



CHAPTER 3

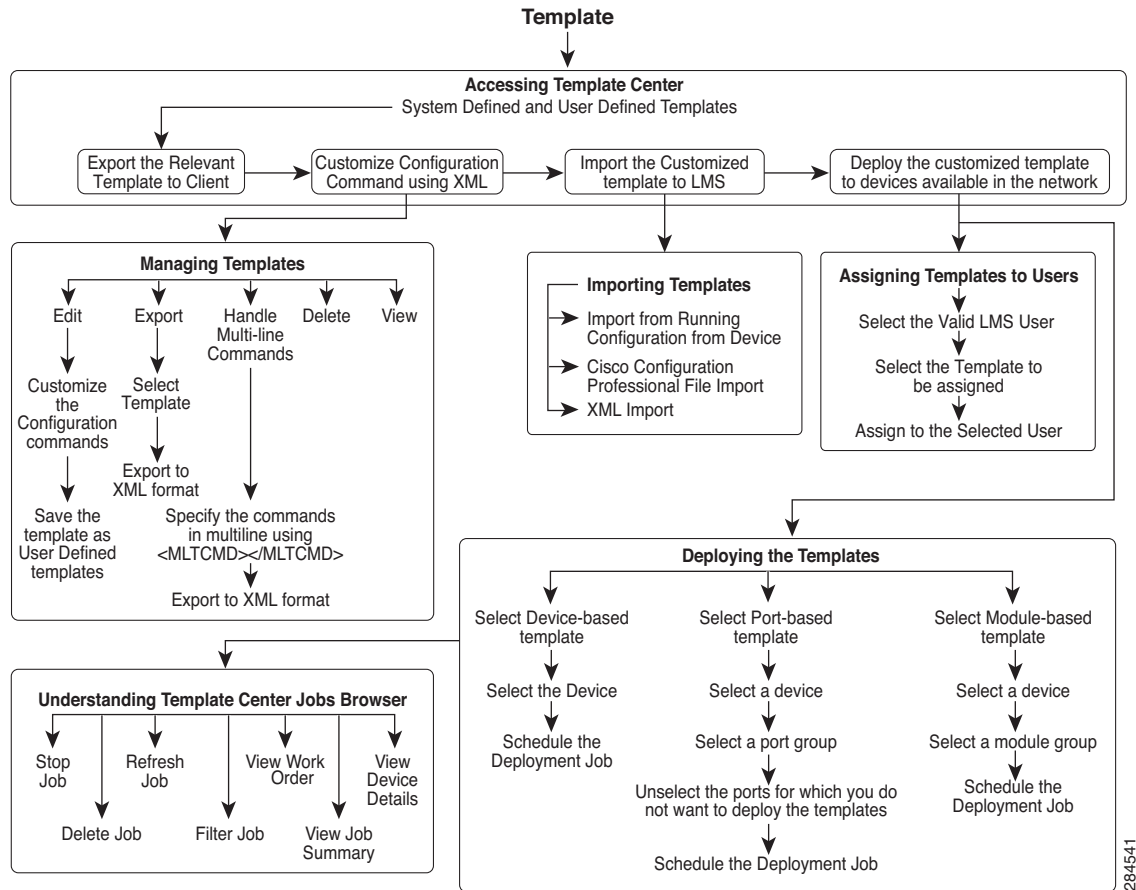
Managing and Deploying Templates

This chapter guides you to manage and deploy configuration templates in LMS.

It explains:

- [Accessing Template Center](#)
- [Creating Configuration Templates](#)
- [Deploying Templates](#)
- [Managing Templates](#)
- [Importing Templates](#)
- [Assigning Templates to Users](#)
- [Understanding the Template Center Jobs Browser](#)
- [Guidelines for Creating Configuration Templates Using IF and FOREACH Statements](#)

Figure 3-1 Managing and Deploying Template Flow Diagram



284/541

Accessing Template Center

The Template Center in LMS provides you with a list of both system-defined templates and user-defined templates. These templates contain configuration commands that can be deployed on the devices in your network. These templates are deployed using Deploy Template jobs in LMS.

You can make customized versions of these system-defined templates, by exporting them, changing CLI's/parameters in template XML according to needs, and importing it back after changing the template name. You can also import templates from a client machine and these templates are stored as user-defined templates in LMS.

It is highly recommended to the user to understand the commands in the template and use it according to their network requirements and other configurations already done/to be done.

To access Template Center, go to **Configuration > Tools > Template Center**.

[Table 3-1](#) describes a list of system-defined templates shipped into LMS 4.2.

Table 3-1 System-defined Templates

Template	Description
DMP Location Configuration	This template configures location information on access ports connected to Digital Media Player. This is a port-based template.
Guaranteed Audio	<p>This Template offers voice services with point-to-point guarantees in an MPLS network. It also offers predictable packet delivery characteristics at various network conditions and loads.</p> <p>When you configure this profile, the system attempts to display video for all participants; however, it does not guarantee that the video of all participants is displayed. For those participants whose video is not displayed, participants are downgraded to audio-only and the profile guarantees preservation of the audio portion of the call.</p>
Heterogeneous Video Conference	<p>This template allows the participants to use different video formats.</p> <p>You can configure different frame rates, bit rates, codecs, or resolutions, and you have the flexibility to choose what profiles to configure, depending on the nature of the participants.</p>
Homogeneous Video Conference	This template allows all the participants in the conference to use the same video format. You must configure the same bit rate, frame rate, codec, resolution, and so on . Only one codec, resolution, and bit rate is configured. All other participants are forced to negotiate to match this profile to join the video conference. If negotiation fails, they fall back to audio-only participants.
Identity - Change of Authorization	<p>This template provides a mechanism for changing the attributes of a session after authentication. When a change in authentication, authorization, and accounting (AAA) policy occurs for a user or user group, administrators can send the RADIUS CoA packets from the AAA server, such as the Cisco Secure Access Control Server (ACS), to re-initialize authentication and apply the new policies.</p> <p>In LMS, you can use this CoA template to generate the configuration commands that can be deployed on devices in your network device to enable Change of Authorization on the device.</p>
IPVSC Location Configuration	This template configures location information on access ports connected to IP Video Surveillance Camera. This is a port-based template.
L2 Access Edge Interface Configuration	<p>This template focuses on Ethernet access interface. It provides Cisco best practice for interface configuration that includes Port security, dhcp snooping, IP Source guard (IPSG), Dynamic ARP Inspection (DAI) and Quality of Service (QoS).</p> <p>This template requires global configuration for IPSG, DAI, and DHCP snooping.</p>
Location Configuration	This template configures location information on access ports connected to any endpoint. This is a port-based template.

Table 3-1 System-defined Templates (continued)

Template	Description
MACsec	<p>This template allows you to enable MACsec to provide secure, encrypted communication on wired LANs.</p> <p>MACsec allows unauthorized LAN connections to be identified and excluded from communication within the network. MACsec defines a security infrastructure to provide data confidentiality and data integrity. MACsec can mitigate attacks on Layer 2 protocols and work with any type of traffic carried over Ethernet links.</p> <p>You can use this template to configure:</p> <ul style="list-style-type: none"> • Security policy to be applied to the session after the supplicant passes 802.1x authentication. • Authentication Failure Policy. • MKA policy. <p>Guidelines for this template:</p> <ul style="list-style-type: none"> • Select any value from the Authentication Failure Policy drop-down list, only if Static Link Policy is Always Secure Sessions. For other values of Static Link Policy, select No Change as the Authentication Failure Policy. • Enter a value for VLAN To Be Used only if Authentication Failure Policy is Authorize into a VLAN. • Enter a name of the other MKA Policy only if MKA Policy is Other Policy. <p>Note If you do not adhere to these guidelines, wrong commands can get deployed.</p>

Table 3-1 System-defined Templates (continued)

Template	Description
Performance Monitoring	<p>You can configure the following for endpoints like Cisco Unified Video Advantage (CUVA), Cisco TelePresence Movi, Tandberg, Webex Servers, and voice data on all endpoints:</p> <ul style="list-style-type: none"> • A flow record to specify the key and non-key fields you want to monitor. • A flow monitor that includes the flow record and flow exporter. • A class to specify the filtering criteria. • A policy to include one or more classes. • One or more performance-monitor type flow monitors. • Reaction ID, jitter and threshold of lost packets. <p>Before you deploy any Performance Monitoring template on a router, you must apply the license command on the router devices.</p> <p>To apply the license in a router:</p> <ol style="list-style-type: none"> 1. Go to config mode. 2. Enter the following commands: <pre style="margin-left: 20px;">license boot module <device series> technology-package datak9 wr mem</pre> 3. Reboot the router.
Performance Monitoring-CUVA	This template allows you to configure Performance Monitor on Cisco Unified Video Advantage (CUVA). CUVA adds video to your communications experience by providing video telephony functionality to Cisco Unified IP phones.
Performance Monitoring-Movi	This template allows you to configure Performance Monitor on Cisco TelePresence Movi. Cisco TelePresence Movi extends the benefits of face-to-face video collaboration to remote workers.
Performance Monitoring-Tandberg	This template allows you to configure Performance Monitor on all Cisco all Tandberg Endpoints. Tandberg video endpoints work together to provide video users with the full functionality of IP telephony.
Performance Monitoring-Voice	This template allows you to configure Performance Monitor for voice data on all endpoints.
Performance Monitoring-Webex Servers	This template allows you to configure Performance Monitor on Webex Servers.
PFR	<p>This template caters for Performance Routing (PFR) that provides best path optimization and advanced load balancing of traffic over the WAN and to the Internet for enterprise networks with multiple paths.</p> <p>You can</p> <ul style="list-style-type: none"> • Configure traffic classes for performance routing. • Configure performance metrics of these individual traffic classes. • Control the traffic by applying suitable traffic class and link policies.

Table 3-1 System-defined Templates (continued)

Template	Description
QoS	<p>This template provides Quality of Service (QoS) macros to switch ports upon detection of a Medianet endpoint.</p> <p>You can</p> <ul style="list-style-type: none"> • Select specific network traffic. • Prioritize it according to its relative importance. • Use QoS macros to provide preferential treatment of traffic in your network.
RSVP	<p>Resource Reservation Protocol (RSVP) signals the QoS needs of an application's traffic along the devices, in the end-to-end path through the network.</p> <p>You can configure:</p> <ul style="list-style-type: none"> • User or application that requires an RSVP request. • Bandwidth that has to be reserved. • Admission policy that the devices uses to admit the RSVP message.
SBA	<p>LMS provides various Smart Business Architecture (SBA) templates to configure resilience, QoS, security and, scalability for SBA networks, for different types of devices. For more information, see Creating Configuration Templates.</p>
SCH	
SCH on IOS and ASA platforms	<p>This template allows you to configure Smart Call Home (SCH) parameters on IOS and ASA devices.</p>
SCH on MDS platform	<p>This template allows you to configure Smart Call Home parameters on MDS devices.</p> <p>Note You can use this template only on MDS devices with NX-OS 4.1(3) or higher software version. SanOS is not supported for the HTTPS transport.</p> <p>In this template, when you enter the Contact Phone Number, it should be in international format and begin with a + sign. You can use hyphens but no spaces in between, for example:</p> <ul style="list-style-type: none"> • +1-100-100-1000 • +11001001000 • +919840011111 <p>The phone number can have a maximum of 17 characters, including the + sign. LMS validates only the format of the phone number and not the maximum length. If the phone number has more than 17 characters, the command will fail when you deploy the template on the device.</p>

Table 3-1 System-defined Templates (continued)

Template	Description
SCH on Nexus platform	<p>This template allows you to configure Smart Call Home parameters on Nexus devices.</p> <p>Note You can use this template only on Nexus devices with NX-OS 4.1(3) or higher software version. SanOS is not supported for the HTTPS transport.</p> <p>In this template, when you enter the Contact Phone Number, it should be in international format and begin with a + sign. You can use hyphens but no spaces in between, for example:</p> <ul style="list-style-type: none"> • +1-100-100-1000 • +11001001000 • +919840011111 <p>The phone number can have a maximum of 17 characters, including the + sign. LMS validates only the format of the phone number and not the maximum length. If the phone number has more than 17 characters, the command will fail, when you deploy the template on the device.</p>
SGA Access	<p>The Security Group Access (SGA) Access template allows you to enable SXP on the Access devices and allows you to propagate the Security Group Tags (SGT) across network devices that do not have hardware support for Cisco TrustSec.</p> <p>You can use this template to configure:</p> <ul style="list-style-type: none"> • Default SGT Exchange Protocol (SXP) password. • SXP address connection. • Default SXP source IP address.
SGACL-IOS	<p>In security group access lists (SGACLs), you can control the operations based on assigned security groups. The grouping of permissions into a role simplifies the management of the security policy. As you add users to the Cisco NX-OS device, you simply assign one or more security groups and they immediately receive the appropriate permissions. You can modify security groups to introduce new privileges or restrict current permissions.</p>
SGACL-NEXUS	<p>In security group access lists (SGACLs), you can control the operations based on assigned security groups. The grouping of permissions into a role simplifies the management of the security policy. As you add users to the Cisco NX-OS device, you simply assign one or more security groups and they immediately receive the appropriate permissions. You can modify security groups to introduce new privileges or restrict current permissions.</p>
SGA Core	<p>The Security Group Access (SGA) Core template allows you to enable SXP on the Nexus devices and allows you to propagate the Security Group Tags (SGT) across Nexus devices that do not have hardware support for Cisco TrustSec.</p> <p>You can use this template to configure:</p> <ul style="list-style-type: none"> • Default SGT Exchange Protocol (SXP) password. • SXP address connection. • Default SXP source IP address.

Table 3-1 System-defined Templates (continued)

Template	Description
Small Branch EIGRP DMVPN FaxRelay	<p>This Template caters for services ready small branch. The configuration includes security features like DMVPN (primary and backup), Firewall (Zone based), IPS and unified communications (SRST).</p> <p>The WAN link is T1, encapsulation is Frame Relay. Backup is SHSDL with ATM IMA.</p> <p>Hardware and Software Pre-requisites</p> <p>HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash</p> <p>1800 series with IOS 12.4.(20)T2 K9 and above with advanced enterprise package.</p>
Small Branch EIGRP DMVPN Only	<p>This Template caters for services ready small branch. The configuration includes security features like DMVPN (primary and backup), Firewall (Zone based), IPS. The WAN link is T1, encapsulation is Frame Relay. Backup is SHSDL with ATM IMA.</p> <p>Hardware and Software Pre-requisites</p> <p>HWIC-1T, HWIC-2SHDSL, 128 MB DRAM, 64 MB flash</p> <p>1800 series with IOS 12.4.(15)T7 K9 and above with advanced enterprise package.</p> <p>T100 Crads should be available in the device.</p>
Small Branch EIGRP GETVPN FaxPassThrough	<p>This Template caters for services ready small branch. The configuration includes security features like GETVPN (primary) and DMVPN (backup), Firewall (Zone based), IPS and unified communications (CME SIP).</p> <p>The WAN link is T1 encapsulation is PPP. Backup is SHSDL with ATM IMA.</p> <p>Hardware and Software Pre-requisites</p> <p>HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash</p> <p>1800 series with IOS 12.4.(20)T2 K9 and above with advanced enterprise package.</p>
Small Branch OSPF GETVPN FaxPassThrough	<p>This Template caters for services ready small branch. The configuration includes security features like GETVPN (primary) and DMVPN (backup), Firewall (Zone based), IPS and unified communications (SIP SRST).</p> <p>The WAN link is T1, encapsulation is Frame Relay. Backup is SHSDL with ATM IMA.</p> <p>Hardware and Software Pre-requisites</p> <p>HWIC-1T1/E1, PVDM2-32, AIM-CUE, 128 MB DRAM, 64 MB flash</p> <p>1800 series with IOS 12.4.(20)T2 K9 and above with advanced enterprise package.</p>
SXP-IOS	<p>Some network devices do not support secured group tag (SGT). For such devices, you can use the SGT Exchange Protocol (SXP) to propagate SGTs. This template is used for SXP configuration. An SXP peer that sends IP-to-SGT binding information to another peer is called SXP Speaker. Any device that receives the binding table and applies it to the ingress port for tagging is called SXP listener. You must configure the SXP peer connection on both the speaker and the listener. When using password protection, make sure that you use the same password on both the speaker and the listener devices.</p>

Table 3-1 System-defined Templates (continued)

Template	Description
SXP-NEXUS	Some network devices do not support secured group tag (SGT). For such devices, you can use the SGT Exchange Protocol (SXP) to propagate SGTs. This template is used for SXP configuration. An SXP peer that sends IP-to-SGT binding information to another peer is called SXP Speaker. Any device that receives the binding table and applies it to the ingress port for tagging is called SXP listener. You must configure the SXP peer connection on both the speaker and the listener. When using password protection, make sure that you use the same password on both the speaker and the listener devices.
Video Transcode	The template provides video transcoding services, where video can be converted from one format to another. You can configure video transcoding when the bit rate, frame rate, resolution, or codec is different between two endpoints.

**Note**

The Basic Small Branch Network provides security and network manageability for the small branch, and integrates the various network services to the branch office router. To deploy these templates ensure that device management IP address is configured in Fa 0/0. This template will remove the IP address in all the other interfaces mentioned in the template.

The above note is applicable for templates such as Small Branch EIGRP DMVPN Only, Small Branch OSPF GETVPN FaxPassThrough, Small Branch EIGRP DMVPN FaxRelay and Small Branch EIGRP GETVPN FaxPassThrough.

Supported SBA Templates

LMS provides various SBA templates to configure resilience, QoS, security, and scalability for Smart Business Architecture networks, for different types of devices. The various SBA templates supported in this release are:

Name of Template	Description
Access Switch Global Configuration	Use this template to configure Virtual LANs, in-band management, DHCP snooping and ARP inspection on the switch.
Distribution Layer Switch Global Configuration	Use this template to configure an in-band management interface, IP unicast routing, and IP multicast routing.
Core Switch Global Configuration	Use this template to configure an in-band management interface, IP unicast routing, IP multicast routing. Use this template to configure an in-band management interface, IP unicast routing, and IP multicast routing.
LAN Switch Universal Configuration	Use this template to configure the features and services that are common across all LAN switches, regardless of the type of platform or role in the network. These are system settings that simplify and secure the management of the solution.

Name of Template	Description
Client Connectivity Configuration	Use this template to configure switch interfaces to support clients and IP phones, port security on the interface, DHCP snooping, and ARP inspection and BPDU Guard on the interface.
Multicast Source Discovery Protocol (MSDP) for Core Switches	Use this template to enable Multicast Source Discovery Protocol (MSDP) for core switches.
Catalyst 4500 Access Switch Global Configuration	Use this template to configure Virtual LANs, in-band management, DHCP snooping and ARP inspection on the switch.
Catalyst 4500 Distribution Layer Connectivity to Access Layer	Use this template to configure connectivity to access layer switches.
Catalyst 4500 Client Connectivity Configuration	Use this template to configure switch interfaces to support clients and IP phones, port security on the interface, DHCP snooping, ARP inspection and BPDU guard on the interface.
Catalyst 4500 Platform Configuration	This is a platform template that defines macros used in Catalyst 4500 Series templates to apply the platform specific configuration.
Catalyst 4500 and 6500 LAN Switch Universal Configuration	Use this template to configure the features and services that are common across all LAN switches, regardless of the type of platform or role in the network. These are system settings that simplify and secure the management of the solution.
Catalyst 6500 Series switches Platform Configuration	This is a platform template that defines macros used in Catalyst 6500 Series templates to apply the platform specific configuration.
Catalyst 6500 Distribution Layer Switch Global Configuration	Use this template to configure an in-band management interface, IP unicast routing, IP multicast routing.
Catalyst 3750 and 3750X Platform Configuration	This is a platform template that defines macros used in Catalyst 3750 and 3750X series templates to apply the platform specific configuration.
Catalyst 3750G Distribution Layer Switch Global Configuration	Use this template to configure an in-band management interface, IP unicast routing, IP multicast routing.
Catalyst 2960-S and 3750-X Platform Configuration	This is a platform template that defines macros that is used in Catalyst 2960-S and 3750-X series templates to apply the platform specific configuration.
Distribution Layer Aggregation Configuration	Use this template to configure links in the core layer that are configured as point-to-point Layer 3 routed EtherChannels.
Connectivity to WAN Routers and LAN Core	Use this template to configure connectivity to WAN Routers and LAN Core.
Infrastructure Connectivity to Routers for 2960 Switches	Use this template when connecting to a network infrastructure device that does not support LACP like a router.
Catalyst 4500 Infrastructure Connectivity to Switches	Use this template to connect to another switch when LACP is set to active on both sides to ensure a proper EtherChannel is formed.
Catalyst 4500 Infrastructure Connectivity to Routers	Use this template to connect to a network infrastructure device that does not support LACP like a router.

Name of Template	Description
Cat6500 Connectivity to WAN Routers and LAN Core	Use this template to connect to WAN Routers and LAN Core.
Cat6500 Distribution Layer Connectivity to Access Layer	Use this template to configure connectivity to access layer switches.
3750X 3560X Infrastructure Connectivity to Distribution Switch	Use this template to connect to another switch when Link Aggregation Control Protocol (LACP) is set to active on both sides to ensure that a proper EtherChannel is formed.
3750X 3560X Infrastructure Connectivity to WAN Router	Use this template to connect to a network infrastructure device that does not support LACP like a router.
Catalyst 3750 Distribution Layer Connectivity to Access	Use this template to configure connectivity to access layer switches.
Cat 2960S Infrastructure Configuration to Distribution Switches	Use this template to connect to another switch when LACP is set to active on both sides to ensure that a proper EtherChannel is formed.
Catalyst 3560-X Platform Configuration	This is a platform template that defines macros used in Catalyst 3560-X series templates to apply the platform specific configuration.

Creating Configuration Templates

CLI templates are user-defined templates that are created based on your own parameters. CLI templates allow you to choose the elements in the configurations. LMS provides variables that you replace with actual values and logic statements.

Prerequisites for Creating CLI Templates

Creating CLI templates is an advanced function that should be done by expert users. Before you create a CLI template, you should:

- Understand to what devices the CLI you create can be applied.
- Understand the data types supported by Prime NCS (WAN).

To create a new configuration template:

-
- Step 1** Select **Configuration > Tools > Template Center > CLI Template Creation**.
 - Step 2** Enter the name of the template.
 - Step 3** Enter the help description for the template.
 - Step 4** Enter the template description.
 - Step 5** Click the icon to select the device type for applying the configuration template.
 - Step 6** Select the device type from the device selector and click **OK**.



Note You cannot create configuration template, if you select a non supported device type. Configuration template will be created only for supported device type, if you select both supported and non-supported device types.

- Step 7** Select the OS Name from the dropdown list.
- Step 8** Enter the CLI content in the text area provided in the Template Detail pane.
For example, enter `hostname`
- Step 9** Click **Manage Variables** button to include variables in the CLI content. The Manage Variable window appears.

To add a new variable to the CLI content:

- a. Click **Add Row**.
- b. Enter the name of the variable. For example, enter `devicehostname`.
- c. Select the variable type as String, Integer or IPv4Address. For example, select string.
- d. Enter the display label of the variable. For example, Enter `HostName`
- e. Enter the help description for the variable.
- f. Select Required checkbox, if you want the variable to appear as mandatory field.

- g. Click the arrow icon next to **Name** to enter the range, default value and validation expression for the variable.

Validation expression indicates an expression which is used to validate the variable. For example, if the variable is hostname, the following validation expression can be used:

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

The above expression indicates that you can enter only a single word without any spaces as hostname.

Range field will be disabled, if you select variable type as String or IPv4Address.

- h. Click **Save** to save the variable details.
- i. Click **Add** to add the variable to the CLI content. For example, hostname `${devicehostname}` will be displayed.

To close the Manage Variable window, click **Close**.

You can see the content in form view on clicking the **Form View** tab.

You can edit or delete the required variable from the Manage Variable window.

You can also filter the variables using the Filter or Advanced Filter option.

Table 3-2 Filter Details

Field	Description
Quick Filter	<p>You can filter the variable based on the following:</p> <ul style="list-style-type: none"> • Name • Type • Description • Display Name • Required
Advanced Filter	<p>Select Match type as All or Any.</p> <ul style="list-style-type: none"> • All - To filter the variables that match all the selected parameters. • Any - To filter the variables that match any of the selected parameter. <p>Select a parameter for which you want to filter the variables. The values displayed are:</p> <ul style="list-style-type: none"> • Default Value • Description • Display Name • Max Value • Min Value • Name • Required • Type • Validation Expression <p>Select the right criterion with respect to the parameter. The values are:</p> <ul style="list-style-type: none"> • Contains • Does not contain • Starts with • Ends with • Is empty • Is not empty • Is exactly (or equals) • Does not equal • Is greater than • Is less than • Is greater than or equal to • Is less than or equal to <p>Enter a value corresponding to the parameter that you have selected.</p>
Manage Preset Filter	You can edit or remove a preset filter.

Step 10 Click **Save to File** to save the newly created template details. To return to the previous page, click **Cancel**.

Click **Import to Template Center** to import the newly created configuration template to Template Center.

For details on how to use IF and FOREACH statements while generating configuration templates, see [Guidelines for Creating Configuration Templates Using IF and FOREACH Statements](#).

Deploying Templates

Templates are deployed to devices using Deploy Template job in LMS. You can deploy these templates for devices, ports and modules.

By default, LMS groups the templates as:

- Custom Templates—Lists all the user-defined templates assigned to the current user.
- Cisco Best Practises Templates—Lists all the system-defined templates.

You can use the filter option to group the templates.

In LMS 4.2, click the expandable icon before each template (triangle-shaped) to see the details of each template. For more details, see [Template Details](#).

To deploy a template:

Step 1 Select **Configuration > Tools > Template Center > Deploy**.

The Template Deployment page appears, displaying Template Selector pane.

You can select templates to deploy configurations.

[Table 3-3](#) describes the Template Selector pane.

Table 3-3 *Template Selector*

Column/Button	Description
Template Name	Shows the name of the system and user-defined templates.
Features	Shows the feature related to the template.
Type	Shows the type of the template (Partial or Complete). <ul style="list-style-type: none"> • Partial—Supports some of the configurations for the device. • Complete—Supports complete configuration for the device.
Role In Network	Role of the device in the network layer (Edge, Core, Access, Distribution)
Category	Shows the category of the template.
Created By	User who created or imported this template. By default, for all system-defined template it will be System and for SBA templates it will be Cisco.

Table 3-3 Template Selector

Column/Button	Description
Scope	Shows the scope of the template for device, port, or module.
Filter (button)	<p>Click Filter. Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click Go to filter details.</p> <p>The following Filter By options are available:</p> <ul style="list-style-type: none"> • Template Name—Select Template Name and enter the complete name. • Type—Select Type and enter the type (partial, complete) • Role In Network—Select RIN and enter the RIN (access, distribution, core) • Category—Select Category and enter the device category • Created By—Select Created By and enter the user name • Scope—Select Scope and enter the scope (device, port, module) <p>You can also use wild card character (*) along with the search text to filter.</p>

Step 2 Select templates and click **Next**.

You can select:

- One Complete with multiple partial templates
- Multiple partial templates

You cannot select multiple Complete templates.

When you select multiple templates, if conflicting features exists between templates, then the deploy template flow will not proceed and a warning message is shown. See [Importing Templates](#) for more information on conflicting features.

The Choose Device Groups pane appears, displaying the Device Selector. Choose the devices, or device groups on which you wish to deploy the templates.

The Device Selector displays devices that are common and applicable to the selected templates.



Note Starting from LMS 4.2.2 Release, the single Performance Routing template will be replaced with three templates namely PfR Basic MC (Master Controller) Template, PfR Basic Border Router, and PfR Advanced MC Template.



Note If the devices selected is more than 2000, the progress bar is not shown.

Step 3 Select devices from the Device Selector and click **Next**.

If you are unable to view any devices in the Device Selector, you do not have any supported devices for the template.

- If you have selected port-related templates, Choose Port Groups pane appears, displaying the Port Selector.
 - Select port groups from the Port Group Selector and click **Next**.

The Review Port Groups page appears with a list of selected devices and selected ports, from the previous page, associated with each device.

- Unselect the ports that you want to exclude from the deployment.
- If you have selected module-related templates, Choose Module Groups pane appears, displaying the Device Selector.

Step 4 Click **Next**, the corresponding template pane appears, allowing you to enter the applicable values for the template.



Note For SGACL-IOS template, the configuration command will fail if the device having SYSOID "1.3.6.1.4.1.9.1.282" and image version "12.2(50)SY" is not present in "adventerprisek9" package.

Step 5 Enter the values and click **Next**.

The Adhoc Configuration for Selected Port/Device Groups pane appears, allowing you to enter the configuration commands that will be deployed on the selected devices or ports in addition to the commands in the template. The commands that you enter here will not be validated by LMS.

This is optional.

Step 6 Click **Next**.

The Schedule Deployment pane appears, displaying Scheduler and Job Options details.

[Table 3-4](#) describes the fields and options in the Schedule Deployment pane.

Table 3-4 Schedule Deployment Pane Description

Options/Field	Description
Schedule Options	Specifies the type of schedule for the job: <ul style="list-style-type: none"> • Immediate—Runs the report immediately. • Once—Runs the report once at the specified date and time. • Daily—Runs daily at the specified date and time. • Weekly—Runs weekly on a day of the week and at the specified time. • Monthly—Runs monthly on a day of the month and at the specified time.
Job Description	Enter a description for the job that you are scheduling. This is a mandatory field. Accepts alphanumeric values and special characters.
E-mail	Enter the e-mail address to which the job sends messages when the job has run. You can enter multiple e-mail addresses separated by comma.
Job Options	The following job options are available: <ul style="list-style-type: none"> • Copy Startup to Running Config upon failure—If template deployment job fails, the startup configuration of the device is copied to running configuration. • Enable Job Password—Select Enable Job Password and enter the Login user name, Login Password and Enable Password details.
Preview CLI (button)	Click Preview CLI to open the Configuration Preview pop-up dialog box. You can select the device name from the drop-down list to view the CLI commands that will be deployed on to the device.

Step 7 Enter a Job Description, select the Schedule and Job options and click **Finish**.

A notification message appears along with the Job ID. The newly created job appears in the Template Center Jobs.

Template Details

You can see the following details when you click the expandable icon before each template (triangle-shaped) to see the details of each template:

- Name—Name of the template. For example, Access PortChannel Interface.
- Description—Description of the template. For example, Template for configuring Portchannel Interface on Access Switches.
- Task—Configuration task of the template. For example, Port Configuration.
- Version—Version of the template. For example, 1.0.
- Feature—Features supported for this template.
- Hardware—The hardware platform supported for deploying this template.
- Reference—Displays any reference text for the template. It can be a link for additional information about the template, or a file in the server.
- Tag—Displays the tags that have been specified for the template. You can have multiple tags for a single template. You can use this for filtering the templates using the Advanced Filter.

Managing Templates

LMS allows you to edit, delete, export and view templates.

By default, LMS groups the templates as:

- Custom Templates—Lists all the user-defined templates assigned to the current user.
- Cisco Best Practices Templates—Lists all the system-defined templates.

You can use the filter option to group the templates.

This section details:

- [Editing Templates](#)
- [Deleting Templates](#)
- [Exporting Templates](#)
- [Handling Multi-line Commands](#)
- [Viewing Template Details](#)

Editing Templates

You can edit the default values of a template (system or user-defined) and save it as user-defined template.

In LMS 4.2, each template has a reference section. In the reference section, you can add a link to provide additional information about the template. The information that you enter in the **Text To Display** text box appears as a link in the expandable pane of the template. When you click the link, it launches the URL or opens the file specified and provides the additional information. You can provide the additional information from a URL or from a file in the server.

The link must start with `http://`. The reference files can have the following extensions: `html`, `txt`, `csv`, `pdf`, `doc`, `docx`, `xls`, `xlsx`, and have to be stored in the location:

- `NMSROOT\htdocs\config-templates-help` (On Windows)
- `NMSROOT/htdocs/config-templates-help` (On Solaris and Soft Appliance)

`NMSROOT` is the LMS install directory. For Solaris and Soft Appliance, it will be `/opt/CSCOpX`.

You can also specify tags for your template that can be used as filters for the templates. You can specify multiple tags for a single template, each tag should be comma separated.

To edit a template:

Step 1 Select **Configuration > Tools > Template Center > Manage**.

The Manage Templates page appears, displaying the Template Selector pane.

[Table 3-3](#) describes the Template Selector pane.

Step 2 Select the template that you need to edit and click **Edit**.

The Edit Template page appears.

Step 3 You can edit the Reference link.

Step 4 You can edit the Tag.

Step 5 Edit the default values of the template and click **Save**.

You can create a new template from an existing template (system or user-defined) and click **Save As** to save it as user-defined template.

You can edit a Cisco Best Practices Template and click **Save As** to save the template as a new template.

The Template Management page appears, displaying the Template with edited values.

Deleting Templates

You can use the Delete option to remove an existing template from the Template Selector pane.



Note You cannot delete a system-defined template from the Template Selector pane.

To delete an existing template:

-
- Step 1** Select **Configuration > Tools > Template Center > Manage**.
The Manage Templates page appears, displaying the Template Selector pane.
[Table 3-3](#) describes the Template Selector pane.
- Step 2** Select an existing user-defined template from the Template Selector pane.
- Step 3** Click **Delete**.
The selected user-defined template is deleted from the Template Selector pane.
-

Exporting Templates

You can use the Export option to export an existing template to a remote or a client machine. The template exported will be in XML format.

To export an existing template:

-
- Step 1** Select **Configuration > Tools > Template Center > Manage**.
The Manage Templates page appears, displaying the Template Selector pane.
[Table 3-3](#) describes the Template Selector pane.
- Step 2** Select an existing template from the Template Selector pane.
- Step 3** Click **Export**.
A dialog box appears, prompting you to open or save the template XML file.
-

Handling Multi-line Commands

In LMS 4.2, you can enter multi-line commands like, banner and crypto certificate commands, as a part of the templates in Template Center. The multi-line commands must be within the tag <MLTCMD> and </MLTCMD>. The commands within the MLTCMD tags are considered as a single command and will be downloaded as a single command onto the device.

These tags are case-sensitive and you must enter them only in uppercase. You cannot start this tag with a space. You can have a blank line within a multi-line command.

Example 1

```
<MLTCMD> banner login "Welcome to  
Cisco Prime LMS - you are using  
Multi-line commands" </MLTCMD>
```

Example 2

```
cmd1<MLTCMD>cmd2  
cmd3  
cmd4  
cmd5</MLTCMD>cmd6
```

Example 2

```
cmd1<MLTCMD>  
cmd2  
cmd3  
cmd4  
cmd5</MLTCMD>cmd6
```

In Example 1 and 2, cmd1,cmd2,cmd3,cmd4,cmd5 and cmd6 are all commands and will be deployed to the device as a single command.

Viewing Template Details

You can use the View Template option to view the details of an existing template from the Template Selector pane.

To view the details of an existing template:

-
- Step 1** Select **Configuration > Tools > Template Center > Manage**.
- The Manage Templates page appears, displaying the Template Selector pane.
- [Table 3-3](#) describes the Template Selector pane.
- Step 2** Select an existing template from the Template Selector pane.
- Step 3** Click **View**.
- A pop-up window appears, you can view the selected template as XML.
-

Importing Templates

LMS allows you create a user-defined configuration template by importing:

- Configuration commands from an existing template (.xml file) stored on a client machine (See [Importing from XML File](#))
- A text file generated using Cisco Configuration Professional tool stored on a client machine (See [Importing from a Cisco Configuration Professional File](#))
- A running configuration from a device (See [Importing Running Config from Device](#))

You can also create a new template file (.xml) using the guideline specified in the XML schema. See [Config Template XML Schema](#) for information.

You can also download config templates from Cisco.com from the URL:

<http://www.cisco.com/cisco/software/release.html?mdfid=283434800&flowid=19062&softwareid=283418816&release=Enterprise%20-%20BN%20SBA&reind=AVAILABLE&rellifecycle=&reltype=latest>.



Note

When you import a template with a name that is already used by another template in LMS, a message appears prompting you to overwrite the template (user-defined) in LMS. System-defined templates cannot be overwritten.

Importing from XML File

To import a template from XML file:

Step 1 Select **Configuration > Tools > Template Center > Import**.

The Import Templates page appears, displaying Choose Import Mode pane.

Step 2 Select **Config Template** from Choose Source Type option.

Step 3 Click **Browse** to select the configuration file (.xml file) stored on a client machine.

Before you import a template, you must ensure that the values of each field do not exceed the respective character limitation. The details are given in the table below.

If the values of each field exceed the character limitation, you will not be able to import the template.

Field	Maximum Number of Characters
Template Name	64
Author	64
Description	1024
Template Version	64
Task	64
Scope	64
Template Type	64
Features	255

Field	Maximum Number of Characters
Hardware Platform	600
PIN	64
Reference Text	100
Reference URL	100
Reference Type	10
Tags	1024

Step 4 Click **Finish**.

A message appears stating that the template has been imported successfully.

Importing from a Cisco Configuration Professional File

To import a template from a Cisco Configuration Professional file:

Step 1 Select **Configuration > Tools > Template Center > Import**.

The Import Templates page appears, displaying Choose Import Mode pane.

Step 2 Select **CCP Config** from Choose Source Type option.

Step 3 Click **Browse** to select the Cisco Configuration Professional file (.txt format) stored on a client machine.

Step 4 Click **Next**.

The View and Edit Configuration pane appears, displaying the configuration commands in the text box.

You can edit these configuration commands. You must ensure that the configuration commands are valid because LMS does not validate these commands.

Step 5 Click **Next**.

The Choose Device Types pane appears.

You need to:

- Choose the image platform for applying the imported configuration from the drop-down list.
- Enter the minimum supported image version for the image platform.
- Choose the device groups for applying the configuration.

Step 6 Click **Next**.

The Choose Conflicting Tags pane appears, displaying the List of Conflicting Features dialog box.

Here, you need to add the list of conflicting features in a file and add it in the Import Template flow. This is optional.

A feature in the template might conflict with a feature of another template. In this case, if you have selected templates that have feature conflicts with each other, then deploy flow will not proceed, and a warning message is shown.

For example,

In the Template Center, you have the following two templates:

- Template A—Deploys Auto Smartport feature and the conflicting feature is CDP
- Template B—Deploys CDP feature

If you have selected both Template A and Template B in the Deploy Template flow, the conflicting feature CDP of Template A with the CDP feature of Template B creates a conflict and this will prevent the Deploy Template job flow to proceed, and a warning message is displayed.

In this case, you have to select templates that do not have feature conflicts with each other and then proceed with the deploy flow.

Table 3-5 describes the fields in the List of Conflicting Features dialog box.

Table 3-5 List of Conflicting Features

Column/Button	Description
Feature	Name of the conflicting feature.
Warning Message	Warning message displayed if the conflicting feature exists
Configuration	Shows the configuration commands of the conflicting feature
Delete (Button)	Delete the conflicting feature file.
Add (Button)	Create a conflicting feature file.
Edit (Button)	Modify an existing conflicting feature file.

Step 7 Click **Next**.

The Enter Template Details pane appears, allowing you to enter the template details described in table.

Table 3-6 describes the fields in Enter Template Details pane.

Table 3-6 Enter Template Details

Field	Description
Template Name	<p>Enter a valid name for the template. Ensure the template name you enter is unique.</p> <p>Note When you import a template with a name that is already used by another template in LMS, a message appears prompting you to overwrite the template (user-defined) in LMS. System-defined templates cannot be overwritten.</p> <p>You can enter a maximum of 64 characters.</p>
Description	<p>Provide a description of the template.</p> <p>You can enter a maximum of 1024 characters.</p>
Task	<p>Enter the task description of the template.</p> <p>You can enter a maximum of 64 characters.</p>

Table 3-6 Enter Template Details

Field	Description
Version	Enter the version of the template. You can enter a maximum of 64 characters.
Scope	Choose the scope of the template. For example, device, port, or module.
Feature	Enter the template feature. You can enter a maximum of 255 characters.
Hardware Platform	Enter the applicable hardware platform for the template. You can enter a maximum of 600 characters.
PIN	Choose the PIN (place of the device in the network) for the template. For example, edge.
Image Feature	Enter the image feature for the template.
Type	Choose the type of the template (Complete, Partial)

Step 8 Click **Finish**.

A message appears stating that the template has been created successfully.

Importing Running Config from Device

To import a running config as a template from a device:

Step 1 Select **Configuration > Tools > Template Center > Import**.

The Import Templates page appears, displaying Choose Import Mode pane.

Step 2 Select **Running Config from Device** from Choose Source Type option.**Step 3** Select a device from the Device Selector.**Step 4** Click Next.

The View and Edit Configuration pane appears, displaying the configuration commands in the text box.

You can edit these configuration commands. You must ensure that the configuration commands are valid because LMS does not do any validation on these commands.

Step 5 Click **Next**.

The Choose Device Types pane appears.

You need to:

- Choose the applicable image platform from the drop-down list.
- Enter the minimum supported image version for the image platform.
- Select the applicable device categories from the Device Type Selector.

Step 6 Click **Next**.

The Choose Conflicting Tags pane appears, displaying the List of Conflicting Features dialog box.

[Table 3-5](#) describes the fields in the List of Conflicting Features dialog box.

Step 7 Click **Next**.

The Enter Template Details pane appears, allowing you to enter the template details described in table.

[Table 3-6](#) describes the fields in Enter Template Details pane.

Step 8 Click **Finish**.

A message appears stating that the template has been created successfully.

Assigning Templates to Users

You can assign templates to users with Network Operator and Network Administrator privileges.

A network administrator must assign template access privileges to other users.

**Note**

View the Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

To assign templates to users:

Step 1 Select **Configuration > Tools > Template Center > Assign Template to User**.

The Assign Templates to Users page appears, displaying the Assign Templates dialog box.

Step 2 Enter the username of the user to whom you want to assign the templates.

This should be a valid LMS user.

Step 3 Select the template that you want to allocate to the user from the Available templates list box and click **Add**.

You can select more than one template, by holding down the Shift key while selecting the template.

The selected templates appear in the Selected Templates list box.

To remove assigned templates, select the templates from the Selected Templates list box and click **Remove**.

Step 4 Add all the required Templates to the Selected Templates list box.

- Step 5** Click **Assign** to assign the template access privileges to the specified user.
- For a specified user, to see the assigned templates, enter the username in the Username field and click **Show Assigned**.
- The templates assigned to the user appear in the Selected Templates list box.
- Step 6** Click **Report** to generate the User Template Report.
- The User Template Report shows the list of users and the templates assigned for each user.



Note By default, all the templates are assigned to admin users. Therefore, the User Template Report will not list the users with Admin privileges.

Understanding the Template Center Jobs Browser

You can browse the template deployment jobs registered on the system. Using the Template Center Jobs, you can manage template jobs. That is, you can stop, delete, refresh, or filter jobs using this job browser. You can also view the template job details such as work order, device details, job summary.



Note View Permission Report (**Reports > System > Users > Permission**) to check whether you have the required privileges to perform this task.

Select either:

Configuration > Tools > Template Center > Jobs.

Or

Configuration > Job Browsers > Template Center

The Template Center Jobs page appears, displaying the List of Template Deployment Jobs pane and Job Details pane for a job.

[Table 3-7](#) describes the List of Template Jobs pane in the Template Center Jobs.

Table 3-7 List of Template Center Jobs

Column/Button	Description
Job ID	<p>Unique number assigned to a template job when it is created.</p> <p>For periodic jobs such as Daily, Weekly, the job IDs are in the number.x format. The x represents the number of instances of the job. For example, 1001.3 indicates that this is the third instance of the Job ID 1001.</p>
Status	<p>Status of the job:</p> <ul style="list-style-type: none"> • Successful—When the job is successful. • Failed—When the job has failed. <p>The number, within brackets, next to Failed status indicates the count of the devices that had failed for that job. This count is displayed only if the status is Failed.</p> <p>For example, if the status displays Failed(5), then the count of devices that had failed amounts to 5.</p> <ul style="list-style-type: none"> • Stopped—When the job has been stopped. • Running—When the job is in progress. • Waiting—When the job is awaiting approval (if job approval has been enabled). • Rejected—When the job has been rejected (if job approval has been enabled).
Description	Description of the job, entered at the time of job creation.
Owner	User who created the job.
Scheduled at	Date and time at which the job was scheduled.
Completed at	Date and time at which the job was completed.
Schedule Type	<p>Type of job schedule—Immediate, Once, Daily, Weekly, Monthly.</p> <p>For periodic jobs, the subsequent instances will run only after the earlier instance of the job is complete.</p>
Stop (button)	Stop or cancel a running job.
Delete (button)	Deletes the selected job from the Template Center Jobs. You can select more than one job to delete.
Refresh Job (button)	<p>Select a Job and click Refresh Job.</p> <p>The Job Details pane gets refreshed showing the latest status of the job.</p>

Table 3-7 List of Template Center Jobs

Column/Button	Description
Filter (button)	<p>Click Filter and select a Filter By criteria from the drop-down list and enter the details in the Equals field.</p> <p>The following Filter By options are available:</p> <ul style="list-style-type: none"> • Job ID—Select Job ID and enter the Job ID number. • Status—Select Status and enter the status (Successful, Failed, Cancelled, Running, Waiting, Rejected). • Description—Select Description and enter the complete name. • Owner—Select Owner and enter the user name. • Scheduled at—Select Scheduled at and enter the schedule time details. • Completed at—Select Completed at and enter the completed time details. • Schedule Type—Select Schedule Type and enter the type (Immediate, Once, Daily, Weekly, Monthly)
Refresh (icon)	Click to refresh the List of Template Jobs table.

Table 3-8 describes the Job Details pane in the Template Center Jobs.

Table 3-8 Template Deployment Job Details

Tab	Description
Work Order	Shows the work order details for the selected job.
General Info	<p>The General Info in the work order displays the following details:</p> <ul style="list-style-type: none"> • Description—Job description entered at the time of job creation. • Owner—User who created the job. • Schedule Type—Type of job schedule (Immediate, Once, Daily, Weekly, Monthly). • Schedule Time—Time at which the job was scheduled to run. The Schedule Time is applicable for periodic jobs and not for Immediate jobs.
Job Policies	<p>The Job Policies in the work order displays the following details:</p> <ul style="list-style-type: none"> • E-mail Notification—E-mail notification status (Enabled/Disabled) • E-mail Ids—E-mail IDs registered for e-mail notification • Execution Policy—Job Execution policy as Parallel • Copy Startup to Running Config upon failure—Displays the status (Enabled/Disabled) • Job Password—Login Password for the job. • Job UserName—Login Username for the job.

Table 3-8 Template Deployment Job Details

Tab	Description
Device and Template Details	Shows the following Device and Template details of the job: <ul style="list-style-type: none"> • Device Template Details • Devices List • Port Template Details • Port Group Details • Module Template Details • Module Details
Device Details	Shows the list of devices added in the Template Deployment job.
Device	Shows the device name.
Status	Status of the device (Success, Failure).
Message Summary	Shows the device status summary.
Show Details	Select the device name and click Show Details . A pop-up window appears, displaying the following details for the device: <ul style="list-style-type: none"> • Device Name—Name of the device. • Device Status—Status of the device (Success, Failure). • Protocol—Protocol details running on the device. • Summary—Shows the device status summary. • CLI Output—Shows the CLI output.
Filter	Click Filter . Select a Filter By criteria from the drop-down list and enter the details in the Equals field. Click Go to filter details. The following Filter By options are available: <ul style="list-style-type: none"> • Device—Select Device and enter the first few letters or the complete name of the device. • Status—Select Status and enter the status (Success, Failure) • Message Summary—Select Message Summary and enter the first few letters of the message summary.

Table 3-8 Template Deployment Job Details

Tab	Description
Job Summary	Shows the job summary details for the selected job.
General Info	The General Info in the job summary shows the following details: <ul style="list-style-type: none"> • Status—Status of the device at the time of job creation. • Start Time—Start time of the job. • End Time—End time of the job.
Job Messages	Shows the following job messages: <ul style="list-style-type: none"> • Pre-job Execution • Post-job Execution
Device Updates	Shows the following update on the devices in the job: <ul style="list-style-type: none"> • Successful • Failed • Not Attempted • Pending

Guidelines for Creating Configuration Templates Using IF and FOREACH Statements

The following are the guidelines that have to be followed while creating configuration templates:

- Parameter can be specified in two ways:
 - `${vlan-id}` - This is how parameters are specified in the old templates. The same can be used in LMS 4.2.
 - `$vlan-id` - Recommended from LMS 4.2.
- Parameter name should not start with number. For example, it should not be `${123vlan-id}`. The correct way of representing it is `${vlan-id}`.
- Parameter name and other special characters (, or and etc) / commands should be separated by space. For example, interface range `${interfaceType} ${port1} , ${interfaceType} ${port2}`

Syntax/Example for IF

The following show the syntax/example of If / if – else / nested – if statement:

```
#if( $option == "heterogeneous" )
    dspfarm profile $PROFILE_ID conference video heterogeneous
#elseif ( $option == "homogeneous" )
    dspfarm profile $PROFILE_ID conference video homogeneous
#else
    dspfarm profile $PROFILE_ID conference video guaranteed-audio
#end
```

See [Sample Template for IF Statement](#) for more details.

[Table 3-9](#) lists the relational and logical operators used in If / if - else / nested - if statement. You can use short version or text version while creating templates.

Table 3-9 *Relational and Logical Operators*

Type of operator	short version	text version
Equal	==	eq
not equal	!=	ne
greater than	>	gt
greater or equal than	>=	ge
less than	<	lt
less or equal than	<=	le
logical and	&&	and
logical or		or
logical not	!	not

Example

```
## logical AND
#if( $foo && $bar )
    dspfarm profile $PROFILE_ID
#end
## logical OR
#if( $foo || $bar )
    dspfarm profile $PROFILE_ID
#end
##logical NOT
#if( !$foo )
    dspfarm profile $PROFILE_ID
#end
```


Syntax/Example for FOREACH

The following show the syntax/example of foreach:

```
#foreach( $product in $allProducts )
    this is the for loop for $product
#end
```

This #foreach loop causes the \$allProducts list to be looped over for all of the products in the list. Each time through the loop, the value from \$allProducts is placed into the \$product variable.

XML Specification for Template

The following are the xml specification for template:

- Textarea / Textbox component can be used
- Data type should be specified as list

Example

```
<parameter name="allProducts">
  <description>Enter the product ids separated by comma [A,B,C]</description>
  <html-component>textarea</html-component>
  <default-value/>
  <data-type>list</data-type>
  <mandatory>true</mandatory>
  <isGlobal>true</isGlobal>
  <help-description>Enter the product IDs</help-description>
  <syntax>
    <min/>
    <max/>
    <pattern/>
  </syntax>
</parameter>
```

You cannot enter special characters such as < and &&, as the parser interprets it as the start of a new element and character entity.

There are two ways where you can use special character such as < and &&:

- Parser ignores the special characters if you enter it within CDATA section. A CDATA section starts with "<![CDATA[" and ends with "]]>". See [Example 1](#).
- Use "&" instead of "&&" and "<" instead of "<". See [Example 2](#).

Example 1

```
<![CDATA[
sccp ccm group ${UCM_GROUP_ID}

#foreach ( ${PROFILE_ID} in $ALL-PROFILE_ID )

    this is the for loop for $PROFILE_ID

    #if ( ${PROFILE_ID} == "vas" && ${UCM_GROUP_ID} == "vvv" )
        PROFILE_ID is vas
    #else
        wrong PROFILE_ID : ${PROFILE_ID}
    #end

#end

#end
```

```
]]>
```

**Note**

Nested CDATA sections are not allowed. The CDATA closing tag "]]>" should not have spaces or line breaks.

Example 2

```
#if (${interfaceType} and "FastEthernet")
interface range ${interfaceType} ${port1}, ${interfaceType} ${port2}
#end

#if (${interfaceType} lt "FastEthernet")
interface range ${interfaceType} ${port1}, ${interfaceType} ${port2}
#end
```