CHAPTER 4

# Designing and Deploying Templates for Configuring

You use templates to define device parameters and settings, which you can later deploy to a specified number of devices based on device type. Templates enhance productivity when you are implementing new services or a new site. Altering configurations across a large number of devices can be tedious and time-consuming, and templates save you time by applying the necessary configurations and by ensuring consistency across devices.

Table 4-1 describes the process for creating and deploying templates.

***Table 4-1 Process for Using Configuration Templates***

| Task | Additional Information |
|---|---|
| 1. Create a template. | Under the **Design** menu, choose which type of template to create. |
| 2. Publish the template. | After you have created the template, click the **Publish** icon to publish the template and make it available to be deployed. |
| 3. Deploy the template. | Under the **Deploy** menu, choose which template to deploy. |
| 4. Verify the status of the template deployment. | Choose **Tools > Task Manager > Jobs Dashboard** to verify the status of the template deployment. |

This chapter contains the following sections:

# About Templates for Branch Design and Deployment

When you have a site, office, or branch that uses a similar set of devices and configurations, you can use configuration templates to build a generic configuration that you can apply to one more or more devices in the branch. You can also use configuration templates when you have a new branch and want to quickly and accurately set up common configurations on the devices in the branch.

## What Is Deploying a Branch?

Deploying a branch is creating the minimum configurations for the branch router. Prime NCS (WAN) allows you to create a set of required features that include:

- Feature templates for the Ethernet interface
- Feature templates for the routing configuration
- CLI template for additional features you require

All of the templates you create can then be added to a single *composite template*, which aggregates all the individual feature templates you need for the branch router. You can then use this composite template when you perform branch deployment operations and to replicate the configurations at other branches.

When you have a set of similar devices across a branch, you can deploy a composite template that includes “golden” configurations to simplify deployment and ensure consistency across your device configurations. You can also use the composite template to compare against an existing device configuration to determine if there are mismatches.

### Related Topics

- Creating Configuration Templates for Branch Deployment, page 4-2
- Creating and Deploying Composite Templates for Branch Deployment, page 4-4

# Creating Configuration Templates for Branch Deployment

The following sections explain how to create and deploy configuration templates that are commonly used in branch deployments:

- Creating an Ethernet Interface Configuration Template
- Creating an EIGRP Routing Configuration Template
- Creating a RIP Routing Configuration Template
- Creating a CLI Configuration Template

## Creating an Ethernet Interface Configuration Template

Many branch deployments require an Ethernet interface configuration template, which you then include in the composite template for branch deployments.

To create an Ethernet interface configuration template:

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

**Step 2** Under the Features and Technologies folder, expand **Interfaces**, then click **Ethernet Interfaces**.

**Step 3** Enter the basic template information.

**Step 4** From the Device Type drop-down list, choose **Routers**.

**Step 5** Under Template Detail, click **Add Row** in the Ethernet Interfaces table.

**Step 6** Complete the fields for an Ethernet interface that is configured on the device. (If, for example, you enter "GigabitEthernet0/1" in the Interface field, the GigabitEthernet0/1 interface must be physically present on the device.)

**Step 7** In the IP Address field, enter a valid IP and mask configuration; for example, 192.168.1.1 255.255.255.0.

**Step 8** Click **Save**.

**Step 9** Click **Save as New Template**.

# Creating an EIGRP Routing Configuration Template

Many branch deployments require an EIGRP routing configuration template, which you then include in the composite template for branch deployments.

To create an EIGRP routing configuration template:

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

**Step 2** Under the Features and Technologies folder, expand **Routing**, then click **EIGRP**.

**Step 3** Enter the basic template information.

**Step 4** From the Device Type drop-down list, choose **Routers**.

**Step 5** Under Template Detail, click **Add Row** in the EIGRP Routes table.

**Step 6** Enter an Autonomous System (AS) Number and a passive interface such as FastEthernet0/0, and choose a value for Auto Summary.

**Step 7** Click **Save**.

**Step 8** Click **Save as New Template**.

# Creating a RIP Routing Configuration Template

Many branch deployments require a RIP routing configuration template, which you then include in the composite template for branch deployments.

To create a RIP routing configuration template:

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

**Step 2** Under the Features and Technologies folder, expand **Routing**, then click **RIP**.

**Step 3** Enter the basic template information.

**Step 4** From the Device Type drop-down list, choose **Routers**.

**Step 5** Under Template Detail, click **Enable RIP**.

**Step 6** Choose a RIP version.

**Step 7** Under Advanced Configuration, choose:

- **IP Network List**—Enter network IP addresses, such as 10.10.10.10.
- **Passive Interfaces**—Enter a passive interface, such as **FastEthernet0/0**.

**Step 8** Click **Save**.

**Step 9** Click **Save as New Template**.

## Creating a CLI Configuration Template

Many branch deployments require a CLI configuration template, which you then include in the composite template for branch deployments.

To create a CLI configuration template:

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

**Step 2** Under the Features and Technologies folder, expand **CLI Template**s, then click **CLI**.

**Step 3** Enter the basic template information.

**Step 4** From the Device Type drop-down list, choose **Routers**.

**Step 5** Under Template Detail, click the **CLI Content** tab, and then enter the following text:

```
banner motd #Welcome to Prime NCS#
```

**Step 6** Click **Save**.

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

# Creating and Deploying Composite Templates for Branch Deployment

You create a composite template if you have a collection of existing feature or CLI templates that you want to apply collectively to devices. You specify the order in which the templates contained in the composite template are applied to devices.

If you have multiple similar devices replicated across a branch, you can create and deploy a “master” composite template to all the devices in the branch. This master composite template can also be used later when you create new branches.

**Step 1** Choose **Design > Templates > Configuration**, then click C**omposite Template**.

**Step 2** Enter parameters for the composite template.

**Step 3** From the Validation Criteria drop-down list, choose the devices to which all of the templates contained in the composite template apply. For example, if in your composite template you have a template that applies to Cisco 7200 Series routers and another that applies to all routers, choose the Cisco 7200 Series routers in the Device Type drop-down menu.

**Note** If a device type is grayed out, the template cannot be applied on that device type.

**Step 4** Under Template Details, choose the templates to include in the composite template.

**Step 5** Using the arrows, put the templates in the composite into 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**.

**Step 7** Navigate to the My Templates folder and choose the template you just saved.

**Step 8** Click the **Publish** icon to publish the template so it can be deployed.

**Step 9** Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

**Step 10** Click **Deploy** on the template you published.

**Step 11** Specify the deployment options as explained in Specifying Template Deployment Options.

**Step 12** Click **OK**.

**Step 13** Choose **Tools > Task Manager > Jobs Dashboard** to verify the status of a template deployment.

# Creating Configuration Templates

Prime NCS (WAN) provides the following types of configuration templates:

- 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 NCS (WAN) provides variables that you replace with actual values and logic statements. You can also import templates from Cisco Prime LAN Management System. See Creating and Deploying CLI Templates.
- Feature and technology templates—Configurations that are specific to a feature or technology in a device's configuration. See Creating and Deploying Feature and Technology Templates.
- 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. See Creating and Deploying Composite Templates for Branch Deployment.

**Note** All templates must be *published* before they can be deployed to devices.

You use templates to define device parameters and settings, which you can later deploy to a specified number of devices based on device type. Altering configurations across a large number of devices can be tedious and time-consuming, and templates save you time by applying the necessary configurations and ensuring consistency across devices.

## Default Configuration Templates

Prime NCS (WAN) ships with default configuration templates that you can find under **Design > Configuration Templates > My Templates > OOTB**. These templates are described in Table 4-2.

*Table 4-2 Prime NCS (WAN)-Provided Configuration Templates*

| Use This Configuration Template ... | To Do This... |
|---|---|
| Medianet – PerfMon | Configure performance monitoring for Medianet. |
| PA with WAAS | Configure Cisco Performance Agent[1] and Wide Area Application Services (WAAS). |
| PA without WAAS | Configure Cisco Performance Agent without WAAS. |
| Collecting Traffic Statistics | Collect network traffic statistics. |

1. Cisco Performance Agent is a licensed feature of Cisco IOS Software. It offers comprehensive application performance and network usage data to help network administrators accurately assess user experience and optimize the use of network resources.

# 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:

- Have expert knowledge and understanding of the CLI and be able to write the CLI in Apache VTL. For more information about Apache Velocity Template Language, see http://velocity.apache.org.
- Understand to what devices the CLI you create can be applied.
- Understand the data types supported by Prime NCS (WAN).
- Understand and be able to manually label configurations in the template.

# Creating and Deploying CLI Templates

Before creating a CLI template, make sure you have satisfied the prerequisites as described in Prerequisites for Creating CLI Templates.

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

**Step 2** Expand the **CLI Template folder**, then click **CLI**.

**Step 3** Enter the basic template information.

**Step 4** From the Validation Criteria drop-down list, choose the device types to which this CLI template can be applied.

The Device Type field lists product types, product families, and model numbers.

**Step 5** Under Template Detail, click **Manage Variables**.

This allows you to specify a variable for which you will define a value when you deploy the template.

**Step 6** Click **Add Row** and enter the parameters for a new variable, then click **Save**.

**Step 7** Enter the CLI information.

**Note** In the CLI field, you must enter code using Apache VTL.

**Step 8** To view a list of all variables used in the template, click **Form View** (this is a read-only view), then click **Manage Variables** to change the variables.

**Step 9** Click **Save As New Template**.

**Step 10** Navigate to the My Templates folder and choose the template you just saved.

**Step 11** Click the **Publish** icon at the top-right corner, then click **OK**.

**Step 12** Click the **Go to Deployment** icon and go to the **Deploy > Configuration tasks** page.

**Step 13** Click **Deploy** on the template you published.

**Step 14** Specify the deployment options as explained in Specifying Template Deployment Options.

**Step 15** Click **OK**.

## Understanding Database Variables in CLI Templates

When a device is discovered and added to Prime NCS (WAN), you can use the database values that were gathered during the inventory collection to create CLI templates. For example, if you want to create and deploy a CLI template to shut down all interfaces in a branch, you can create a CLI template that contains the following commands:

```
#foreach ($interfaceName in $interfaceNameList)
interface $interfaceName \n
shutdown
#end
```

where *$interfaceNameList* is the database variable type whose value will be retrieved from the database. *$interfaceNameList* has a default value of `Inventory::EthernetProtocolEndpoint.IntfName`.

To populate *interfaceNameList* with the value from the database, you must create a properties file to capture the query string as described below and save it in the /opt/CSCOlumos/conf/ifm/template/InventoryTagsInTemplate folder.

### Sample Property File

Filename: interface.properties

```
# for interface name tag->Name
EthernetProtocolEndpoint.IntfName=select u.name from EthernetProtocolEndpoint u where
u.owningEntityId =
# say for other attributes of EthernetProtocolEndpoint Model, should we define tags
# any good generic way of accepting tags -attr+its mapped query ?
```

After you create the CLI template and the property file and deploy the CLI template, the following CLI is configured on the devices. This output assumes the device has two interfaces (Gigabitethernet0/1 and Gigabitethernet0/0):

```
interface GigabitEthernet0/0
shutdown
interface GigabitEthernet0/1
shutdown
```

**Note** *InterfaceNameList* is a Prime NCS (WAN) default database variable.

Verify that the Enterprise JavaBeans Query Language (EJB QL) specified in the properties file returns a list of strings; or, if a single element is specified, the EJB QL should return a list containing one element.

## Specifying Template Deployment Options

After you publish a template and want to deploy it to one or many devices, you can specify devices, values, and scheduling information to tailor your deployment. Table 4-3 explains the deployment options.

*Table 4-3 Deploy > Configuration Task Options*

| Option | Description |
|---|---|
| Device Selection | Displays the list of devices to which you want to deploy the template. |
| 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 you want to change, enter a new value, and click **Apply**.<br>**Note** The changes you make apply only to the specific configuration you are deploying. To change the configuration template for *all* future deployments, choose **Design > Configuration Templates** 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. |
| Summary | Summarizes your deployment option selections. |

# Creating Feature and Technology Templates

Feature and technology templates are templates that are based on device configuration. Feature and technology templates focus on specific features or technologies in a device's configuration. When you add a device to Prime NCS (WAN), Prime NCS (WAN) gathers the device configuration for the model you added.

**Note** Prime NCS (WAN) does not support every configurable option for all device types. If Prime NCS (WAN) does not have a feature and technology template for the specific feature or parameter you want configure, create a CLI template as described in Creating and Deploying CLI Templates.

## Creating and Deploying Feature and Technology Templates

You create feature and technology templates to simplify the deployment of configuration changes. For example, you can create an SNMP feature and technology template and then quickly deploy it to the devices you specify. You can also add one or more feature and technology templates to a composite template. If you do, when you update the SNMP template, the composite template in which the SNMP template is contained automatically has your latest changes.

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

**Step 2** Expand the **Features and Technologies** folder, choose an appropriate subfolder, then choose a template type to create.

**Step 3** Enter the basic template information.

**Step 4** From the Validation Criteria drop-down list, choose the device types to which this feature template can be applied. The Device Type field lists product types, product families, and model numbers.

**Note** 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.

**Step 5** Under Template Detail, enter the CLI information.

**Step 6** Click **Save As New Template**.

**Step 7** Navigate to the My Templates folder and choose the template you just saved.

**Step 8** Click the **Publish** icon to publish the template so it can be deployed.

**Step 9** Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

**Step 10** Click **Deploy** on the template you published.

**Step 11** Specify the deployment options as explained in Specifying Template Deployment Options.

**Step 12** Click **OK**.

# Creating and Deploying a Static Routing Template

You can use a template to configure a static route. Static routes can be overwhelming in a large or complicated network. By creating a static routing template, you can avoid making manual changes each time there is a change in the network.

To create and deploy a static routing template:

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

**Step 2** Expand the **Features and Technologies** folder, expand the **Routing** subfolder, then click **Static**.

**Step 3** Enter the basic template information.

**Step 4** Under Template Detail, click **Add Row**, then complete the fields.

**Note** For Permanent Route, choose

- **True** to specify that the route will not be removed from the routing table, even if the next-hop interface shuts down or next-hop IP address is not reachable.
- **False** to specify that the route will be removed from the routing table, even if the next-hop interface shuts down or next-hop IP address is not reachable.

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

**Step 6** Navigate to the My Templates folder and choose the template you just saved.

**Step 7** Click the **Publish** icon to publish the template so it can be deployed.

**Step 8** Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

**Step 9** Click **Deploy** on the template you published.

**Step 10** Specify the deployment options as explained in Specifying Template Deployment Options.

**Step 11** Click **OK**.

# Creating and Deploying an ACL Template

To create and deploy a template to configure access lists:

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

**Step 2** Expand the Features and Technologies folder, expand the Security subfolder, then click ACL.

**Step 3** Enter the basic template information.

**Step 4** Under Template Detail, click **Add Row**, then complete the fields described in Table 4-4.

*Table 4-4 ACL Template Details*

| Field | Description |
|---|---|
| Name/Number | Name or number of the ACL. |
| Applied To | Enter the interface of the router on which to apply the ACL. It is recommended that you apply the ACL on the interface closest to the source of the traffic. |
| Type | Choose:<br>**Standard**—Standard IP ACLs control traffic based on the source IP address.<br>**Extended**—Extended IP ACLs identify traffic based on source IP address, source port, destination IP address, and destination port. |
| Description | Description of the ACL. |

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

**Step 6** Navigate to the My Templates folder and choose the template you just saved.

**Step 7** Click the **Publish** icon to publish the template so it can be deployed.

**Step 8** Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

**Step 9** Click **Deploy** on the template you published.

**Step 10** Specify the deployment options as explained in Specifying Template Deployment Options.

**Step 11** Click **OK**.

# Creating Security Configuration Templates

You can create security configuration templates for the following features:

- Dynamic Multipoint VPN (DMVPN)
- Group Encrypted Transport VPN (GETVPN)

# Creating a DMVPN Template

To create a DMVPN template, follow these steps:

**Step 1** Choose **Design > Configuration > Features and Technologies > Security > DMVPN**.

The Dynamic Multipoint VPN Configuration Template page opens.

**Step 2** In the Template Basic section, enter a name and a description in the appropriate fields.

**Step 3** From the Validation Criteria drop-down list, choose a device type from the drop-down list and enter the OS version.

**Step 4** In the Template Detail section, enter the IKE Authentication and Encryption policy.

**Step 5** In the IKE Authentication Type field, click the anchored plus button (**+**), and choose the IKE authentication type.

If you choose the default Pre-Shared key, you must provide the secret key and reconfirm it. If you choose the Digital Certificate as the authentication type, the router must have a digital certificate issued by a Certificate Authority to authenticate itself.

**Step 6** In the IKE Authentication Policy section, click the **Add Row** button to add the IKE policies

**Step 7** Enter the priority, and choose Authentication, Diffie-Hellman (D-H) Group, Encryption, Hash, and Lifetime from the drop-down list.

To delete the IKE policies, choose the policy and click **Delete**.

To edit the parameters of the IKE policy, click a row or field and edit its parameters.

**Step 8** Click **Save** to save the configuration.

**Step 9** In the Encryption policy field, click the anchored plus button (**+**) to add the Transform Set Profile.

**Step 10** In the Transform Set Profile dialog box, enter a name and choose the acceptable combination of security protocols and algorithm from the drop-down list to configure the transform set.

**Step 11** Enable IP compression and choose a mode for the transform set.

**Step 12** To delete the transfer set, choose the transfer set and click **Delete**. To edit the parameters of the transfer set, click a row or field and edit its parameters.

**Step 13** Click **Save** to save the configuration.

**Step 14** In the Topology and Routing Information section, choose the topology and the device role. For the Routing Protocol, choose the Extended Interior Gateway Routing Protocol (EIGRP) or Routing Information Protocol Version 2 (RIPv2). Use the Other option to configure other protocols.

**Note** The routing information are disabled when you select Hub as the device role.

**Step 15** Enter the required information in the NHRP and Tunnel Parameters section.

**Step 16** In the NHS Server Information section, add the Next Hub server information, including the IP Address of Hub's physical interface and the IP address of Hub's tunnel interface.

**Note** If you check the Cluster Support check box, add the information, such as Cluster ID, Max Connection, and Next Hub Server. The template with the NHS cluster configuration will be applied only to the device running Cisco IOS Software version 15.1(2)T or later.

**Step 17** Click **Save As New Template**.

The new template appears in the My Templates folder.

**Step 18** Click the **Publish** icon to publish the template so it can be deployed.

**Note** After you create the template, publish it to make it available for deployment.

For a list and descriptions of elements on the Dynamic Multipoint VPN Template page, see Table 4-5.

*Table 4-5 Dynamic Multipoint VPN Template Page*

| Element | Field Description |
|---|---|
| **Template Basic tab** | |
| Name | Enter a name for the DMVPN template. |
| Description | (Optional) Enter a description for the DMVPN template. |
| **Validation Criteria tab** | |
| Device Type | Choose the device type from the drop-down list. |
| OS Version | Enter the OS version for the device. |
| **IPsec Information** | |
| Authentication Type | Click the Preshared Keys or Digital Certificates radio button.<br>• Preshared Keys—Allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase.<br>• Digital Certificates—Authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. Certificates provide nonrepudiation of communication between two peers, meaning that it can be proven that the communication actually took place. |
| Priority | The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common security association (SA). If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number.<br>Valid values range from 1 to 10000. The lower the number, the higher the priority. If you leave this field blank, Security Manager assigns the lowest unassigned value starting with 1, followed by 5, and continuing in increments of 5. |
| Authenticate | Choose the authentication type from the drop-down list. |

*Table 4-5 Dynamic Multipoint VPN Template Page*

| Element | Field Description |
|---|---|
| Diffie-Hellman Group | The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are:<br>1—Diffie-Hellman Group 1 (768-bit modulus).<br>2—Diffie-Hellman Group 2 (1024-bit modulus).<br>5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group. |
| Encryption policy | Choose the encryption policy from the drop-down list. Choose the encryption algorithm from the drop-down list. The encryption algorithm used to establish the Phase 1 SA for protecting phase 2 negotiations:<br>AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys.<br>AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys.<br>AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys.<br>DES—Encrypts according to the Data Encryption Standard using 56-bit keys.<br>3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option. |
| Hash | The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are:<br>• SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5.<br>• MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA. |
| Lifetime | The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.<br>You can specify a value from 60 to 2147483647 seconds. The default is 86400. |
| **Transform Set** | |
| Name | Enter the transform set name. The transform set encrypts the traffic on the tunnel. |
| ESP Encryption Algorithm | The algorithm used to encrypt the payload. Choose the encryption algorithm from the drop-down list. The options are:<br>• ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm.<br>• ESP with the 192-bit AES encryption algorithm.<br>• ESP with the 256-bit AES encryption algorithm.<br>• ESP with the 168-bit DES encryption algorithm (3DES or Triple DES).<br>• Null encryption algorithm. |

*Table 4-5 Dynamic Multipoint VPN Template Page*

| Element | Field Description |
|---|---|
| ESP Integrity Algorithm | The algorithm used to check the integrity of the payload. Choose the integrity algorithm from the drop-down list. The options are:<br>• ESP with the MD5 (HMAC variant) authentication algorithm.<br>• ESP with the SHA (HMAC variant) authentication algorithm. |
| AH Integrity | Choose the AH integrity from the drop-down list. The options are:<br>• AH with the MD5 (Message Digest 5) (a Hash-based Message Authentication Code [HMAC] variant) authentication algorithm.<br>• AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm. |
| Compression | Enable the IP compression to compress payload. IP compression with the Lempel-Ziv-Stac (LZS) algorithm. |
| Mode | Choose the mode to transport the traffic. |
| **Device Role and Topology** | |
| Spoke radio button | Check the Spoke radio button to configure the router as a Spoke in the topology. |
| Hub radio button | Check the Hub radio button to configure the router as a Hub in the topology. |
| Dynamic Connection between Spokes | Check the Create Dynamic Connection between spokes check box to configure the dynamic connection between spokes. |
| EIGRP | Choose the routing information. |
| RIPV2 | Choose the routing information. |
| Other | Check the **Other** check box to select other routing protocol. |
| **NHRP and Tunnel Parameters** | |
| Network ID | Enter the NHRP Network ID.The network ID is a globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295. |
| Hold Time | Enter the number of seconds that the Next Hop Resolution Protocol (NHRP) NBMA addresses should be advertised as valid. The default value is 7200 seconds. |
| Tunnel Key | Enter the tunnel key. The tunnel key is used to enable a key ID for a particular tunnel interface. The range is from 0 to 4294967295. |
| NHRP Authentication String | Enter the Authentication String. |
| IP MTU | Enter the MTU size of IP packets that are sent on a particular interface. The default value for Ethernet and the serial interface is 1500. The default value varies depending upon the media type. |
| TCP Maximum Segment Size | Enter the TCP maximum segment size. The range is from 500 to 1460. |
| Physical Interface | Enter the physical interface. |
| NHS Fallback Time | (Optional) Enter the NHS fallback time in seconds. The range is from 0 to 60. |
| **NHS Server** | |
| Cluster ID | Enter the cluster value to form a group having one or more hubs. The range is from 0 to 10. |
| Max Connections | Enter the maximum number of connections that can be active in a particular group/cluster. |

*Table 4-5 Dynamic Multipoint VPN Template Page*

| Element | Field Description |
|---|---|
| Priority | The priority of the particular hub in a cluster. Depends on the priority of the spoke router that will form a tunnel with the hub devices. |
| Next Hop server | Enter the IP address of the next-hop server. |
| Hub's Physical IP Address | Enter the IP address of the hub's physical interface. |

# Deploying DMVPN Templates

To deploy the DMVPN template, follow these steps.

**Note** You must publish the specified template before it can be deployed to devices.

**Step 1** Choose **Deploy > Configuration Tasks > My Templates**.

**Step 2** On the My Templates page, select the DMVPN template, and click the **Tasked View** button.

**Step 3** From the Deploy Task pad, click **Deploy**.

The Template Deployment page opens.

**Step 4** From the device selection section, select the list of devices on which to deploy the template.

**Step 5** In the Value Assignment section, click the radio button to select the device.

**Step 6** For DMVPN, you can change the values for GRE IP Address, Subnet Mask, and Tunnel Throughput Delay.

**Step 7** If you have changed the values, click **Apply**. For elements on the page, see Table 4-5.

**Note** The spoke option for Cisco IOS Software version 15.1(2)T or later should display the NHS cluster configuration section.

**Step 8** In the Schedule section, enter the Job Name, then click one of the following radio buttons:

- **Run**—To run the job immediately.
- **Run at Schedule Time**—To specify a time to run the job.

**Step 9** Under Summary, verify your entries, then click **OK**.

# Creating a GET VPN Group Member Template

To create a GETVPN group member template:

**Step 1** Choose **Design > Configuration > Features and Technology > Security > GETVPN-GroupMember**.

The GETVPN-GroupMember Configuration Template page appears.

**Step 2** In the Template Basic section, enter a name, description, and author name in the appropriate fields.

**Step 3** From the Validation Criteria drop-down list, choose a device type from the drop-down list and enter the OS version.

**Step 4** In the Group Information section, enter the group name and the group ID.

**Step 5** Click the **IKE Authentication Policy +** button to add the IKE authentication information.

**Step 6** In the IKE Authentication Policy dialog box, click the **Pre-Shared key** or **Digital Certificate** radio button.

The key server authenticates by using the digital certificate. The router must have a digital certificate issued by a Certificate Authority to authenticate itself.

**Step 7** In the IKE Policy section, click **Add Row and** add the IKE policies, then click **Save**. Click on the **Row** or **Field** to edit the parameters. Select the IKE policies from the list and click **Delete** to delete the IKE policies.

**Step 8** Enter the registration interface for the group member.

**Step 9** In the Traffic Detail section, enter the Local Exception ACL and the Fail Close ACL.

**Step 10** In the Key Servers section, enter the Primary Key Servers and Secondary Key Servers IP addresses/Hostname.

**Step 11** Click **Add Row** or **Delete** to add or delete the secondary key server. If you want to edit the secondary key server, click on the **Row** or **Field** and edit the IP address of the key server.

**Step 12** In the Migration section, check the Enable Passive SA check box to enable passive SA. Use this option to turn on the Passive SA mode on this group member.

For a list and description of elements on the GETVPN Group Member template page, see Table 4-6.

**Note** After you create the template, publish it to make it available for deployment.

**Step 13** Click **Save As New Template**.

The template you created appears under My Templates.

**Step 14** Click the **Publish** icon to publish the template so it can be deployed.

*Table 4-6 GETVPN Group Member Template Page*

| Element | Field Description |
|---|---|
| **Template Basic tab** | |
| Name | Enter a name for the GETVPN group. |
| Description | (Optional) Enter a description for the GETVPN template. |
| Author | (Optional) Enter the author name. |
| **Validation Criteria tab** | |
| Device Type | Choose a device type from the drop-down list. |
| OS Version | Enter the OS version for the device type. |
| **Template Detail** | |
| Group Name | Enter the group name for the GETVPN group member template. |
| Group ID | Enter a unique identity for the GETVPN group member. This can be a number or an IP address. The range is from 0 to 2147483647. |

*Table 4-6 GETVPN Group Member Template Page*

| Element | Field Description |
|---|---|
| **IKE Authentication Policy** | |
| Authorization Type | Click the Preshared Keys or Digital Certificates radio button:<br>• Preshared Keys—Preshared keys allow for a secret key to be shared between two peers and to be used by IKE during the authentication phase.<br>• Digital Certificates—An authentication method in which RSA key pairs are used to sign and encrypt IKE key management messages. Certificates provide nonrepudiation of communication between two peers, meaning that it can be proven that the communication actually took place. |
| Priority | The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common SA. If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number.<br>Valid values range from 1 to 10000. The lower the number, the higher the priority. |
| Encryption | Choose the encryption algorithm from the drop-down box.The encryption algorithm is used to establish the Phase 1 SA for protecting Phase 2 negotiations:<br>• AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys.<br>• AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys.<br>• AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys.<br>• DES—Encrypts according to the Data Encryption Standard using 56-bit keys.<br>• 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option. |
| Hash | The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are:<br>• SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5.<br>• MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA. |
| Diffie-Hellman Group | The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are:<br>• 1—Diffie-Hellman Group 1 (768-bit modulus).<br>• 2—Diffie-Hellman Group 2 (1024-bit modulus).<br>• 5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group. |

*Table 4-6 GETVPN Group Member Template Page*

| Element | Field Description |
|---|---|
| Lifetime | The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure your IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.<br>You can specify a value from 60 to 2147483647 seconds. The default is 86400. |
| Registration Interface | Enter the interface to which the crypto map needs to be associated. |
| **Traffic Details** | |
| Local Exception ACL | Choose an ACL for the traffic that must be excluded from the encryption. |
| Fail Close ACL | Choose an ACL for the traffic that must be sent in clear text until the group member registers with the key server. If the Fail Close feature is configured, all the traffic passing through the group member will be dropped until the group member is registered successfully. Once the group member registers successfully and SAs are downloaded, this feature turns off by itself. |
| **Key Server Information** | |
| Primary Key Server | Specify the primary key server IP address to which the client connects. The primary key server is responsible for creating and distributing group policies to all group members and periodically synchronizing with the secondary key servers. The server with the highest priority is elected as a primary key server. |
| Secondary Key Server | Specify the secondary key server IP address to which the group member falls back when the primary key server registration fails. A group member can be configured to register to any available key server from a list of all secondary key servers. Group member configuration determines the registration order. The key server defined first is contacted first, followed by the second defined key server, and so on. You can have a maximum of eight key servers for a group member. |
| **Migration** | |
| Enable Passive SA | The Passive SA mode overrides the receive-only SA option on the key server and encrypts all outbound traffic. Use this option to turn on the Passive SA mode on the group member. |

# Creating a GET VPN Key Server Template

Use the GETVPN Key Server template to create the template.

To create a GETVPN Key Server template:

**Step 1** Choose **Design > Configuration > Features Technologies > Security > GETVPN-KeyServer**.

The GETVPN-KeyServer Configuration Template page opens.

**Step 2** In the Template Basic section, enter a name, description, and author in the appropriate fields.

**Step 3** From the Validation Criteria drop-down list, choose a device type from the drop-down list and enter the OS version.

**Step 4** In the Group Information section, enter the group name and group ID.

**Step 5** Click the **IKE Authentication Policy +** button to add the IKE authentication information. The IKE Authentication Policy dialog box opens.

**Step 6** Click the **Pre-Shared key** radio button or the **Digital Certificate** radio button.

**Step 7** In the IKE Authentication Policy section, click **Add Row** to add the IKE policies.

**Step 8** In the IKE Policy section, click **Add Row** and add the IKE policies. Click on the **Row** or **Field** to edit the parameters. Select the IKE policies from the list and click **Delete** to delete the IKE policies.

**Step 9** Enter the WAN IP address of the device and check the Dead Peer Detection (DPD) check box to enable DPD on all key servers, to effectively keep track of the states of other key servers.

**Step 10** In the Key Server Profile section, select the Rekey tab, and choose the Distribution method from the drop-down list. Enter the required information in the Rekey section.

**Step 11** To encrypt rekey messages, use the RSA key. You can either select the existing RSA key from the drop-down list or click the **+** button to create a new RSA key.

**Step 12** To generate an RSA key, provide the key label and modulus. Check the **Exportable** key check box, if you want to export the certificate.

**Step 13** In the Add KeyServer dialog box, select the GETVPN Traffic tab, and enter the traffic to be encrypted, the encryption policy, and anti-replay.

**Step 14** Choose the Rekey Encryption algorithm from the drop-down list to encrypt the rekey.

**Step 15** In the Key Server Profile page, click the GETVPN Traffic tab.

**Step 16** In the GETVPN Traffic dialog box, enter the Traffic to be encrypted, the encryption policy, and anti-replay.

**Step 17** Click the **Encryption Policy +** button to add the transform sets that are to be part of this encryption policy.

**Step 18** In the Migration section, check the **Enable Receive Only SA Feature** to send traffic in clear text to all group members. This feature can decrypt any arriving encrypted traffic.

**Note** After you create the template, publish it to make it available for deployment.

**Step 19** Click **Save As New Template**.

The template you created appears under My Templates.

**Step 20** Click the **Publish** icon to publish the template so it can be deployed.

For a list and descriptions of elements on the GETVPN Key Server template page, see Table 4-7.

*Table 4-7 GETVPN Key Server Template Page*

| Element | Description |
|---|---|
| **Template Basic tab** | |
| Name | Enter a name for the GETVPN group. |
| Description | (Optional) Enter a description for the GETVPN template. |
| Author | (Optional) Enter the author name. |
| **Validation Criteria tab** | |
| Device Type | Choose a device type from the drop-down list. |
| OS Version | Enter the OS version. |

*Table 4-7 GETVPN Key Server Template Page (continued)*

| Element | Description |
|---|---|
| **Template Detail** | |
| Group Name | Enter the group name for the template. |
| Group ID | Enter a unique identity for the GETVPN group. This can be a number or an IP address. The range is from 0 to 2147483647. |
| WAN IP Address | Enter the WAN IP address. |
| **IKE Authentication Policy** | |
| Authorization type | Click the **Pre-shared key** or **Digital Certificates** radio button. This is for initial IKE authorization between the key servers and group members. |
| Priority | The priority value of the IKE proposal. The priority value determines the order of the IKE proposals compared by the two negotiating peers when attempting to find a common SA. If the remote IPsec peer does not support the parameters selected in your first priority policy, the device tries to use the parameters defined in the policy with the next lowest priority number.<br>Valid values range from 1 to 10000. The lower the number, the higher the priority. |
| Encryption | Choose an encryption algorithm from the drop-down list.The encryption algorithm is used to establish the Phase 1 SA for protecting Phase 2 negotiations.<br>• AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys.<br>• AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys.<br>• AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys.<br>• DES—Encrypts according to the Data Encryption Standard using 56-bit keys.<br>• 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option. |
| Hash | The hash algorithm used in the IKE proposal. The hash algorithm creates a message digest, which is used to ensure message integrity. Options are:<br>• SHA (Secure Hash Algorithm)—Produces a 160-bit digest. SHA is more resistant to brute-force attacks than MD5.<br>• MD5 (Message Digest 5)—Produces a 128-bit digest. MD5 uses less processing time than SHA. |
| Diffie-Hellman Group | The Diffie-Hellman group to use for deriving a shared secret between the two IPsec peers without transmitting it to each other. A larger modulus provides higher security but requires more processing time. The two peers must have a matching modulus group. Options are:<br>1—Diffie-Hellman Group 1 (768-bit modulus).<br>2—Diffie-Hellman Group 2 (1024-bit modulus).<br>5—Diffie-Hellman Group 5 (1536-bit modulus, considered good protection for 128-bit keys, but group 14 is better). If you are using AES encryption, use this group (or higher). The ASA supports this group as the highest group. |

*Table 4-7 GETVPN Key Server Template Page (continued)*

| Element | Description |
|---|---|
| Lifetime | The lifetime of the SA, in seconds. When the lifetime is exceeded, the SA expires and must be renegotiated between the two peers. As a general rule, the shorter the lifetime (up to a point), the more secure the IKE negotiations will be. However, with longer lifetimes, future IPsec security associations can be set up more quickly than with shorter lifetimes.<br>You can specify a value from 60 to 86400 seconds. The default is 86400. |
| WAN IP Address | Enter the WAN IP address. |
| Dead Peer Detection | Check the Dead Peer Detection check box to enable dead peer detection for key servers to effectively keep track of their states. |
| **Accordian Pane** | |
| Distribution Method radio button | Choose a distribution method. The distribution method is used to send the rekey information from key server to group members. The options are Unicast or Multicast. |
| Multicast IP Address | When you choose Multicast as the distribution method, specify the multicast address to which the rekey must be transmitted. |
| KEK Lifetime | Enter the KEK lifetime, in seconds.The range is from 120 to 86400. |
| TEK Lifetime | Enter the TEK lifetime, in seconds. The range is from 120 to 86400. |
| Retransmit Key | Enter the frequency and duration of the rekey retransmission, in seconds. |
| RSA Key for Rekey encryption | Enter the details of the RSA key that is used to encrypt the rekey information. |
| Rekey Encryption Method | Choose the encryption algorithm from the drop-down list. The encryption algorithm is used to encrypt keys.<br>• AES-128—Encrypts according to the Advanced Encryption Standard using 128-bit keys.<br>• AES-192—Encrypts according to the Advanced Encryption Standard using 192-bit keys.<br>• AES-256—Encrypts according to the Advanced Encryption Standard using 256-bit keys.<br>• DES—Encrypts according to the Data Encryption Standard using 56-bit keys.<br>• 3DES—Encrypts three times using 56-bit keys. 3DES is more secure than DES, but requires more processing for encryption and decryption. It is less secure than AES. A 3DES license is required to use this option. |
| **GETVPN Traffic** | |
| Traffic to encrypt | (Optional) Choose an ACL name from the drop-down list that corresponds to the traffic to be encrypted. The access list defines the traffic to be encrypted. Only the traffic that matches the “permit” lines will be encrypted.<br>**Note** Be sure not to encrypt certain traffic that should always be permitted even if the encrypted sessions are not up. |
| Encryption Policy | Choose the transform sets from the drop-down list that should be used to encrypt the traffic. Add the transform set from the table, which is used to encrypt traffic between the peers.<br>From the drop-down list, choose transform sets for encrypting traffic. From the table, add another transform set for encrypting traffic between peers. |
| Anti Replay | Choose the time-based or counter-based anti-replay option. |

*Table 4-7 GETVPN Key Server Template Page (continued)*

| Element | Description |
|---|---|
| **Migration** | |
| Enable Receive Only SA feature | Check the **Enabling Receive Only SA feature** check box to send the traffic in clear text, while retaining the capability to decrypt any arriving encrypted traffic. |

# Deploying GETVPN Templates

This task enables you to deploy the GETVPN group member and key server template.

**Note** Before you can deploy your template to devices, you must publish the template.

To deploy the GETVPN template:

**Step 1** Choose **Deploy > Configuration Tasks > My Templates.**

**Step 2** On the My Templates page, select the **GETVPN-GroupMember or KeyServer** template, and click the **Tasked View** button.

**Step 3** From the Deploy Task Pad, click **Deploy**.

The Template Deployment page opens.

**Step 4** From the Device Selection section, select the device and the location.

**Step 5** In the Value Assignment section, click the radio button to select the device.

**Step 6** For GETVPN-GroupMember, you can change the values for Registration Interface, Enable Passive SA, Local Exception Policy ACL, and Fail Close ACL.

**Step 7** For GETVPN Key Server, you can change the values for Keyserver, WAN IP Address, ACL, Priority, and Cooperative servers.

**Step 8** If you changed the values, click **Apply**. For elements on the page, refer to Table 4-6 and Table 4-7.

**Step 9** Click the Schedule section, enter the Job Name, then click one of the following radio buttons:

- **Run**—To run the job immediately.
- **Run at Schedule Time**—To specify a time to run the job.

**Step 10** Under Summary, verify your entries, then click **OK**.

# Importing and Deploying a Configuration Template

In addition to creating new configuration templates, you can import configurations from Cisco Prime LAN Management Solution (LMS). If you have “golden” templates in Cisco Prime LMS, you can import those configurations into Prime NCS (WAN) and save them as configuration templates that you can deploy to the devices in your network.

Before you import a configuration, you must first export and save the configuration from Cisco Prime LMS.

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

**Step 2** Expand the **CLI Template folder**, then choose the **CLI** template.

**Step 3** Click the **Import** icon at the top right of the CLI template page.

**Step 4** Browse to the configuration .xml file that you previously exported from Cisco Prime LMS, then click **OK**.

**Step 5** Navigation to the My Templates folder and choose the configuration you imported.

**Step 6** To view the contents of the configuration, click the **CLI Content** tab.

To view the parameters defined in the configuration, click the **Form View** tab. These values are read-only.

To change any of the variables defined in the configuration, click **Manage Variables**.

**Step 7** Click the **Publish** icon to publish the template so it can be deployed.

**Step 8** Click the **Go to Deployment** icon and go to the **Deploy > Configuration Tasks** page.

**Step 9** Click **Deploy** on the template you published.

**Step 10** Specify the deployment options as explained in Specifying Template Deployment Options.

**Step 11** Click **OK**.

# Troubleshooting Template Deployment

The most common reasons that a template might not be deployed are:

- One or more devices are unreachable—Verify that the device credentials are correct; ping the device to verify that it is reachable. (See Using 360° View for more information.)
- A device CLI returned an error because the CLI was incorrect—Verify that the CLI commands contained in the template are correct by running the commands on a test device.