template.
Save Configurations to NVRAM	Select the checkbox to save the configuration to the access points' NVRAM (IOS access points only).
Enable Device Specific Settings for this Wizard Template	Select the checkbox to enable device-specific settings in this template.
Assign Configuration to the Associated Configuration Template	
General Config	From the list, select one previously-defined general configuration to associate to the configuration template.
Security Config	From the list, select one or more previously-defined security configurations to associate to the configuration template. <p>Then click >> to add the general and security configurations to the list.</p> <p>To remove a configuration from the list, select it and click Remove.</p>

- To add the auto-managed configuration and the associated configuration template to the table at the bottom of the screen, click **Add**.

Result: The name of the auto-managed configuration and the configuration template are added to the table.
- To change an auto-managed configuration and its associated configuration template, select it, then click **Modify**.



Note The name cannot be modified; only the criteria and deployment timer can be modified.

- To remove an auto-managed configuration and its associated configuration template from the table, select it, then click **Delete**.
- To preview the configuration template, click the icon under Preview Configuration Template.

Result: The CLI commands that will be applied are displayed.

Step 2 Click **Next** to finish. See [Finishing, page 2-12](#).

Related Topics

- [Assigning an Auto-Managed Configuration, page 8-42](#)
- [Managing Device Configurations, page 8-1](#)

Finishing

After you have deployed the access points in your network:

- The devices will automatically be managed by the WLSE.
- You can use the options listed in the Finish screen to monitor access points and use other WLSE features.