Create Templates to Automate Device Configuration Changes

This chapter contains the following topics:

Why Create New Configuration Templates?

Prime Infrastructure provides a number of out-of-the-box configuration templates that you can use to make changes on your network devices. Those are described in Create a New Features and Technologies Template Using an Existing Template, on page 3.

If you have sufficient privileges, you can also create new templates that meet the exact needs of your environment, and then make those templates available for others to use. You can make the templates as simple or as complex as needed, including grouping multiple templates together into a composite template. Finally, you can associate templates with particular devices by creating configuration groups.

Prime Infrastructure provides out-of-the-box CLI commands that you can use in your templates. It also provides a blank CLI template you can use to create new CLI commands. You can use them singly or with other commands in a composite template.

How you use configuration templates can depend on factors such as how large your network is, the number of designers in your organization, and how much variation there is among devices configuration. For example:

- For a small network with only one or two designers and a limited number of device configurations, start by copying the CLI configurations you know are "good" into a set of templates. You could then combine them into composite templates and make them available to your operators.
- For a large network with many different device configurations, try to identify the configurations you can standardize. This lets you control the amount of exceptions to these standards, and lets you turn features on and off as needed.

Ways to Create Configuration Templates Using Prime Infrastructure

Cisco Prime Infrastructure provides the following types of feature-level configuration templates:

- Features and technologies templates—Configurations that are specific to a feature or technology in a device configuration.
- CLI templates—User-defined templates that are created based on your own parameters. CLI templates allow you to choose the elements in the configurations. Prime Infrastructure provides variables that you replace with actual values and logic statements. You can also import templates from the Cisco Prime LAN Management System.
- Composite templates—Two or more feature or CLI templates grouped together into one template. You specify the order in which the templates contained in the composite template are deployed to devices

Related Topics

Create a New CLI Configuration Template Using a Blank Template, on page 4
Create a New Composite Template, on page 10
Create a New Features and Technologies Template Using an Existing Template, on page 3

Create a New Features and Technologies Template Using an Existing Template

Features and Technologies templates are templates that are based on device configuration and that focus on specific features or technologies in a device's configuration.

When you add a device to Prime Infrastructure, Prime Infrastructure gathers the device configuration for the model you added. Prime Infrastructure does not support every configurable option for all device types. If Prime Infrastructure does not have a Features and Technologies template for the specific feature or parameter that you want to configure, create a CLI template.

Features and Technologies templates simplify the deployment of configuration changes. For example, you can create an SNMP Features and Technologies template and then quickly apply it to devices you specify. You can also add this SNMP template to a composite template. Then later, when you update the SNMP template, the composite template in which the SNMP template is contained automatically has your latest changes.

To create Features and Templates, follow these steps:

Step 1 Choose **Configuration > Templates > Features and Technologies**.

Step 2 In the Features and Technologies menu on the left, choose a template type to create.

Step 3 Complete the fields for that template.

If you are creating a feature template that applies only to a particular device type, the Device Type field lists only the applicable device type, and you cannot change the selection. Specifying a device type helps you to prevent a mismatch; that is, you cannot create a configuration and apply the configuration to a wrong device.

Step 4 Click **Save as New Template**. After you save the template, apply it to your devices.

Step 5 To verify the status of a template deployment, choose **Administration > Dashboard > Jobs Dashboard**.

To modify the deployment parameters for any subsequent configuration template deployments, select a configuration job, then click **Edit Schedule**.

Related Topics

Deployment Flow for Configuration Templates Using the Wizard, on page 11

Prerequisites for Creating CLI Templates

Before you create a CLI template, you must:

- Have expert knowledge and understanding of the CLI and be able to write the CLI in Apache VTL.
- Understand to what devices the CLI you create can be applied.
- Understand the data types supported by Cisco Prime Infrastructure.
- Understand and be able to manually label configurations in the template.

Create a New CLI Configuration Template Using a Blank Template

Use templates to define a set of reusable device configuration commands. A description of CLI templates and how you can use them is displayed in the web GUI when you choose **Configuration** > **Templates** > **Features & Technologies**, then choose **CLI Templates**.

If you want to edit a template that is provided with Cisco Prime Infrastructure, make a copy of the template, give it a new name, and then edit it. See Create a New CLI Configuration Template Using An Existing Template, on page 5.

Templates that you create are stored under **My Templates**.

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.

Step 2 Expand **CLI Templates**, then choose **CLI**.

Step 3 Complete the required fields in **Templates Basic** area.

Step 4 Click the **Ports** radio button, if you want to apply the template to a set of selected interfaces across selected devices The template will be tagged as port based template.

Step 5 In the **Template Detail** area, configure the following:

- Click the **Add Variable** tab. This allows you to specify a variable for which you will define a value when you apply the template. Click **Add Row** and enter the parameters for the new variable, then click Save.

  or

  Search for the global variable in the **Add Global Variable** search box by entering the first few characters of the global variable name and choose the desired global variable you want to apply

- Enter the CLI information. In the CLI tab, you must enter code using Apache VTL. See Apache Velocity Language Template Guide.
- Click **Form View** (a read-only view) to view the variables.

Step 6 Save your template. Click **Save as New Template**, specify the folder (in **My Templates**) in which you want to save the template, then click **Save**.

Related Topics

Deployment Flow for CLI Templates using the Wizard, on page 12
Data Types, on page 6
Manage Database Variables in CLI Templates, on page 7

Create a New CLI Configuration Template Using An Existing Template

The easiest way to create a new configuration template is to find a similar existing template, copy it, and edit it. You can also use this procedure to edit templates that you created. (You can only edit templates that you create.)

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.

Step 2 Expand **CLI Templates**, then choose **System Templates - CLI**.

Step 3 In the Right panel, locate the template you want to copy, hover your mouse cursor over the **i** icon that is displayed next to the template name, then click **Duplicate** in the popup window.

Step 4 In the **Duplicate Template Creation** dialog, specify a name and the folder (under **My Templates**) where you want the new template to be saved, and click **OK**.

For example, if you copy a template that resides under **CLI Templates** > **System Templates - CLI**, by default the template is saved under **My Templates** > **CLI Templates** > **System Templates - CLI (User Defined) My Templates** > **CLI Templates (User Defined)** > **System Templates - CLI (User Defined)**.

Step 5 Add the validation criteria and CLI content as described in Create a New CLI Configuration Template Using a Blank Template.

Example: Updating Passwords Using a CLI Template

The devices in these regions must have an assigned location attribute.

Step 1 If the four groups, North Region, South Region, East Region, and West Region, have not been created:

a) Choose **Inventory** > **Device Management** > **Network Devices(gear icon)** then hover your mouse cursor over **User Defined** and click **Add SubGroup**.

b) In the Create Sub-Group area, enter:

- Group Name: North Region
- Group Description: List of devices in the north region
- Filter: **Location** > **Contains** > **SJC-N**

  To determine the location of a device, choose **Inventory** > **Device Management** > **Network Devices(gear icon)** > **Columns** > **Location**.

The devices for the new group appear under **Device Work Center > User Defined > North**.

c) Do the same for south, east, and west regions.

Step 2 To deploy the password template:

a) Choose **Configuration > Templates > Features and Technologies > CLI Templates > System Templates-CLI**.

b) Select the **Enable Password-IOS** template and click **Deploy**.
c) In the Device Selection area, open the User Defined groups and select the **North Region** and **South Region** groups.
d) In the Value Selection area, enter and confirm the new enable password, then click **Apply**.
e) In the Schedule area, enter a name for the job, the date and time to apply the new template (or click Now), then click **OK**.

Step 3 After the job has run, choose **Administration** > **Dashboards** > **Job Dashboard** to view the status of the job.

Entering Variables in a Template

These topics provide information that will help you when entering variables into a template:

Data Types

Table 1 lists data types that you can configure in the Manage Variables page.

Data Type	Description
String	Enables you to create a text box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
Integer	Enables you to create a text box that accepts only numeric value. If you want to specify a range for the integer, expand the row and configure the Range From and To fields. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
DB	Enables you to specify a database type. See the Manage Database Variables in CLI Templates, on page 7.
DB_Dropdown	Enables you to list the device specific values based on DB Query. To specify value, expand the row and configure the Value field (with a comma-separated value for multiple lists which appears in the UI)
IPv4 Address	Enables you to create a text box that accepts only IPv4 addresses for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.

Drop-down	Enables you to create a list for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field (with a comma-separated value for multiple lists which appears in the UI). To specify value, expand the row and configure the Value field (with a comma-separated value for multiple lists which appears in the UI).
Check box	Enables you to create a check box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field. To specify a default value, expand the row and configure the Default Value field.
Radio Button	Enables you to create a radio button for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field. To specify a value, expand the row and configure the Value field (with a comma-separated value for multiple lists which appears in the UI).
Text Area	Enables you to create a text area which allows multiline values for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.

Manage Database Variables in CLI Templates

You can use database (DB) variables for the following reasons:

- DB variables are one of the data types in CLI templates. You can use the DB variables to generate device-specific commands.
- DB variables are predefined variables. To view the list of predefined DB variables, see the CLITemplateDbVariablesQuery.properties file at the following location: folder/opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate.
- For example, SysObjectID, IPAddress, ProductSeries, ImageVersion are DB variables.When a device is added to Prime Infrastructure, the complete details of the device is collected in the DB variables. That is, the OID of the devices is collected in SysObjectID, product series in ProductSeries, image versions of the device in ImageVersion, and so on.
- Using the data collected by the DB variables, accurate commands can be generated to the device.
- You can select the DB variable in the Type field (using the Managed Variables page). Expand the name field and fill in the default value field with any of the DB variables which you want to use.
- When a device is discovered and added to Prime Infrastructure, you can use the database values that were gathered during the inventory collection to create CLI templates.

Note While it is possible to create a customized query using Enterprise JavaBeans Query Language (EJB QL), only advanced developers should attempt this. We recommend you use the variables defined in the CLITemplateDbVariablesQuery.properties file only.

Use Validation Expressions

The values that you define in the Validation Expression are validated with the associated component value. For example, if you enter a default value and a validation expression value in the design flow, this will be validated during the design flow. That is, if the default value does not match with the entered value in the validation expression, you will encounter a get error at the design flow.

Note The validation expression value works only for the string data type field.

For example, choose **Configuration** > **Templates** > **Features and Technologies**, then choose **CLI Templates** > **CLI**. In the Template Detail area, click the **Add Variable** tab to view the list of Variables. Click the Add plus sign (+) in the Add Variables tab to add a row to the CLI template. Choose String in the Type field, enter the remaining values, and click **Save**. From the list of variables, expand the details of this new variable and configure the regular expression, which will not allow a space in that text box. Enter the following expression in the Validation Expression field.

```
^[\S]+$
```

Default value (optional)—ncs

The value should match with regular expression in the validation expression field.

Save the template, and then select a device. Try to enter a space in the text field. You will encounter a regular expression error.

Add Multi-line Commands

To enter multi-line commands in the CLI Content area, use the following syntax:

```
<MLTCMD>First Line of Multiline Command
Second Line of Multiline Command
......
......
Last Line of Multiline Command</MLTCMD>
```

where:

- <MLTCMD> and </MLTCMD> tags are case-sensitive and must be entered as uppercase.
- The multi-line commands must be inserted between the <MLTCMD> and </MLTCMD> tags.
- The tag cannot be started with a space.
- The <MLTCMD> and </MLTCMD> tags cannot be used in a single line.

Example 1:

```
<MLTCMD>banner_motd Welcome to
Cisco. You are using
Multi-line commands.
</MLTCMD>
```

Example 2:

```
<MLTCMD>banner motd ~ ${message}
</MLTCMD>
```

where {message} is a multi-line input variable.

Restrictions for Using Multi-Line Banner Commands

Prime Infrastructure does not support multi-line banner commands. You can use *banner file xyz format* as shown in the following example.

```
#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
(config)#parameter-map type webauth global
(config-params-parameter-map)# type webauth
(config-params-parameter-map)#banner file tftp://209.165.202.10/banner.txt
(config-params-parameter-map)#^Z
#more tftp://192.168.0.0/banner.txt
Disclaimer:
Usage of this wireless network is restricted to authorized users only.
Unauthorized access is strictly forbidden.
All accesses are logged and can be monitored.
#
```

Add Enable Mode Commands

Use this syntax to add enable mode commands to your CLI templates:

```
#MODE_ENABLE<<commands >>#MODE_END_ENABLE
```

Import and Export a CLI Configuration Template

These topics explain how to export and import configuration templates. Templates can be exported templates have an .xml file name; multiple templates are exported as a zip file.

- If you export multiple configuration templates, the .xml files are placed in a zip file with the prefix name **Exported Templates**.
- Single files are exported and imported as .xml files
- You can import multiple .xml files by selecting individual files or by importing a zip file.
- When you import CLI templates, the user-defined global variables that are part of the file are not imported automatically. You need to add these variables to the CLI template manually.

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.

Step 2 Expand the **CLI Templates** folder and click **System Templates**

Step 3 To export a configuration template:

a) In the Right panel, Select the template(s) that you want to export and click **Export**.

b) Save the files as the desired location.

Step 4 To import a configuration template:

a) Under the **CLI Templates** folder, hover your mouse cursor over the "i" next to **CLI**.
b) Click **Show All Templates**, then click **Import**.
c) In the **Import Templates** dialog box, choose the **My Templates** folder where you want to import the templates, then click **Select Templates** and navigate to the file you want to import.
d) Confirm your choices, then click **OK**.

Create a New Composite Template

All out-of-the-box and user-created templates can be added to a single composite template, which aggregates all of the individual feature templates that you need. When you create a composite template, you can also specify the order in which member templates should be executed. You can use composite templates to make changes to single or groups of devices.

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.

Step 2 Expand the **Composite Templates** folder and choose **Composite Templates**.

Step 3 In the **Template Basic** area, enter a name for the template.

Step 4 In the **Validation Criteria** area, choose the devices to which all of the templates contained in the composite template should apply. For example, if your composite template contains one template that applies to Cisco ASR 900 series routers and another that applies to all routers, you only need to choose **Routers** > **Cisco ASR 900 Series Aggregation Services Routers** from the Device Type list. If a device type is dimmed, the template cannot be applied on that device type.

Step 5 In the **Template Detail** area, choose the templates to include in the composite template. Using the arrows, place the templates in the in the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the interface template.

Step 6 Click **Save as New Template**. After you save the template, and apply it to your devices (see Deployment Flow for Composite Templates Using the Wizard).

Create a Shortcut to Your Templates Using Tags

When you apply a tag to a template, the template is listed under the **My Tags** folder. Tagging a configuration template helps you:

- Search a template using the tag name in the search field
- Use the tagged template as a reference to configure more devices

To tag an existing template, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.

Step 2 Expand the **My Templates** folder and choose the template that you want to tag.

Step 3 Enter a tag name in the **Tag as** text box, then click **Save**.

Deploy Templates to Devices

These topics describe the ways you can deploy (run) groups of commands on devices using configuration templates:

Create Configuration Groups for Deploying Templates to Groups of Devices

If you have devices that require the same configuration, you can create a *configuration group* that contains devices and templates that can be applied to those devices. Creating a configuration group allows you to quickly apply new templates without remembering to which devices the new templates should be deployed.

Composite templates allow you to group smaller templates together, but configuration groups specify the *relationship* between the templates and the groups of devices, and the order in which commands are executed.

Step 1 Choose **Configuration** > **Templates** > **Configuration Groups**.

Step 2 In the Configuration Group Basic area, enter a name.

Step 3 To display devices from which you can make selections, in the Template Selection area, add one or more templates by clicking **Add** and selecting the templates. This also populates the Device Type field.

Step 4 Add additional templates by clicking **Add** in the Template Selection area. You cannot choose templates that are mutually-exclusive; for example, you cannot choose Add-Host-Name-IOS and Add-Host-Name-IOS-XR.

Step 5 Select the devices on which you want to deploy the template, then click **Next** to choose the input option. You can click the **Select** toggle button to choose the devices **By Group** option.

Step 6 In the Device Selection area, select the devices you want to add to the configuration group.

Step 7 If you have multiple templates, the order in which templates will be listed by selecting one and clicking the up or down arrow.

Step 8 Click **Save as New Configuration Group**.

Deployment Flow for Configuration Templates Using the Wizard

Note This deployment flow is not applicable for Controller based templates.

Step 1 After you create a configuration template, click **Deploy**. The Deployment wizard page opens.

Step 2 Select the devices on which you want to deploy the template, then click **Next** to choose the input values.

Step 3 In the **Input Values** tab, you can toggle between the **Form** and **CLI** view.

Step 4 Enter all the mandatory fields for each template, then click **Apply**.

Step 5 After entering the necessary configuration values, click **Next** or click **CLI** to confirm the device and template configuration values.

Step 6 Schedule the deployment job using **Schedule Deployment** tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

  Failure Policy:

  - **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  - **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
  - **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
  - **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 7 Click **Next** to view the job deployment summary.

Step 8 On the **Deployment Summary** tab, you will see the CLI view for each of the device.

Step 9 Click **Finish** to deploy the template.

Step 10 Click **Job Status** in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Deployment Flow for CLI Templates using the Wizard

Step 1 After creating the CLI template, click **Deploy**. The Deployment wizard page opens.

Step 2 Select the devices on which you want to deploy the template from the **Add devices** table. The selected devices appear in the **Devices to deploy** table. You can click the **Select** toggle button to choose the devices **By Group** option.

Step 3 Click **Next** to choose the input option.

Step 4 Select the mode in which you want to deploy the template. The options are **Work Flow** and **Export/Import CSV**.

Step 5 Click the **Work Flow** option and click **Next**. See *Step 6*.

Step 6 Alternately, click **Export/Import CSV** option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.

a) Uncheck the **Do you want Optional Parameters** check box, if you want to skip the optional fields while filling the configuration values in the CSV file.
b) Click **Export CSV** to download the CSV template to your local system.
c) Enter the configuration values for each specific device in the downloaded CSV template.

d) Click **Import CSV** to upload the updated CSV file.The input values automatically gets updated.
e) Click **Next** to input values.

Step 7 In the **Input Values** tab, you can toggle between **Form** and **CLI** view. Configure the following in the Input Values tab:

a) Enter all the mandatory fields for each template, then click **Apply**.

If the validation is successful, then the border of the circle around the selected template changes to green.

Step 8 After entering the necessary configuration values, click **Next** or **CLI** to confirm the device and template configuration values.

Step 9 Schedule the deployment job using **Schedule Deployment** tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

Failure Policy:

- **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
- **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
- **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
- **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 10 Click **Next** to view the job deployment summary.

Step 11 On the **Deployment Summary** tab, you will see the CLI view for each of the device.

Step 12 Click **Finish** to deploy the template.

Step 13 Click **Job Status** in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Add Interactive Commands

An interactive command contains the input that must be entered following the execution of a command.

To enter an interactive command in the CLI Content area, use the following syntax:

```
CLI Command<IQ>interactive question 1<R>command response 1 <IQ>interactive question
2<R>command response 2
```

where <IQ> and <R> tag are case-sensitive and must be entered as uppercase.

For example:

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

Combining Interactive Enable Mode Commands

Use this syntax to combine interactive Enable Mode commands:

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

For example:

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>XXX
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

Adding Interactive Multi-line Commands

This is an example of an interactive command that contains multiple lines:

```
#INTERACTIVE
macro name EgressQoS<IQ>Enter macro<R><MLTCMD>mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
wrr-queue random-detect min-threshold 4 70 80 90 100
wrr-queue random-detect max-threshold 4 80 90 100 100
wrr-queue random-detect min-threshold 5 70 80 90 100
wrr-queue random-detect max-threshold 5 80 90 100 100
wrr-queue random-detect min-threshold 6 70 80 90 100
wrr-queue random-detect max-threshold 6 80 90 100 100
wrr-queue random-detect min-threshold 7 60 70 80 90
wrr-queue random-detect max-threshold 7 70 80 90 100
@</MLTCMD>
#ENDS_INTERACTIVE
```

Deployment Flow for Composite Templates Using the Wizard

Step 1 Choose **Configuration > Templates > Features & Technologies > Composite Templates > Composite Templates**.

Step 2 Enter the required information in the Template Basic section.

Step 3 In the Template Detail section, choose the templates to include in the composite template, and click **Save as New Template**.

Step 4 After creating the composite template, click **Deploy**. The Deployment wizard page opens.

Step 5 Select the devices on which you want to deploy the template. You can click the **Select** toggle button to choose the devices **By Group** option, then click **Next** to choose the input option.

Step 6 Select the devices on which you want to deploy the template from the **Add devices** table. The selected devices appear in the **Devices to deploy** table. .

Step 7 Select the mode in which you want to deploy the template. The options are **Work Flow** and **Export/Import CSV**.

Step 8 Click the **Work Flow** option and click **Next**. See *Step 6*.

Step 9 Alternately, click **Export/Import CSV** option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.

a) Uncheck the **Do you want Optional Parameters** check box, if you want to skip the optional fields while filling the configuration values in the CSV file.
b) Click **Export CSV** to download the CSV template to your local system.
c) Enter the configuration values for each specific device in the downloaded CSV template.
d) Click **Import CSV** to upload the updated CSV file.The input values automatically gets updated.
e) Click **Next** to input values.

Step 10 In the **Input Values** tab, you can toggle between **Form** and **CLI** view. Configure the following in the Input Values tab:

a) Select templates for a device from the navigation widget. To select templates, click the circle (T1, T2, T3, T4, T5 ...) in the upper right corner. If there are more than five templates, click three dots. The drop-down list will pop-up with all the available templates.
b) Enter all the mandatory fields for each template, then click **Apply**.

If the validation is successful, then the border of the circle around the selected template changes to green and green tick mark appears adjacent to the selected templates for the available templates in the popup.

Step 11 After entering the necessary configuration values, click **Next** or **CLI** to confirm the device and template configuration values.

Step 12 Schedule the deployment job using **Schedule Deployment** tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

  Failure Policy:

  - **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  - **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo

template deployment, “Not Attempted” message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.

- **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
- **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 13 Click **Next** to view the job deployment summary.

Step 14 On the **Deployment Summary** tab, you will see the CLI view for each of the device.

Step 15 Click **Finish** to deploy the template.

Step 16 Click **Job Status** in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Deploy Templates to Devices Without Using Configuration Groups

Once a template is saved, it can be deployed (run on) devices. You can deploy a template from the **Configuration** > **Templates** > **Features & Technologies** navigation area, or by using Configuration Groups, which is launched from **Configuration** > **Templates** > **Configuration Groups** (see Create Configuration Groups for Deploying Templates to Groups of Devices , on page 11).

To deploy a customized or system template from the **Features & Technologies** navigation area:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**

Step 2 Expand the drawer that contains the template(s) you want to deploy.

Step 3 Choose the templates you want to deploy, and click **Deploy**.

Step 4 In the **Template Deployment** window, check the settings and schedule and click **OK**.

Configure Controllers Using Configuration Templates

This section describes how to add and apply wireless templates. Templates allow you to set fields that you can then apply to multiple devices without having to reenter the common information.

The controller templates provides access to all Prime Infrastructure templates from a single page. You can add and apply controller templates, view templates, or make modifications to the existing templates. This section also includes steps for applying and deleting controller templates and creating or changing access point templates.

To access the controller templates, choose **Configuration > Templates > Features & Technologies > Features and Technologies > Controller**.

See Controller Templates and Field Descriptions.

Related Topics

Create Controller Templates, on page 17
Add Controller Templates, on page 17

Delete Controller Templates, on page 18
Apply Controller Templates, on page 18
Configure Controller WLAN Client Profiles, on page 19
Configure Controllers to Use Mobile Concierge (802.11u), on page 20
Use AP Groups to Manage WLAN Configuration and Deployment, on page 21
Create WLAN AP Groups Templates, on page 21
Configure Lightweight APs Using Configuration Templates, on page 59
Configure Location Information for Switches Using Templates, on page 46
Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates, on page 46

Create Controller Templates

To create Features and Templates, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Controller Template**.

Step 2 Hover your mouse cursor over the tool tip next to the template type and click New to create the template.

Step 3 Complete the required fields.

If you are creating a feature template that applies only to a particular device type, the Device Type field lists only the applicable device type, and you cannot change the selection. Specifying a device type helps you to prevent a mismatch; that is, you cannot create a configuration and apply the configuration to a wrong device.

Step 4 Click **Save as New Template**. After you save the template, apply it to your devices.

Step 5 To verify the status of a template deployment, choose **Administration > Dashboard > Jobs Dashboard**.

To modify the deployment parameters for any subsequent configuration template deployments, select a configuration job, then click **Edit Schedule**.

Add Controller Templates

To add a new controller template:

Step 1 Choose **Configuration > Features & Technologies > Controller**.

Step 2 Select the template you want to add.

Step 3 Enter the template name.

Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.

Step 4 Provide a description of the template.

Step 5 Click **Save**.

Related Topics

Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Delete Controller Templates

To delete a controller template:

Step 1 Choose **Configuration** > **Features & Technologies** > **My Templates**.

Step 2 Select the template(s) you want to delete, then click **Delete**.

Step 3 Click **OK** to confirm the deletion. If this template is applied to controllers, the Remove Template Confirmation page opens and lists all controllers to which this template is currently applied.

Step 4 Select the check box of each controller from which you want to remove the template.

Step 5 Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the template.

Related Topics

Add Controller Templates, on page 17
Apply Controller Templates, on page 18

Apply Controller Templates

You can apply a controller template directly to a controller or to controllers in a selected configuration group.

To apply a controller template, follow these steps:

Step 1 Choose **Configuration > Features & Technologies > Controller**.

Step 2 From the left sidebar menu, choose the category of templates to apply.

Step 3 Click the template name for the template that you want to apply to the controller.

Step 4 Click **Apply to Controllers** to open the Apply to Controllers page.

Step 5 Select the check box for each controller to which you want to apply the template.

To select all controllers, select the check box that appears at the left most corner of the controllers table.

Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

Step 6 Choose between applying the template directly to a controller or to all controllers in a selected configuration group.

To apply the template directly to a controller (or controllers), follow these steps:

a) Select the **Apply to controllers selected directly** radio button. The Apply to Controllers page lists the IP address for each available controller along with the controller name and the configuration group name (if applicable).

b) Select the check box for each controller to which you want to apply the template.

Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

To apply the template to all controllers in a selected configuration group, follow these steps:

a) Select the **Apply to controllers in the selected Config Groups** radio button. The Apply to Controllers page lists the name of each configuration group along with the mobility group name and the number of controllers included

b) Select the check box for each configuration group to which you want to apply the template.

Configuration groups which have no controllers cannot be selected to apply the templates.

Step 7 You can perform the following additional operations:

- If you select the Save Config to Flash after apply check box, the save config to Flash command is executed after the template is applied successfully.
- If you select the Reboot Controller after apply check box, the controller reboots after the template is successfully applied.

This configuration results can be viewed in the Template Results page by enabling the View Save Config / Reboot Results option.

Step 8 Click **Save**.

You can apply some templates directly from the Template List page. Select the check box(es) of the template(s) that you want to apply, choose **Apply Templates** from the Select a command drop-down list, and click **Go** to open the Apply to Controllers page. Select the check box(es) of the controllers to which you want to apply this template, and click **OK**.

Related Topics

Add Controller Templates, on page 17

Configure Controller WLAN Client Profiles

When a client tries to associate with a WLAN, it is possible to determine the client type from the information received in the process. The controller acts as the collector of the information and sends the ISE with the required data in an optimal form.

Follow these guidelines when configuring client profiling:

By default, client profiling will be disabled on all WLANs.

- Client profiling is supported on access points that are in Local mode and FlexConnect mode.
- Profiling is not supported for clients in the following scenarios:
  - Clients associating with FlexConnect mode APs in Standalone mode.
  - Clients associating with FlexConnect mode APs when local authentication is done with local switching is enabled.
- Both DHCP Proxy and DHCP Bridging mode on the controller are supported.
- Accounting Server configuration on the WLAN must be pointing at an ISE running 1.1 MnR or later releases. Cisco ACS does not support client profiling.
- The type of DHCP server used does not affect client profiling.
- If the DHCP_REQUEST packet contains a string that is found in the Profiled Devices list of the ISE, then the client will be profiled automatically.
- The client is identified based on the MAC address sent in the Accounting request packet.
- Only MAC address should be sent as calling station ID in accounting packets when profiling is enabled.
- With profiling enabled for local switching FlexConnect mode APs, only VLAN override is supported as an AAA override attribute.

To configure client profiling, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > WLANs > WLAN Configuration.**

Step 2 Click the **Advanced** tab.

Step 3 Select the **DHCP Profiling** check box to enable DHCP profiling.

Step 4 Select the **HTTP Profiling** check box to enable HTTP profiling.

HTTP client profiling is supported since controller Version 7.3.1.31.

Step 5 Click **Save**.

See the section *Controller >WLANs > WLAN Configuration > Advanced* in Cisco Prime Infrastructure Reference Guide

Configure Controllers to Use Mobile Concierge (802.11u)

Mobile Concierge is a solution that enables 802.1X capable clients to interwork with external networks. The Mobile Concierge feature provides service availability information to clients and can help them to associate available networks.

The services offered by the network can be broadly classified into two protocols:

- 802.11u MSAP
- 802.11u HotSpot 2.0

The following guidelines and limitations apply to Mobile Concierge:

- Mobile Concierge is not supported on FlexConnect Access Points.
- 802.11u configuration upload is not supported. If you perform a configuration upgrade and upload a configuration on the controller, the HotSpot configuration on the WLANs is lost.

To configure Mobile Concierge (802.11u) groups:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > WLANs > WLAN Configuration.**

Step 2 Click the **Hot Spot** tab.

Step 3 Complete the required fields on the following tabs:

- 802.11u Configuration
- Others
- Realm
- Service Advertisements
- Hotspot 2.0

Step 4 Click **Save as New Template.**

See the section *Controller > WLANs > WLAN Configuration* in Cisco Prime Infrastructure Reference Guide

Use AP Groups to Manage WLAN Configuration and Deployment

- Remember the following points when managing WLAN configurations using AP groups
- AP Groups (for controllers Release 5.2 and later) are referred to as AP Group VLANs for controllers prior to 5.2.
- To display all available WLAN profile names, delete the current WLAN profile name from the text box. When the current WLAN profile name is deleted from the text box, all available WLAN profiles appear in the drop-down list.
- Each access point is limited to 16 WLAN profiles. Each access point broadcasts all WLAN profiles unless the WLAN override feature is enabled. The WLAN override feature allows you to disable any of the 16 WLAN profiles per access point.
- The WLAN override feature applies only to older controllers that do not support the 512 WLAN feature (can support up to 512 WLAN profiles).

Related Topics

Create WLAN AP Groups Templates, on page 21
Add WLAN AP Groups, on page 22
Delete WLAN AP Groups, on page 22

Create WLAN AP Groups Templates

Site-specific VLANs or AP groups limit the broadcast domains to a minimum by segmenting a WLAN into different broadcast domains. Benefits include more effective management of load balancing and bandwidth allocation.

To configure WLAN AP Groups, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies** > **Controller** > **WLANs** > **AP Groups.**

The **WLAN** > **AP Groups** page appears, and the number of controllers and virtual domains that the template is applied to automatically populates. The last column indicates when the template was last saved.

The Applied to Controllers number is a link. Clicking the number opens an Applied to Controllers page, which displays the controller name and IP address to which that template is applied, as well as the time it was applied and its status. The Applied to Virtual Domains number is also a link. Clicking this link opens an Applied to Virtual Domains page that shows all partition names.

Step 2 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**. To modify an existing template, click the template name. The AP Groups template page appears.

This page displays a summary of the AP groups configured on your network. In this page, you can add, remove, edit, or view details of an AP group. Click in the Edit column to edit its access point(s). Select the check box in the WLAN Profile Name column, and click **Remove** to delete WLAN profiles.

The maximum characters that you can enter in the Description text box is 256.

Related Topics

Use AP Groups to Manage WLAN Configuration and Deployment, on page 21
Add WLAN AP Groups, on page 22

Delete WLAN AP Groups, on page 22

Delete WLAN AP Groups

To delete an access point group, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies.**
Choose **Controller > WLANs > AP Groups** from the left sidebar menu.

Step 2 Click **Remove**.

Related Topics

Use AP Groups to Manage WLAN Configuration and Deployment, on page 21
Add WLAN AP Groups, on page 22
Create WLAN AP Groups Templates, on page 21

Add WLAN AP Groups

You can create or modify a template for dividing the WLAN profiles into AP groups.

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > WLANs > AP Groups.**

Step 2 Choose **Add Template** from the Select a command drop-down list, and click **Go**.

Step 3 Enter a name and group description for the access point group. The group description is optional.

Step 4 If you want to add a WLAN profile, click the **WLAN Profiles** tab and configure the following fields:

a) Click **Add**.
b) Type a WLAN profile name or choose one from the WLAN Profile Name drop-down list.
c) Enter an interface/interface group or choose one from the Interface/Interface Group drop-down list.

To display all available interfaces, delete the current interface from the Interface text box. When the current interface is deleted from the Interface text box, all available interfaces appear in the drop-down list.

d) Select the **NAC Override** check box, if applicable. The NAC override feature is disabled by default.
e) Specify the policy configuration parameters by clicking the **Add/Edit** link.

- • Policy Name—Name of the policy.
  • Policy Priority—Configure policy priority between 1 and 16. No two policies can have same priority. Only 16 Policy mappings are allowed per WLAN. Selected policy template for the mapping will be applied first if it does not exist on the controller.

f) When access points and WLAN profiles are added, click **Save**.

Step 5 If you want to add a RF profile, click the **RF Profiles** tab, and configure the following fields:

- 802.11a—Drop-down list from which you can choose an RF profile for APs with 802.11a radios.
- 802.11b—Drop-down list from which you can choose an RF profile for APs with 802.11b radios.
- When RF profiles are added, click **Save**.

See the section *Controller > 802.11 > RF Profiles* in Cisco Prime Infrastructure Reference Guide

Configure FlexConnect Users in FlexConnect AP Groups

You can click the **Users configured in the group** link that appears when the FlexConnect **Local Authentication** check box is enabled to view the list of FlexConnect users. You can create FlexConnect users only after you save the FlexConnect AP Group.Maximum 100 FlexConnect users are supported in controller Release 5.2.x.x and later. If controller Release 5.2.0.0, and earlier supports only 20 FlexConnect users.

To delete a FlexConnect User, choose a user from the FlexConnect Users list, and then click **Delete**.

To configure a FlexConnect user, follow these steps:

Step 1 Choose **Configuration > Features & Technologies > Controller > FlexConnect >FlexConnect AP Groups**.

Step 2 Hover the mouse on **FlexConnect AP Groups** and select **Show All Templates**.

Step 3 Click the **Local Authentication** tab and select the **FlexConnect Local Authentication** check box to enable local authentication for this FlexConnect group.

Step 4 Click the **Users configured in the group** link. The FlexConnect Users page appears.

Step 5 If you want to add a new user, choose **Add User** from the Select a command drop-down list, and click **Go**. The **Add User** page appears.

Step 6 In the User Name text box, enter the FlexConnect username.

Step 7 In the Password text box, enter the password.

Step 8 Reenter the password in the Confirm Password text box.

Step 9 Click **Save**.

See the section *Controller > FlexConnect > FlexConnect AP Groups* in Cisco Prime Infrastructure Reference Guide.

Configure Device-Based and User-Based Controller Policies

The Policy Configuration Templates page enables you to configure the device-based policies on the controller. You can configure policies for a user or a device on the network. The maximum number of policies that you can configure is 64. Policies are not applied on WLANs and AP groups if AAA override is configured on the controller.

To configure Policy Configuration templates:

Step 1 Choose **Configuration > Templates > Features &Technologies > Controller > WLANs > Policy Configuration**.

Step 2 If you want to add a new template, choose **Add Template** from the Select a command drop-down list, and click **Go**.

Step 3 Configure the required fields.

Step 4 Click **Save as New Template**.

Configure AAA on Controllers Using Config Templates

To add a new template with general security information for a controller, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security**.

Step 2 Choose **AAA** > **General - AAA** from the left sidebar menu.

Step 3 Click New beside the template you want to add.

Step 4 Configure the following fields:

- Template Name—Template Name is the unique key used to identify the template. A template name is mandatory to distinguish between two templates that have identical key attributes.
- Maximum Local Database Entries (on next reboot)—Enter the maximum number of allowed database entries. This becomes effective on the next reboot.
- Mgmt User Re-auth Interval—Enter the termination interval for management users.

Step 5 Click **Save**.

Step 6 The template appears in the Template List page. In the Template List page, you can apply this template to controllers.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure RADIUS Authentication Servers to Control User Access to Controllers

You can add a RADIUS authentication template or make modifications to an existing template. After these server templates are configured, controller users who log into the controller through the CLI or GUI are authenticated.

See the section *Controller > Security > AAA > RADIUS Auth Servers* in Cisco Prime Infrastructure Reference Guide.

Configure RADIUS and TACACS Server Fallback Settings on Controllers

To add and configure a RADIUS TACACS Fallback template or modify an existing template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > AAA > RADIUS TACACS+ Fallback**.

Step 2 From the Radius Fallback group box, configure the following:

- From the Radius Fallback Mode drop-down list, you can choose one of the following:
  - Off—Disables fallback.
  - Passive—You must enter a time interval.
  - Active—You must enter a username and time interval.

Step 3 From the **TACACS Fallback** group box, configure the following:

- Choose either **Enable** or **Disable** from the Fallback Mode drop-down list.
- In the Time Interval text box, enter a value for TACACS Fallback test interval in seconds.

Step 4 Click **Save as New Template**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure Local EAP Timeout Settings

This page allows you to specify a timeout value for local EAP. You can then add or make changes to an existing local EAP general template.

If any RADIUS servers are configured on the controller, the controller tries to authenticate the wireless clients using the RADIUS servers first. Local EAP is attempted only if no RADIUS servers are found, either because the RADIUS servers timed out or no RADIUS servers were configured. If four RADIUS servers are configured, the controller attempts to authenticate the client with the first RADIUS server, then the second RADIUS server, and then local EAP. If the client attempts to then reauthenticate manually, the controller tries the third RADIUS server, then the fourth RADIUS server, and then local EAP.

Related Topics

Configure Authentication Order When Using LDAP and a Local Database to Control User Access to Controllers, on page 25

Configure Authentication Order When Using LDAP and a Local Database to Control User Access to Controllers

You can specify the order that LDAP and local databases use to retrieve user credential information. This page allows you to add or make modifications to an existing network user credential retrieval priority template.

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > Local EAP > Network Users Priority**.

Step 2 Use the left and right arrow keys to include or exclude network user credentials in the right page.

Step 3 Use the up and down keys to determine the order credentials are tried.

Step 4 Click **Save**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure Credentials Used for Controller User authentication (Local Network Templates)

With this template, you can store the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. For example, local EAP might use the local user database as its back end database to retrieve user credentials. This page allows you to add or make modifications to an existing local network user template. You must create a local net user and define a password when logging in as a web authentication client.

To configure a Local Network Users template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > AAA > Local Net Users**.

Step 2 Click **Import CSV** to import from a file, then click **Browse** to navigate to the file. Then continue to Step 6. If you disable the import, continue to Step 3.

Only CSV file formats are supported.

Prime Infrastructure reads data from the second row onwards. The first row in the file is treated as the header and the data is not read by Prime Infrastructure . The header can either be blank or filled.

Step 3 Enter the following details:

- Username
- Password
- Profile
- Description.

The Profile column if left blank (or filled in with **any profile**) means a client on any profile can use this account.

Step 4 Use the drop-down list to choose the SSID which this local user is applied to or choose the any SSID option.

Step 5 Enter a user-defined description of this interface.

Step 6 Click **Save**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Control How Many Concurrent Login Sessions a User Can Have

You can set the maximum number of concurrent logins that each single user can have.

To add a user login template or make modifications to an existing template, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies** > **Controller** > **Security** > **User Login Policies**.

Step 2 Enter the maximum number of concurrent logins each single user can have.

Step 3 Click **Save as New Template**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure APs to Filter on MAC Addresses

To add a MAC filter template or make modifications to an existing template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > AAA > MAC Filtering** or choose **Security > MAC Filtering**.

Step 2 Click **Import CSV** to import a file containing access point MAC addresses.

Step 3 Enter the desired file path or click Browse to import the file.

The import file must be a CSV file with MAC address, profile name, interface, and description (such as 00:11:22:33:44:55, Profile1, management, test filter). If you disable the Import from File check box, continue to step 4.

The client MAC address appears.

Step 4 Choose the profile name to which this MAC filter is applied or choose the **Any Profile** option.

Step 5 Use the drop-down list to choose from the available interface names.

Step 6 Enter a user-defined description of this interface.

Step 7 Click **Save as New Template**.

You cannot use MAC address in the broadcast range.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure AP or MSE Controller Authorization

These templates are devised for Cisco 11xx/12xx series access points converted from Cisco IOS to lightweight access points or for 1030 access points connecting in bridge mode. See the Cisco Mobility Services Engine Configuration Guide for further information.

To add a MSE authorization template or make modifications to an existing template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > AAA > AP or MSE Authorization.**

Step 2 Click **Import CSV** to import a file containing access point MAC addresses.

You can only import a CSV file. The file format parallels the fields in the GUI and therefore includes access point base radio MAC, Type, Certificate Type (MIC or SSC), and key hash (such as 00:00:00:00:00:00, AP, SSC, xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx). No other file formats are not supported.

Step 3 Enter the desired file path or click **Browse** to import the file.

Step 4 Click **Save As New Template**.

You cannot use MAC address in the broadcast range.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure Controllers to Manually Disable Clients By MAC Address

This page allows you to add a manually disable client template or make modifications to an existing disabled client template.

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > Manually Disable Clients**.

Step 2 Enter the MAC address of the client you want to disable.

Step 3 Enter a description of the client you are setting to disabled.

Step 4 Click **Save as New Template**.

You cannot use a MAC address in the broadcast range.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure Controllers' Client Exclusion Policies

To add a client exclusion policies template or modify an existing client exclusion policies template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > Client Exclusion Policies**.

Step 2 Complete the following fields:

- **Template Name**—Enter a name for the client exclusion policy.
- **Excessive 802.11 Association Failures**—Enable to exclude clients with excessive 802.11 association failures.
- **Excessive 802.11 Authentication Failures**—Enable to exclude clients with excessive 802.11 authentication failures.
- **Excessive 802.1X Authentication Failures**—Enable to exclude clients with excessive 802.1X authentication failures.
- **Excessive 802.11 Web Authentication Failures**—Enable to exclude clients with excessive 802.11 web authentication failures.
- **IP Theft or Reuse**—Enable to exclude clients exhibiting IP theft or reuse symptoms.

Step 3 Click **Save as New Template**

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure AP Authentication Using MFP

Management Frame Protection (MFP) provides for the authentication of 802.11 management frames by the wireless network infrastructure. Management frames can be protected to detect adversaries who are invoking denial of service attacks, flooding the network with associations and probes, interjecting as rogue access points, and affecting the network performance by attacking the QoS and radio measurement frames.

When enabled, the access point protects the management frames it transmits by adding a message integrity check information element (MIC IE) to each frame. Any attempt to copy, alter, or replay the frame invalidates the MIC, causing any receiving access point configured to detect MFP frames to report the discrepancy. An access point must be a member of a WDS to transmit MFP frames.

When MFP detection is enabled, the access point validates every management frame that it receives from other access points in the network. It ensures that the MIC IE is present (when the originator is configured to transmit MFP frames) and matches the content of the management frame. If it receives any frame that does not contain a valid MIC IE from a BSSID belonging to an access point that is configured to transmit MFP frames, it reports the discrepancy to the network management system.

To add or make modifications for the access point authentication and management frame protection (MFP) template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > AP Authentication and MFP**.

Step 2 From the Protection Type drop-down list, choose one of the following authentication policies:

- **None**—No access point authentication policy.
- **AP Authentication**—Apply authentication policy.
- **MFP**—Apply management frame protection.

Alarm trigger threshold appears only when AP authentication is selected as a protection type. Set the number of hits from an alien access point to ignore before raising an alarm.

The valid range is from 1 to 255. The default value is 255.

Step 3 Click **Save as New Template**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure the Web Auth Authentication Type for a Controller WLAN

With web authentication, guests are automatically redirected to a web authentication page when they launch their browsers. Guests gain access to the WLAN through this web portal. Wireless LAN administrators using this authentication mechanism should have the option of providing unencrypted or encrypted guest access. Guest users can then log into the wireless network using a valid username and password, which is encrypted with SSL. Web authentication accounts might be created locally or managed by a RADIUS server. The Cisco Wireless LAN controllers can be configured to support a web authentication client. You can use this template to replace the Web authentication page provided on the controller.

To add or make modifications to an existing web authentication template, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies** > **Security** > **AAA** > **Web Auth Configuration**.

Step 2 Choose one of the following web authentication type from the drop-down list.

- **default internal**— You can still alter the page title, message, and redirect URL, as well as whether the logo appears. Continue to Step 5.
- **customized web authentication**—Click **Save** and apply this template to the controller. You are prompted to download the web authentication bundle.
- Before you can choose customized web authentication, you must first download the bundle by going to **Config** > **Controller** and choose **Download Customized Web Authentication** from the **Select a command** drop-down list, and click **Go**.
- **external**—you need to enter the URL you want to redirect to after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user is directed to the company home page

Step 3 Select the **Logo Display** check box if you want your company logo displayed.

Step 4 Enter the title you want displayed on the Web Authentication page.

Step 5 Enter the message you want displayed on the Web Authentication page.

Step 6 Provide the URL where the user is redirected after a successful authentication. For example, if the value entered for this text box is http://www.example.com, the user would be directed to the company home page.

Step 7 Click **Save as New Template**.

Related Topics

Download Customized Web Authentication Pages to Controllers, on page 30

Download Customized Web Authentication Pages to Controllers

Before You Begin, follow these steps:

You can download a customized Web Authentication page to the controller. With a customized web page, you can establish a username and password for user web access.

When downloading customized web authentication, you must follow these strict guidelines:

- Provide a username.
- Provide a password.
- Retain a redirect URL as a hidden input item after extracting from the original URL.
- Extract the action URL and set aside from the original URL.

Include scripts to decode the return status code.

Step 1 Download the sample login.html bundle file from the server. The following figure displays .html file. The login page is presented to web users the first time they access the WLAN if web authentication is turned on.

Figure 1: Login.html

Step 2 Edit the login.html file and save it as a .tar or .zip file.

You can change the text of the Submit button to read Accept terms and conditions and Submit.

Step 3 Make sure you have a Trivial File Transfer Protocol (TFTP) server available for the download. Keep these guidelines in mind when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable. However, if you want to put the TFTP server on a different network while the management port is down, add a static route if the subnet where the service port resides has a gateway (config route add *IP address of TFTP server*).
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as Prime Infrastructure because the built-in TFTP server of Prime Infrastructure and third-party TFTP server use the same communication port.

Step 4 Download the .tar or .zip file to the controller(s).

The controller allows you to download up to 1 MB of a .tar file containing the pages and image files required for the Web authentication display. The 1 MB limit includes the total size of uncompressed files in the bundle.

You can now continue with the download.

Step 5 Copy the file to the default directory on your TFTP server.

Step 6 Choose **Configuration > Network > Network Devices > Wireless Controller**.

Step 7 Click on a Device Name. If you select more than one device, the customized Web authentication page is downloaded to multiple controllers.

Step 8 From the left sidebar menu, choose **System > Commands**.

Step 9 From the Upload/Download Commands drop-down list, choose **Download Customized Web Auth,** and click **Go**.

Step 10 The IP address of the controller to receive the bundle and the current status are displayed.

Step 11 Choose **local machine** from the File is Located On field. If you know the filename and path relative to the root directory of the server, you can also select TFTP server.

For a local machine download, either .zip or .tar file options exists, but Prime Infrastructure does the conversion of .zip to .tar automatically. If you chose a TFTP server download, only .tar files would be specified.

Step 12 Enter the maximum number of times the controller should attempt to download the file in the Maximum Retries field.

Step 13 Enter the maximum amount of time in seconds before the controller times out while attempting to download the file in the Timeout field.

Step 14 The files are uploaded to the c:\tftp directory. Specify the local filename in that directory or click **Browse** to navigate to it.

Step 15 Click **OK**.

If the transfer times out, you can simply choose the TFTP server option in the File Is Located On field, and the server filename is populated for you. The local machine option initiates a two-step operation. First, the local file is copied from the workstation of the administrator to the built-in TFTP server of Prime Infrastructure . Then the controller retrieves that file. For later operations, the file is already in the TFTP directory of Prime Infrastructure server, and the download web page now automatically populates the filename.

Step 16 Click the **Click here to download a sample tar file** link to get an option to open or save the login.tar file.

Step 17 After completing the download, you are directed to the new page and able to authenticate.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18
Configure the Web Auth Authentication Type for a Controller WLAN, on page 30

Configure External Web Authorization Servers for Controllers

To create or modify an External Web Auth Server template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > External Web Auth Server** or choose **Security > External Web Auth Server**.

Step 2 Enter the server address of the external web auth server.

Step 3 Click **Save as New Template**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure Password Policies for Controllers

To add or make modifications to an existing password policy template, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies** > **Controller** > **Security** > **Password Policy**.

Step 2 You can enable or disable the following settings:

- Password must contain characters from at least 3 different classes such as uppercase letters, lowercase letters, digits, and special characters.
- No character can be repeated more than 3 times consecutively.
- Password cannot be the default words like cisco or admin.
- Password cannot be “cisco”, “ocsic”, “admin”, “nimda’ or any variant obtained by changing the capitalization of letters, or by substituting ‘1” “|” or “!” for i, or substituting “0” for “o”, or substituting “$” for “s”.
- Password cannot contain username or reverse of username.

Step 3 Click **Save**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Apply Controller Templates

You can apply a controller template directly to a controller or to controllers in a selected configuration group.

To apply a controller template, follow these steps:

Step 1 Choose **Configuration > Features & Technologies > Controller**.

Step 2 From the left sidebar menu, choose the category of templates to apply.

Step 3 Click the template name for the template that you want to apply to the controller.

Step 4 Click **Apply to Controllers** to open the Apply to Controllers page.

Step 5 Select the check box for each controller to which you want to apply the template.

To select all controllers, select the check box that appears at the left most corner of the controllers table.

Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

Step 6 Choose between applying the template directly to a controller or to all controllers in a selected configuration group.

To apply the template directly to a controller (or controllers), follow these steps:

a) Select the **Apply to controllers selected directly** radio button. The Apply to Controllers page lists the IP address for each available controller along with the controller name and the configuration group name (if applicable).

b) Select the check box for each controller to which you want to apply the template.

Select the **Ignore errors on Apply template to Controllers** check box to ignore errors and apply all commands in the template to the controller. If this check box is not selected, any errors encountered while applying a command in the template to a controller causes the rest of the commands to be not applied.

To apply the template to all controllers in a selected configuration group, follow these steps:

a) Select the **Apply to controllers in the selected Config Groups** radio button. The Apply to Controllers page lists the name of each configuration group along with the mobility group name and the number of controllers included

b) Select the check box for each configuration group to which you want to apply the template.

Configuration groups which have no controllers cannot be selected to apply the templates.

Step 7 You can perform the following additional operations:

- If you select the Save Config to Flash after apply check box, the save config to Flash command is executed after the template is applied successfully.
- If you select the Reboot Controller after apply check box, the controller reboots after the template is successfully applied.

This configuration results can be viewed in the Template Results page by enabling the View Save Config / Reboot Results option.

Step 8 Click **Save**.

You can apply some templates directly from the Template List page. Select the check box(es) of the template(s) that you want to apply, choose **Apply Templates** from the Select a command drop-down list, and click **Go** to open the Apply to Controllers page. Select the check box(es) of the controllers to which you want to apply this template, and click **OK**.

Related Topics

Add Controller Templates, on page 17

Configure Controller Access Control List

An access control list (ACL) is a set of rules used to limit access to a particular interface (for example, if you want to restrict a wireless client from pinging the management interface of the controller). ACLs can be applied to data traffic to and from wireless clients or to all traffic destined for the controller Central Processing Unit (CPU) and can now support reusable grouped IP addresses and reusable protocols. After ACLs are configured in the template, they can be applied to the management interface, the AP-manager interface, or any of the dynamic interfaces for client data traffic; to the Network Processing Unit (NPU) interface for traffic to the controller CPU; or to a WAN.

You can create or modify an ACL template by protocol, direction, and the source or destination of the traffic.

You can now create new mappings from the defined IP address groups and protocol groups. You can also automatically generate rules from the rule mappings you created. These rules are generated with contiguous sequence. That is, if rules 1 through 4 are already defined and you add up to 29 rules.

Existing ACL templates are duplicated into a new ACL template. This duplication clones all the ACL rules and mappings defined in the source ACL template.

This release of Prime Infrastructure provides support to IPv6 ACLs.

To add or modify an existing ACL template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > Access Control Lists**.

Step 2 Complete the following fields:

- Access Control List Name—User-defined name of the template.
- ACL Type—Choose either **IPv4** or **IPv6**. IPv6 ACL is supported from controller Release 7.2.x.

Step 3 Choose **IP Groups** from the left sidebar menu to create reusable grouped IP addresses and protocols.

Step 4 Choose **Add IP Group** from the **Select a command** drop-down list and click **Go** to define a new IP address group.

One IP address group can have a maximum of 128 IP address and netmask combinations. To view or modify an existing IP address group, click the URL of the IP address group. The IP address group page opens.For the IP address of any, an any group is predefined.

Step 5 Edit the following current IP group fields if required in the ACL IP Groups details page:

- IP Group Name
- IP Address
- Netmask OR CIDR Notation
- Enter the Netmask or CIDR Notation and then click **Add**. The list of IP addresses or Netmasks appears in the List of IP Address/Netmasks text box.
- CIDR or Classless InterDomain Routing a protocol which allows the assignment of Class C IP addresses in multiple contiguous blocks. CIDR notation allows you to add a large number of clients that exist in a subnet range by configuring a single client object.
- Netmask allows you to set the subnet mask in dotted-decimal notation rather than the CIDR notation for the IP address property.
- BroadCast/Network
- List of IP Addresses/Netmasks
- Use the Move Up and Move Down buttons to rearrange the order of the list items. Use the Delete button to delete any IP address or Netmask.

Step 6 Choose **Access Control > Protocol Groups** from the left sidebar menu to define an additional protocol that is not a standard predefined one.

The protocol groups with their source and destination port and DSCP are displayed.

Step 7 Choose **Add Protocol Group** from the **Select a command** drop-down list, and click **Go** to create a new protocol group. To view or modify an existing protocol group, click the URL of the group.

The Protocol Groups page appears.

Step 8 Enter a name for a new rule. ACLs are not required to have rules defined. When a packet matches all the parameters of a rule, the action for this rule is exercised.

Step 9 Choose one of the following protocols from the drop-down list:

- Any—All protocols
- TCP—Transmission Control Protocol
- UDP—User Datagram Protocol
- ICMP—Internet Control Message Protocol
- ESP—IP Encapsulating Security Payload
- AH—Authentication Header
- GRE—Generic Routing Encapsulation
- IP—Internet Protocol
- Eth Over IP—Ethernet over Internet Protocol
- Other Port OSPF—Open Shortest Path First
- Other—Any other IANA protocol (http://www.iana.org/)

Some protocol choices (such as TCP or UDP) cause additional Source Port and Dest Port GUI elements to appear.

- Source Port—Specify the source of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.

- Dest Port—Specify the destination of the packets to which this ACL applies. The choices are Any, HTTP, HTTPS, Telnet, RADIUS, DHCP Server, DHCP Client, DNS, L2TP, PPTP control, FTP control, SMTP, SNMP, LDAP, Kerberos, NetBIOS NS, NetBIOS DS, NetBIOS SS, MS Dir Server, Other, and Port Range.

Step 10 Choose **any** or **specific** from the DSCP (Differentiated Services Code Point) drop-down list. If you choose specific, enter the DSCP (range of 0 to 255).

DSCP is a packet header code that can be used to define the quality of service across the Internet.

Step 11 Click **Save**.

Step 12 Choose the ACL template to which you want to map the new groups to define a new mapping. All ACL mappings appear on the top of the page, and all ACL rules appear on the bottom.

Step 13 Choose **Add Rule Mappings** from the **Select a command** drop-down list. The Add Rule Mapping page appears.

Step 14 Configure the following fields:

- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.
- Direction—Any, Inbound (from client) or Outbound (to client).
- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 15 Click **Add**. The new mappings populate the bottom table.

Step 16 Click **Save**.

Step 17 Choose the mappings for which you want to generate rules, and click **Generate**. This automatically creates the rules.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure FlexConnect Access Control List to Control Traffic on Controllers

You can create or modify a FlexConnect ACL template for configuring the type of traffic that is allowed by protocol, and the source or destination of the traffic. The FlexConnect ACLs do not support IPv6 addresses.

To configure and apply an Access Control List template to a Controller, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies** > **Controller** > **Security** > **FlexConnect ACLs**.

Step 2 Enter a name for the new FlexConnect ACL.

Step 3 Click **Save as New Template**.

A FlexConnect ACL template is created. You can now create new mappings from the defined IP address groups and protocol groups. To define a new mapping, choose the ACL template to which you want to map the new groups. All FlexConnect ACL mappings appear on the top of the page, and all FlexConnect ACL rules appear in the bottom.

Step 4 Click **Add Rule Mappings**, then configure the following fields in the FlexConnect ACL IP Protocol Map page:

- Source IP Group—Predefined groups for IPv4 and IPv6.
- Destination IP Group—Predefined groups for IPv4 and IPv6.
- Protocol Group—Protocol group to use for the ACL.

- Action—Deny or Permit. The default filter is to deny all access unless a rule explicitly permits it.

Step 5 Click **Add**. The new mappings populate the bottom table.

Step 6 Click **Save**.

Step 7 Choose the mappings for which you want to generate rules, and click **Generate**. This automatically creates the rules.

Step 8 From the **Select a command** drop-down list in the FlexConnect ACL page, choose **Apply Templates**.

The Apply to Controllers page appears.

Step 9 Select **Save Config to Flash after apply** check box to save the configuration to Flash after applying the FlexConnect ACL to the controller.

Step 10 Select **Reboot Controller after apply** to reboot the controller once the FlexConnect ACL is applied. This check box is available only when you select the Save Config to Flash after apply check box.

Step 11 Select one or more controllers and click **OK** to apply the FlexConnect ACL template.

The FlexConnect ACL that you created appears in **Configure** > **Controller Template Launch Pad** > **IP Address** > **Security** > **Access Control** > **FlexConnect ACLs**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure Access Control List Traffic Control Between the Controller CPU and NPU

CPU ACL configuration with IPv6 is not supported in this release because all IP addresses of controllers on interfaces use IPv4 except the virtual interface. The existing ACLs are used to set traffic controls between the Central Processing Unit (CPU) and Network Processing Unit (NPU).

To add or modify an existing CPU ACL template, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > CPU Access Control List**.

Step 2 Select the check box to enable CPU ACL. When CPU ACL is enabled and applied on the controller, Prime Infrastructure displays the details of the CPU ACL against that controller.

Step 3 From the **ACL Name** drop-down list, choose a name from the list of defined names.

Step 4 From the **CPU ACL Mode** drop-down list, choose which data traffic direction this CPU ACL list controls. The choices are the wired side of the data traffic, the wireless side of the data traffic, or both wired and wireless.

Step 5 Click **Save as New Template**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure Rogue AP and Client Security Policies on Controllers

Rogue templates enable you to configure the rogue policy (for access points and clients) applied to the controller. It also determines whether or not the Rogue Location Discovery Protocol (RLDP) is connected to the enterprise wired network.With RLDP, the controller instructs a managed access point to associate with the rogue access point and sends a special packet to the controller. If the controller receives the packet, the rogue access point is connected to the enterprise network. This method works for rogue access points that do not have encryption enabled.

There can be many rogues with very weak RSSI values that do not provide any valuable information in the rogue analysis. Therefore, you can use this option to filter the rogues by specifying the minimum RSSI value at which the APs should detect rogues.

Rogue access point rules allow you to define rules to automatically classify rogue access points. Cisco Prime Infrastructure applies the rogue access point classification rules to the controllers. These rules can limit the appearance of a rogue on maps based on RSSI level (weaker rogue access points are ignored) and time limit (a rogue access point is not flagged unless it is seen for the indicated period of time). Rogue access point rules also help reduce false alarms.

The new enhancements to the role classification rule are applicable for Cisco WLC 7.4 and later. These enhancements are not applicable to Catalyst 3850, Catalyst 3650, Catalyst 4500 switches, and Cisco 5760 WLAN Controllers (WLC).

To view current classification rule templates, rule type, and the number of controllers to which they are applied, choose **Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > Rogue AP Rules**.

Rogue classes include the following types:

- Malicious Rogue—A detected access point that matches the user-defined malicious rules or has been manually moved from the Friendly AP category.
- Friendly Rogue—Known, acknowledged, or trusted access point or a detected access point that matches user-defined friendly rules.
- Unclassified Rogue—A detected access point that does not match the malicious or friendly rules.

See Combine Multiple Controller Rogue AP Rules in Rogue AP Rule Groups and the following topics in Cisco Prime Infrastructure Reference Guide for more information.

- Controller > Security > Wireless Protection Policies > Rogue Policies
- Controller > Security > Wireless Protection Policies > Rogue AP Rules
- Controller > Security > Wireless Protection Policies > Ignored Rogue AP

Define Controller Rogue AP Classification Rules

To configure rogue rules on Cisco Prime Infrastructure, follow these steps:

1. Create a Rogue AP rule
2. Create a Rogue AP Rule Group that contains all the rules you want to apply
3. Deploy the Rogue AP Rule Group to the controllers

See the section *Controller > Security > Wireless Protection Policies > Rogue AP Rules* in Cisco Prime Infrastructure Reference Guide.

Related Topics

- Combine Multiple Controller Rogue AP Rules in Rogue AP Rule Groups

Combine Multiple Controller Rogue AP Rules in Rogue AP Rule Groups

A rogue access point rule group template allows you to combine more than one rogue access point rule to controllers. To view current rogue access point rule group templates or create a new rule group, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Security > Wireless Protection Policies > Rogue AP Rule Groups**.

Step 2 Enter a template name.

Step 3 To add a Rogue AP rule, click to highlight the rule in the left column. Click **Add** to move the rule to the right column.

Rogue access point rules can be added from the Rogue Access Point Rules section.

Step 4 To remove a rogue access point rule, click to highlight the rule in the right column. Click **Remove** to move the rule to the left column.

Step 5 Use the **Move Up/Move Down** buttons to specify the order in which the rules apply. Highlight the desired rule and click **Move Up** or **Move Down** to move it higher or lower in the current list.

Step 6 Click **Save** to confirm the rogue access point rule list.

Step 7 Click **Deploy** to apply the rule group to the controller.

See View Deployed Rogue AP Rules and the section *Controller > Security > Wireless Protection Policies > Rogue AP Rules* in Cisco Prime Infrastructure Reference Guide.

View Deployed Rogue AP Rules

You can view and edit the Rogue AP Rules that you previously deployed.

Step 1 Choose **Monitor > Network > Network Devices > Wireless Controllers**.

Step 2 Click on a Device Name, then select **Security > Wireless Protection Policies > Rogue AP Rules**.

Step 3 Click on a Rogue AP Rule name to edit the rule.

Step 4 To view Rogue AP alarms, click the Alarm Summary at the top right of the page, then select **Rogue AP**. You can also choose **Dashboard > Wireless > Security** to view Rogue AP information.

Configure SIP Snooping for Controllers

Keep the following guidelines in mind when using SIP Snooping:

- SIPs are available only on the Cisco 5500 Series Controllers and on the 1240, 1130, and 11n access points.

- SIP CAC should only be used for phones that support status code 17 and do not support TSPEC-based admission control.
- SIP CAC will be supported only if SIP snooping is enabled.

To configure SIP Snooping for a controller, follow these steps:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > 802.11 > SIP Snooping**.

Step 2 Configure the following fields:

- **Port Start**
- **Port End**

If single port is to be used, configure both start and end port fields with same number.

Step 3 Click **Save as New Template**.

See the following section in Cisco Prime Infrastructure Reference Guide

- Controller > 802.11 > Load Balancing
- Controller > 802.11 > Band Select
- Controller > 802.11 > Preferred Call
- Controller > 802.11 RF Profiles

Create Management Templates

You can create or modify the templates for the following management parameters of the controllers.

- Trap Receivers
- Trap Control
- Telnet and SSH
- Multiple Syslog servers
- Local Management Users
- Authentication Priority

See Configure a Controller's Management Parameters, for more information.

Use Microsoft LyncSDN With Cisco Prime Infrastructure

LyncSDN configuration is not supported on Virtual and Cisco 2500 Series and Virtual Controllers.

You can create these LyncSDN templates:

- LyncSDN Global Config feature templates
- LyncSDN PolicyFeature templates
- LyncSDN ProfileFeature templates

Related Topics

Configure Controllers to Use Microsoft LyncSDN Diagnostics, on page 41

Configure Controllers to Use Microsoft LyncSDN Policies to Monitor Network Traffic QoS, on page 41
Configure Controllers to Use Microsoft LyncSDN WLAN Profiles , on page 42

Configure Controllers to Use Microsoft LyncSDN Diagnostics

To create parameters to apply to devices using the LyncSDN Global Config feature, follow these steps:

Step 1 Choose **Configuration** > **Features & Technologies** > **Controller** > **LyncSDN** > **LyncSDN Global Config**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.

Step 4 In the Template Detail area, configure the following information:

- Select the LyncServer checkbox to enable or disable the LYNC application on the Prime Infrastructure.
- Enter the port number.
- You can configure support for HTTP/HTTPS communication on Prime Infrastructure for LYNC server. Prime Infrastructure supports only http. For https certificate, you need to provide and approved at Lync server which takes once Lync service is ready from Prime Infrastructure.

Step 5 When you are finished, click **Save as Template**.

Related Topics

Configure Controllers to Use Microsoft LyncSDN Policies to Monitor Network Traffic QoS, on page 41
Configure Controllers to Use Microsoft LyncSDN WLAN Profiles , on page 42

Configure Controllers to Use Microsoft LyncSDN Policies to Monitor Network Traffic QoS

To create parameters to apply to devices using the LyncSDN Policy feature, follow these steps:

Step 1 Choose **Configuration > Features & Technologies > Controller** > **LyncSDN** > **LyncSDN Policy**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.

Step 4 In the Template Detail area, configure the following information:

- Choose the policy of audio lync call on WLAN from the Audio drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.
- Choose the policy of video lync call on WLAN from the Video drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.
- Choose the policy of desktop-share lync call on WLAN from the Application-Sharing drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.
- Choose the policy of file transfer lync call on WLAN from the File-Transfer drop-down list. The possible policy types are Silver, Gold, Platinum, or Bronze.

Step 5 When you are finished, click **Save as Template**.

Related Topics

Configure Controllers to Use Microsoft LyncSDN Diagnostics, on page 41
Configure Controllers to Use Microsoft LyncSDN WLAN Profiles , on page 42

Configure Controllers to Use Microsoft LyncSDN WLAN Profiles

To create parameters to apply to devices using the LyncSDN Profile feature, follow these steps:

Step 1 Choose **Configuration > Features & Technologies > Controller** > **LyncSDN** > **LyncSDN Policy**.

Step 2 In the Template Basic area, enter a name, description, and tag for your template in the appropriate text boxes.

Step 3 In the Validation Criteria area, choose a Device Type from the drop-down list and enter the OS Version.

Step 4 In the Template Detail area, click the Wlan Profile check box and select a policy from the LyncSDN Policy drop-down list.

Step 5 When you are finished, click **Save as Template**.

Related Topics

Configure Controllers to Use Microsoft LyncSDN Diagnostics, on page 41
Configure Controllers to Use Microsoft LyncSDN Policies to Monitor Network Traffic QoS, on page 41

Configure AVC Profiles for Application Classification on Controllers

Application Visibility and Control (AVC) uses the Network Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1400 Layer 4 to Layer 7 protocols. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link usage, and infrastructure upgrades.

AVC is supported only on the following controllers:

- Cisco 2500 and 5500 Series Controllers.
- WiSM 2 Controllers
- Cisco Flex 7500 and Cisco 8500 Series Controllers.

To configure the AVC profile template, follow these steps:

Step 1 Choose **Configuration > Features & Technologies > Controller** > **Application Visibility And Control > AVC Profiles**.

Step 2 If you want to add a new template, hover the mouse on **AVC Profiles** and select **New** or click **AVC Profiles**. To modify an existing template, click the template name.

Step 3 In the **AVC Profile Name** text box, enter the AVC Profile Name.

Note You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application. This allows you to configure up to 32 application actions per WLAN. You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs.

Step 4 Under the AVC Rule List, click **Add Row** to create AVC rules.

- In the **Application Name** field, enter the name of the application.

- In the **Application Group Name** field, enter the name of the application group to which the application belongs.
- From the **Action** drop-down list, choose one of the following:
  - Drop—Drops the upstream and downstream packets corresponding to the chosen application.
  - Mark— Marks the upstream and downstream packets corresponding to the chosen application with the DSCP value that you specify in the Differentiated Services Code Point (DSCP) drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.
  - Rate Limit—If you select Rate Limit as an action, you can specify Average Rate Limit per client and Burst data rate limit. The number of rate limit applications is limited to 3.

The default action is to permit all applications.

- If you select **Mark** as an action, then choose QoS levels from the **DSCP** drop-down list. DSCP is a Packet header code that is used to define quality of service across the Internet. The DSCP values are mapped to the following QoS levels:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.
  - Gold (Video)—Supports the high-quality video applications.
  - Silver (Best Effort)—Supports the normal bandwidth for clients.
  - Bronze (Background)— Provides lowest bandwidth for guest services.
  - Custom—Specify the DSCP value. The range is from 0 to 63.
- In the **DSCP Value** field, enter the value which can be entered only when **Custom** is chosen from the **DSCP** drop-down list.
- If you select **Rate Limit** as an action, you can specify the value in **Avg. Rate Limit (in Kbps)**, which is the average bandwidth limit of that application.
- If you select **Rate Limit** as an action, you can specify **Burst Rate Limit (in Kbps)**, which is the peak limit of that application

Step 5 Click **Save as New Template**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure Devices to Use NetFlow

NetFlow is a protocol that provides valuable information about network users and applications, peak usage times, and traffic routing. This protocol collects IP traffic information from network devices to monitor traffic. The NetFlow architecture consists of the following components:

- Collector—An entity that collects all the IP traffic information from various network elements.
- Exporter—A network entity that exports the template with the IP traffic information. The controller acts as an exporter.

To create NetFlow Monitor or Exporter template:

Step 1 Choose **Configuration > Templates > Features & Technologies > Controller > Netflow**

Step 2 If you want to crate a new Monitor template, hover the mouse cursor over the tool tip next to the **Monitor** template type and click **New**.

Step 3 Complete the required fields and Click **Save as New Template**.

Step 4 If you want to crate a new **Exporter** template, hover the mouse cursor over the tool tip next to the Exporter template type and click **New**.

Step 5 Complete the required fields and Click **Save as New Template**.

Configure Ethernet over GRE (EoGRE) Tunnels on Controllers

Ethernet over GRE (EoGRE) enables tunneling of data traffic from Cisco WLC or Cisco AP to a mobile packet core using EoGRE tunnels.

To add or modify an EoGRE tunneling template, follow these steps:

Step 1 Choose **Configuration** > **Features & Technologies** > **Controller** > **Tunneling** > **EoGRE**.

Step 2 Hover your mouse cursor over the tool tip next to the template type and click **New** to create.

Step 3 Complete the required fields, then and click **Save as New Template,** specify the folder in which you want to save the template, then click **Save**.

Step 4 Click **Deploy** to save and deploy the template to the relevant controller.

Step 5 To verify the status of a template deployment, choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 6 To modify the deployment parameters for any subsequent configuration template deployments, select a configuration job, then click **Edit**.

Related Topics

Add Controller Templates, on page 17
Delete Controller Templates, on page 18
Apply Controller Templates, on page 18

Configure a Lightweight AP Using Template

To configure a new Lightweight Access Point template, follow these steps:

Step 1 Choose **Configuration > Templates > Lightweight Access Points**.

Step 2 Choose **Add Template** from the Select a command drop-down list and click **Go**.

Step 3 Enter a template name in the text box.

Step 4 Enter a template description in the text box.

Step 5 Click **Save as New Template**.

The Lightweight AP Template Detail page contains the following tabs:

- AP Parameters
- Mesh
- 802.11a/n/ac
- 802.11a SubBand

- 802.11b/g/n
- 802.11a/b/g/n
- CDP
- FlexConnect

You can share antenna orientation information among the following radios in Lightweight AP Template:

- 802.11a/n/ac
- 802.11b/g/n
- 802.11a/b/g/n

Note
- You can select **Antenna Type** only as **External** in Lightweight AP Templates.
- Click **Copy below parameters to other radios** to copy the antenna orientation information from the current radio to other radios. Note that this feature works only if the chosen **Antenna Name** is also available in the other radios.

Related Topics

Select the AP Source for AP Template Deployment, on page 45

Select the AP Source for AP Template Deployment

Based on the AP Source selection, the appropriate visualization is loaded on the AP Selection tab.

To select the AP Source:

Step 1 Choose **Configuration** > **Templates** > **Lightweight Access Points**

Step 2 Click the applicable Template Name link in the Lightweight Access Point page.

Step 3 Click the **AP Source** tab and select the visualization:

- **Select APs Manually**—If you select this option, you must select APs manually while trying to push the LWAP template configuration to the APs.
- **Site Maps**—If you select this option, you can select dynamic location based Site Maps for deployment of LWAP template configuration

Configure Autonomous APs Using Templates

To configure a new Autonomous Access Point template, follow these steps:

Step 1 Choose **Configuration > Templates > Autonomous Access Points**.

Step 2 From the Select a command drop-down list, choose **Add Template**.

Step 3 Click **Go**.

Step 4 Enter a Template Name.

Step 5 Enter the applicable CLI commands.

Do not include any show commands in the CLI commands text box. The show commands are not supported.

Step 6 Click **Save**.

Configure Location Information for Switches Using Templates

You can configure the location template for a switch using the Switch Location Configuration template.

To configure a location template for a switch, follow these steps:

Step 1 Choose **Configuration >Templates > Switch Location**.

The Switch Location Configuration template page appears.

Step 2 From the Select a command drop-down list, choose **Add Template**, and click **Go**.

Step 3 Complete the required fields in the New Template page.

Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates

When you migrate an already-managed autonomous access point to lightweight, its location and antenna information is migrated as well. You do not need to reenter the information. Cisco Prime Infrastructure automatically removes the autonomous access point after migration.

The Migration Analysis option does not run during discovery by default. If you prefer to run the migration analysis during discovery, choose **Administration > Settings > CLI Session** to enable this option.

Cisco Prime Infrastructure also supports the migration of autonomous access point to CAPWAP access point.

Choose **Configuration > Templates > Autonomous AP Migration**to access this page. To make a transition from an Autonomous solution to a Unified architecture, autonomous access points must be converted to lightweight access points. After an access point has been converted to lightweight, the previous status or configuration of the access point is not retained.

To create an autonomous AP migration template, follow these steps:

- Choose **Configuration > Autonomous AP Migration**
- From the **Select a command** drop-down list, choose **Add Template**, then click **Go**. If you are updating an already existing template, click the applicable template in the Template Name column.
- To view the migration analysis summary, choose **Monitor > Tools > Autonomous AP Migration Analysis**

For More Information about the field descriptions refer to Cisco Prime Infrastructure Reference Guide

Analyze the Effects of Autonomous AP Migration

To view the Migration Analysis Summary, follow these steps:

Step 1 Choose **Configuration > Templates > Autonomous AP Migration**.

Step 2 Choose **View Migration Analysis Summary** from the Select a command drop-down list, and click **Go**. The Migration Analysis Summary page appears.

The autonomous access points are eligible for migration only if all the criteria have a pass status. A red X designates ineligibility, and a green checkmark designates eligibility. These columns represent the following:

- Privilege 15 Criteria—The Telnet credential provided as part of the autonomous access point discovery must be privilege 15.
- Software Version Criteria—Conversion is supported only in Cisco IOS Release 12.3(7)JA excluding 12.3(11)JA, 12.3(11)JA1, 12.3(11)JA2, and 12.3(11)JA3.
- Role Criteria—A wired connection between the access point and controller is required to send the association request; therefore, the following autonomous access point roles are required:
  - root
  - root access point
  - root fallback repeater
  - root fallback shutdown
  - root access point only
- Radio Criteria—In dual-radio access points, the conversion can happen even if only one radio is of the supported type.
- If an autonomous access point is labeled as ineligible for conversion, you can disable it.

Related Topics

Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates, on page 46

Deploy Configuration Templates

After you create a configuration template, and click **Deploy**. The following tables shoes specify various deployment options as shown in

Table 1: Template Deployment Options

Option	Description
Device Selection	Displays the list of devices to which you want to apply the template. By Device—List all the supported devices. By Group (Device Types)—List only the supported device groups with supported devices. By Group (Location, User Defined)—List all the device groups even if there are no supported devices. But, each group will list only the supported devices. **Note** Search for By Group option will list only the group which contains the supported devices.

Option	Description
Value Assignment	Allows you to specify a variable other than what was previously defined in the configuration template. Click a name, and the previously defined variables are displayed. To change any of the values, click the variable that you want to change, enter a new value, and click **Apply**. You can also update the variables for all selected devices. Click **All Selected Devices** and update variables to apply the changes on all selected devices at the same time. If you want to update variables for a particular device in the list that need not be applicable to other devices, then choose the device and update its variables. All of the other devices will continue to use the variables that were previously defined except for the device for which variables are updated. **Note** The changes that you make apply only to the specific configuration that you are deploying. To change the configuration template for all future deployments, choose **Configuration > Templates > Features & Technologies** and change the template.
Schedule	Allows you to create a meaningful deployment job name, then specify whether to run the job now or in the future. You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.

Job Option	The following job options are available:
	• Failure Policy:
	  • Ignore failure and continue—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
	  • Stop on failure—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
	• Copy Running Config to Startup—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
	• Archive Config after deploy—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Summary	Summarizes your deployment option selections.

Deployment Flow for Model-Based Configuration Templates

Note This deployment flow is not applicable for Controller based templates.

Step 1 After you create a configuration template, click **Deploy**. The Deployment wizard page opens.

Step 2 Select the devices on which you want to deploy the template, then click **Next** to choose the input values.

Step 3 In the **Input Values** tab, you can toggle between Form and CLI view.

Step 4 After entering the necessary configuration values, click **Next** or click **CLI** to confirm the device and template configuration values.

Step 5 Schedule the deployment job using **Schedule Deployment** tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

Failure Policy

- - **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  - **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
  - **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
  - **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 6 Click **Next** to view the job deployment summary.

Step 7 On the Deployment Summary tab, you will see the CLI view for each of the device.

Step 8 Click **Finish** to deploy the template.

Step 9 Click **Job Status** in the pop-up dialog box to launch the **Job Dashboard** to view the status of the job.

Global Variables

The global user variables are variables which are accessible in all scripts. Each user variable must have a name that begins with *gv*. The name should begin with alphabets. Special characters allowed are dot appended with gv, hyphen and underscore.

You can create, delete or edit a global variable.

Step 1 Choose **Configuration** > **Templates** > **Global Variable.**

Step 2 From the Define Global Variable page, click **Add Row**.

Step 3 Specify a name, description, type and display label.

Step 4 Click **Save** to save the new variable.

The global variables created here can be applied while creating the CLI and Features and Technologies templates.

Related Topics

- Create a New Features and Technologies Template Using an Existing Template

Shared Policy Objects

Policy objects enable you to define logical collections of elements. They are reusable, named components that can be used by other objects and policies. They also eliminate the need to define a component each time that you define a policy.

Objects are defined globally. This means that the definition of an object is the same for every object and policy that references it. However, many object types (such as interface roles) can be overridden at the device level. This means that you can create an object that works for most of your devices, then customize the object to match the configuration of a particular device that has slightly different requirements.

To improve efficiency and accuracy in your configuration templates, you can create shared policy objects to include in your configuration templates. You create interface roles or network objects that you can add to your configuration templates.

Related Topics

Define Interface Roles, on page 50
Define Network Objects, on page 51
Create a Security Rule Parameter Map, on page 51
Create a Security Service Group, on page 52
Create a Security Zone, on page 52

Define Interface Roles

Interface roles allow you to define policies to specific interfaces on multiple devices without having to manually define the names of each interface. Interface roles can refer to any of the actual interfaces on the device, including physical interfaces, subinterfaces, and virtual interfaces such as loopback interfaces.

If you create an all-Ethernets interface role, you can define identical advanced settings for every Ethernet interface on the device with a single definition. You add this interface role to a configuration template, then deploy the template to the selected devices to configure the Ethernet interfaces.

Interface roles are especially useful when applying policies to new devices. As long as the devices that you are adding share the same interface naming scheme as existing devices, you can quickly deploy the necessary configuration template containing the interface role to the new devices.

For example, you can use interface roles to define the zones in a zone-based firewall configuration template. You might define an interface role with a naming pattern of DMZ*. When you include this interface role in a template, the configuration is applied to all interfaces whose name begins with “DMZ” on the selected devices. As a result, you can assign a policy that enables anti-spoof checking on all DMZ interfaces to all relevant device interfaces with a single action.

Step 1 Choose **Configuration** > **Templates** > **Shared Policy Objects.**

Step 2 In the Shared Policy Objects pane , choose **Shared** > **Interface Role** .

Step 3 From the Interface Role page, click **Add Object**.

Step 4 From the Add Interface Role page, create matching rules for the interface role.

When you define the zone-based template, for example, all of the interfaces on the device that match the specified rules will become members of the security zone represented by this interface role. You can match interfaces according to their name, description, type, and speed.

Step 5 Click **OK** to save the configurations.

Related Topics

Shared Policy Objects, on page 50

Define Network Objects

Network objects are logical collections of IP addresses or subnets that represent networks. Network objects make it easier to manage policies.

There are separate objects for IPv4 and IPv6 addresses; the IPv4 object is called “networks/hosts,” and the IPv6 object is called “network/hosts-IPv6.” Except for the address notation, these objects are functionally identical, and in many instances the name network/host applies to either type of object. Note that specific policies require the selection of one type of object over the other, depending on the type of address expected in the policy.

You can create shared policy objects to be used in the following configuration templates:

- Zone-based firewall template
- Application Visibility

Step 1 Choose **Configuration** > **Templates** > **Shared Policy Objects** > **Shared** > **IPv4 Network Object** .

Step 2 From the Network Object page, click **Add Object** and add a group of IP addresses or subnets.

Step 3 Click **OK** to save the configurations.

Related Topics

Shared Policy Objects, on page 50

Create a Security Rule Parameter Map

To create and use a set of parameter map objects in the firewall rules, do the following:

Step 1 Choose **Configuration** > **Templates** > **Shared Policy Objects.**

Step 2 In the Shared Policy Objects pane , choose **Shared** > **Security Rule Parameter Map** .

Step 3 From the Security Rule Parameter Map page, click **Add Object**.

Step 4 Specify a name and description for the parameter map that is being created.

Step 5 From the parameters list, select the parameters you want to apply and provide a value for each of them.

Step 6 To specify Device Level Override, choose **Device Level Override** > **Add Device** .

Step 7 Select the device you wish to add, and click **OK**.

Step 8 Click **OK** to save the configurations.

Related Topics

Shared Policy Objects, on page 50

Create a Security Service Group

To create and use a set of parameter map objects in the firewall rules, do the following:

Step 1 Choose **Configuration** > **Templates** > **Shared Policy Objects.**
Step 2 In the Shared Policy Objects pane , choose **Shared** > **Security Service** .
Step 3 From the Security Service page, click **Add Object**.
Step 4 Specify a name and description for the service that is being created.
Step 5 Select the service data from the available list. If you select TCP or UDP, provide a list of port numbers or port ranges (separated by comma).
Step 6 To specify Device Level Override, choose **Device Level Override** > **Add Device**.
Step 7 Select the device you wish to add, and click **OK**.
Step 8 Click **OK** to save the configurations.

Related Topics

Shared Policy Objects, on page 50

Create a Security Zone

Step 1 Choose **Configuration** > **Templates** > **Shared Policy Objects.**
Step 2 In the Shared Policy Objects pane , choose **Shared** > **Security Zone**.
Step 3 From the Security Zone page, click **Add Object**.
Step 4 Specify a name and description for the security zone that is being created.
Step 5 Specify a set of rules that defines the interfaces that must be attached to the zone.
Step 6 To specify Device Level Override, choose **Device Level Override** > **Add Device** .
Step 7 Select the device you wish to add, and click **OK**.
Step 8 Click **OK** to save the configurations.

Related Topics

Shared Policy Objects, on page 50

What are Configuration Groups

You might want to associate a set of configuration templates with specific devices. If you have devices that require the same configuration, you can create a *configuration group* that associates configuration templates with devices. Creating a configuration group allows you to quickly apply new templates without remembering to which devices the new templates should be deployed.

Composite templates allow you to group smaller templates together, but only configuration groups specify the relationship between the templates and the groups of devices to which those templates apply. You can also specify the order in which the templates in the configuration group are deployed to the devices.

Before you create a configuration group, you should:

- Create configuration templates for the devices in your configuration group.
- Determine which devices should be included in the configuration group.

Related Topics

- Create a New Features and Technologies Template Using an Existing Template
- Apply Changes to Groups of NEs Using User Defined Groups

Apply Changes to Groups of NEs Using User Defined Groups

Step 1 Choose **Configuration > Templates > Configuration Groups**.

Step 2 Complete the required fields. The device types displayed depend on what you select from the Device Type field.

Step 3 Where needed, change a template's order in the group by selecting it and clicking the up or down arrow.

Step 4 Click **Save as a New Configuration Group**. The possible configuration groups are:

- Success—Indicates that a configuration group has been successfully created.
- Pending—One or more devices in the configuration group have changes that have not yet been deployed. For example, if you add a new device to the configuration group, the status of the new device is *Pending*. If you modify a configuration template to which the configuration group is associated, all devices in the configuration group have the status *Pending*.
- Scheduled—Indicates that a configuration group deployment is scheduled. When a configuration group is *Scheduled*, any devices in the group that are *Pending* or *Failed* are changed to *Scheduled*. If a device is *Deployed*, it remains *Deployed* and its status does not change to *Scheduled*.
- Failure—Deployment has failed for one or more devices in the configuration group.

Related Topics

Create a New Features and Technologies Template Using an Existing Template, on page 3
What are Configuration Groups, on page 52

What is a WLAN Controller Configuration Group

By creating a configuration group, you can group controllers that should have the same mobility group name and similar configuration. You can assign templates to the group and push templates to all of the controllers in a group. You can add, delete, or remove configuration groups, and download software, IDS signatures, or a customized web authentication page to controllers in the selected configuration groups. You can also save the current configuration to nonvolatile (flash) memory to controllers in selected configuration groups.

Note A controller cannot be a member of more than one mobility group. Adding a controller to one mobility group removes that controller from any other mobility group to which it is already a member.

By choosing **Configuration > Templates > WLAN Controller Configuration Groups**, you can view a summary of all configuration groups in the Prime Infrastructure database. Choose **Add Configuration Groups** from the **Select a command** drop-down list to display a table with the following columns:

- Group Name—Name of the configuration group.
- Templates—Number of templates applied to the configuration group.

Related Topics

- Create Controller Configuration Groups and Apply Configuration Templates to them

Create Controller Configuration Groups and Apply Configuration Templates to them

To create a configuration group, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **WLAN Controller Configuration Groups**.

Step 2 Fromthe **Select a command** drop-down list, choose **Add Config Group**, then click **Go**.

Step 3 Enter the new configuration group name. It must be unique across all groups.

- If Enable Background Audit is selected, the network and controller audits occur for this configuration group.
- If Enable Enforcement is selected, the templates are automatically applied during the audit if any discrepancies are found.

Step 4 Other templates created in Prime Infrastructure can be assigned to a configuration group. The same WLAN template can be assigned to more than one configuration group. Choose from the following:

- Select and add later—Click to add a template at a later time.
- Copy templates from a controller—Click to copy templates from another controller. Choose a controller from a list of current controllers to copy its applied template to the new configuration group. Only the templates are copied.

Note The order of the templates is important when dealing with radio templates. For example, if the template list includes radio templates that require the radio network to be disabled prior to applying the radio parameters, the template to disable the radio network must be added to the template first.

Step 5 Click **Save**. The Configuration Groups page appears.

- After you create a configuration group, Prime Infrastructure allows you to choose and configure multiple controllers by choosing the template that you want to push to the group of controllers.
- General—Allows you to enable mobility group.
- To enable the Background Audit option, set template-based audit in **Administration** > **System** > **Audit Settings**.
- Controllers
- Country/DCA
- Templates—Allows you to select the configuration templates that you have already created.
- Apply/Schedule
- Audit
- Reboot
- Report—Allows you to view the most recent report for this group.

Related Topics

What is a WLAN Controller Configuration Group, on page 53
Add or Remove Controllers from Controller Configuration Groups, on page 55

Set DCA Channels for a Controller Configuration Group, on page 55
Schedule the Deployment of Templates to a Controller Configuration Group, on page 56
Audit Controller Configuration Groups to Ensure Compliance, on page 57
Reboot Configuration Groups, on page 57
View the Status of Template Deployments to Controller Configuration Groups, on page 58

Add or Remove Controllers from Controller Configuration Groups

To add or remove controllers from a configuration group, follow these steps:

Step 1 Choose **Configuration > Templates > WLAN Controller Configuration Groups**.

Step 2 Click a group name in the Group Name column, then click the **Audit** tab.

The columns in the table display the IP address of the controller, the configuration group name the controller belongs to, and the mobility group name of the controller.

Step 3 Click to highlight the row of the controller that you want to add to the group, then click **Add**.

Step 4 To remove a controller from the group, highlight the controller in the Group Controllers area and click **Remove**.

Step 5 Click the **Apply/Schedule** tab, click **Apply** to add or remove the controllers to the configuration groups, then click **Save Selection**.

Related Topics

What is a WLAN Controller Configuration Group, on page 53
Set DCA Channels for a Controller Configuration Group, on page 55
Schedule the Deployment of Templates to a Controller Configuration Group, on page 56
Audit Controller Configuration Groups to Ensure Compliance, on page 57
View the Status of Template Deployments to Controller Configuration Groups, on page 58

Set DCA Channels for a Controller Configuration Group

You can configure one or more countries on a controller. After countries are configured on a controller, the corresponding 802.11a/n DCA channels are available for selection. At least one DCA channel must be selected for the 802.11a/n network. When the country codes are changed, the DCA channels are automatically changed in coordination.

Note 802.11a/n and 802.11b/n networks for controllers and access points must be disabled before configuring a country on a controller. To disable 802.11a/n or 802.11b/n networks, choose **Configure** > **Controllers**, select the desired controller that you want to disable, choose **802.11a/n** or **802.11b/g/n** from the left sidebar menu, and then choose **Parameters**. The Network Status is the first check box.

To add multiple controllers that are defined in a configuration group and then set the DCA channels, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **WLAN Controller Configuration Groups**.

Step 2 From the **Select a command** drop-down list, choose **Add Config Groups**, then click **Go**.

Step 3 Create a configuration group by entering the group name and mobility group name.

Step 4 Click **Save**, then click the **Controllers** tab.

Step 5 Highlight the controllers that you want to add, and click **Add**. The controller is added to the Group Controllers page.

Step 6 Click the **Country/DCA** tab. The Country/DCA page appears. Dynamic Channel Allocation (DCA) automatically selects a reasonably good channel allocation amongst a set of managed devices connected to the controller.

Step 7 Select the **Update Country/DCA** check box to display a list of countries from which to choose.

Step 8 Those DCA channels that are currently configured on the controller for the same mobility group are displayed in the Select Country Codes page. The corresponding 802.11a/n and 802.11b/n allowable channels for the chosen country is displayed as well. You can add or delete any channels in the list by selecting or deselecting the channel and clicking **Save Selection**.

A minimum of 1 and a maximum of 20 countries can be configured for a controller.

Related Topics

What is a WLAN Controller Configuration Group, on page 53
Schedule the Deployment of Templates to a Controller Configuration Group, on page 56
Audit Controller Configuration Groups to Ensure Compliance, on page 57
View the Status of Template Deployments to Controller Configuration Groups, on page 58

Schedule the Deployment of Templates to a Controller Configuration Group

The scheduling function allows you to schedule a start day and time for provisioning.

To apply the mobility groups, mobility members, and templates to all of the controllers in a configuration group, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **WLAN Controller Configuration Groups**.

Step 2 Click a group name in the Group Name column, then choose the **Apply/Schedule** tab.

Step 3 Click **Apply** to start the provisioning of mobility groups, mobility members, and templates to all of the controllers in the configuration group. After you apply, you can leave this page or log out of Prime InfrastructureThe process continues, and you can return later to this page to view a report.

Note Do not perform any other confi1guration group functions during the provisioning process.

A report is generated and appears in the Recent Apply Report page. It shows which mobility groups, mobility members, or templates were successfully applied to each of the controllers.

Step 4 Enter a starting date in the text box or use the calendar icon to choose a start date.

Step 5 Choose the starting time using the hours and minutes drop-down lists.

Step 6 Click **Schedule** to start the provisioning at the scheduled time.

Related Topics

What is a WLAN Controller Configuration Group, on page 53
Add or Remove Controllers from Controller Configuration Groups, on page 55
Set DCA Channels for a Controller Configuration Group, on page 55

View the Status of Template Deployments to Controller Configuration Groups, on page 58

Audit Controller Configuration Groups to Ensure Compliance

The Configuration Groups Audit page allows you to verify if the configuration complies of the controller with the group templates and mobility group. During the audit, you can leave this window or log out of Prime Infrastructure. The process continues, and you can return to this page later to view a report.

Do not perform any other configuration group functions during the audit verification.

To perform a configuration group audit, follow these steps:

Step 1 Choose **Configuration > Templates > WLAN Controller Configuration Groups**.

Step 2 Click a group name in the Group Name column, then click the **Audit** tab.

Step 3 Click to highlight a controller on the Controllers tab, choose **>> (Add)**, and **Save Selection**.

Step 4 Click to highlight a template on the Templates tab, choose **>> (Add)**, and **Save Selection**.

Step 5 Click **Audit** to begin the auditing process.

A report is generated and the current configuration on each controller is compared with that in the configuration group templates. The report displays the audit status, the number of templates in sync, and the number of templates out of sync.

This audit does not enforce Prime Infrastructure configuration to the device. It only identifies the discrepancies.

Step 6 Click **Details** to view the Controller Audit report details.

Step 7 Double-click a line item to open the Attribute Differences page. This page displays the attribute, its value in Prime Infrastructure, and its value in the controller.

Step 8 Click **Retain Prime Infrastructure Value** to push all attributes in the Attribute Differences page to the device.

Step 9 Click **Close** to return to the Controller Audit Report page.

Related Topics

What is a WLAN Controller Configuration Group, on page 53
Add or Remove Controllers from Controller Configuration Groups, on page 55
Schedule the Deployment of Templates to a Controller Configuration Group, on page 56
View the Status of Template Deployments to Controller Configuration Groups, on page 58

Reboot Configuration Groups

Step 1 Choose **Configuration > Templates > WLAN Controller Configuration Groups**.

Step 2 Click a group name in the Group Name column, then click the **Reboot** tab.

Step 3 Select the **Cascade Reboot** check box if you want to reboot one controller at a time, waiting for that controller to come up before rebooting the next controller.

Step 4 Click **Reboot** to reboot all controllers in the configuration group at the same time. During the reboot, you can leave this page or log out of Prime Infrastructure. The process continues, and you can return later to this page and view a report.

The Recent Reboot Report page shows when each controller was rebooted and what the controller status is after the reboot. If Prime Infrastructure is unable to reboot the controller, a failure is shown.

View the Status of Template Deployments to Controller Configuration Groups

To display all recently applied reports under a specified group name, follow these steps:

Step 1 Choose **Configuration > Templates > WLAN Controller Configuration Groups**.

Step 2 Click a group name in the Group Name column, then click the **Report** tab. The Recent Apply Report page displays all recently applied reports including the apply status, the date and time the apply was initiated, and the number of templates. The following information is provided for each individual IP address:

- Apply Status—Indicates success, partial success, failure, or not initiated.
- Successful Templates—Indicates the number of successful templates associated with the applicable IP address.
- Failures—Indicates the number of failures with the provisioning of mobility group, mobility members, and templates to the applicable controller.
- Details—Click Details to view the individual failures and associated error messages.

Step 3 To view the scheduled task reports, click the **click here** link at the bottom of the page.

Related Topics

What is a WLAN Controller Configuration Group, on page 53
Add or Remove Controllers from Controller Configuration Groups, on page 55
Set DCA Channels for a Controller Configuration Group, on page 55
Schedule the Deployment of Templates to a Controller Configuration Group, on page 56

Create Wireless Configuration Templates

The following sections describe how to create wireless configuration templates for:

- Lightweight access points
- Autonomous access points
- Switches
- Converting autonomous access points to lightweight access points

Related Topics

- Configure Lightweight APs Using Configuration Templates
- Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates
- Configure Location Information for Switches Using Templates

Configure Lightweight APs Using Configuration Templates

To create a template for a lightweight access point, follow these steps:

Step 1 Choose **Configuration > Templates > Lightweight Access Points**.

Step 2 From the **Select a command** drop-down list, choose **Add Template**, then click **Go**.

Step 3 Enter a name and description for the template and click **Save**. If you are updating an already existing template, click the applicable template in the Template Name column.

Step 4 Click each of the tabs and complete the required fields.

Related Topics

Migrate an Autonomous Access Point to a Lightweight Access Point Using AP Migration Templates, on page 46

Configure Device - Based Policies for APs

Use the Policy Configuration Templates page to configure device-based policies on a controller. You can configure policies for a user or a device on the network.

The maximum number of policies that you can configure is 64. Policies are not applied on WLANs and AP groups if AAA override is configured on the controller.

Step 1 Choose **Configuration > Templates > Features and Technologies.**

Step 2 From the left sidebar menu, choose **Features and Technologies > Controller > WLANs > Policy Configuration**. The Policy Configuration Template page displays.

Step 3 Complete the following fields:

- Name—Name of the policy template
- Description—Description of the policy template.
- Tags—Search keywords applicable to this template.
- Device Type (validation criteria)—The device product family, series or type used to validate the template (CUWN, for Cisco Unified Wireless Network, is the default).
- Policy Name—Name of the policy.
- Policy Role—The user type or the user group the user belongs to. For example, student, employee.
- EAP Type—EAP authentication method used by the client. The available types are as follows:
  - LEAP
  - EAP-FAST
  - EAP-TLS
  - PEAP
- Device Type—Choose the device type to which this policy applies (e.g., Apple Laptop).
- VLAN ID—VLAN associated with the policy.
- IPv4 ACL—Choose an IPv4 ACL for the policy from the list
- QoS—Choose the policy's Quality of Service level from the list. You can choose one of the follows:
  - Platinum (Voice)—Assures a high QoS for Voice over Wireless.

- Gold (Video)—Supports the high-quality video applications.
- Silver (Best Effort)—Supports the normal bandwidth for clients.
- Bronze (Background)— Provides the lowest bandwidth for guest services.

- Session Timeout—Maximum amount of time, in seconds, before a client is forced to re-authenticate. The default value is 0 seconds.
- Sleeping Client Timeout—Maximum amount of time, in hours, before a guest client is forced to re-authenticate. The default value is 12 hours. The range is from 1 to 720 hours.

Step 4 When you are finished, click **Save as new template**.