



## Setup Wizards

---

CVDM-VPNSM allows you to set up VPN module features with the help of wizards, which simplifies complex configuration tasks.

CVDM-VPNSM provides the following Setup wizards:

- **Site-to-Site VPN Connection Setup wizard**—This wizard allows you to create and configure a site-to-site VPN. See [Using the Site-to-Site VPN Connection Setup Wizard, page 2-1](#).
- **Secure GRE Tunnel Setup wizard**—This wizard allows you to create a secure GRE tunnel on the device for protected traffic flow. See [Using the Secure GRE Tunnel Setup Wizard, page 2-12](#).
- **Remote Access Server Setup wizard**—This wizard allows you to create and configure a remote access server connection. See [Using the Remote Access Server Setup Wizard, page 2-18](#).

## Using the Site-to-Site VPN Connection Setup Wizard

The Site-to-Site VPN Connection Setup wizard allows you to create a secure site-to-site VPN and configure settings for it, such as crypto connections, IKE policy information, and policies for protecting the traffic flowing on the connection.

For more information about site-to-site VPNs, see [Chapter 3, “Site-to-Site VPN Configuration.”](#)

- 
- Step 1** Click **Setup** at the top of the window and click **Wizard** in the left-most pane. The main VPN Wizard page appears.
  - Step 2** Select the Site-to-Site VPN Connection radio button.
  - Step 3** Click **Launch the Selected Task**.
-

## Configuring the Crypto Connection

In Step 1 of the Site-to-Site VPN Connection Setup wizard, you create a crypto connection between the device and the peer. CVDM-VPNSM automatically detects the inside and outside VLANs.

For more information about configuring crypto connections for site-to-site VPNs, see [Configuring Crypto Connections, page 3-2](#).



### Note

You can click the **Advance...** button to display the Add Crypto Connection dialog box. This dialog box provides more detailed options for defining a crypto connection. For more information, see [Add Crypto Connection Dialog Box, page 2-4](#).

To create a crypto connection using the fields on this page, define the following.


GUI Element	Action/Description
VPN Module list or field	Select, from the list, the slot on the device where the VPN module is located (if there are multiple VPN modules in the chassis).  If there is only one VPN module in the chassis, the VPN Module field displays the slot on the device where the VPN module is located. You cannot edit this field.
<b>IP Address pane</b>	
IP address field	Enter the IP address of the interface VLAN, which is the Layer 3 VLAN that contains only the VPN module inside port. This IP address is used by the remote peer to connect to this site.  <b>Note</b> The interface VLAN is removed from all trunk ports on the switch.
Mask list	Select, from the list, the subnet mask address of the interface VLAN.

GUI Element	Action/Description
<b>VPN Outside Interface pane</b>	
Available Ports Table	<p>Select the VPN outside interface. The outside interface is used to connect to the device. You can only select one port. If you require additional ports, you must add and configure a site-to-site VPN from the <b>Setup &gt; Site-to-Site</b> page. For more information, see <a href="#">Chapter 3, “Configuring Site-to-Site VPNs.”</a></p> <p>This table contains the port selector, which allows you to select ports. For more information, see <a href="#">Port Selector, page 3-9</a>.</p>
Advance... button	<p>Click to display the Add Crypto Connection dialog box. This dialog box provides more detailed options for defining a crypto connection. For more information, see <a href="#">Add Crypto Connection Dialog Box, page 2-4</a>.</p>

## Add Crypto Connection Dialog Box

This dialog box provides more detailed options for configuring your crypto connection.

Define the following.


GUI Element	Action/Description
<b>VPN Inside Interface pane</b>	
Interface VLAN field	<p>Specify the interface VLAN, which is the Layer 3 VLAN that contains only the VPN module inside port.</p> <p><b>Note</b> The interface VLAN is removed from all trunk ports on the switch.</p> <p>You can create a VLAN or select from an available VLAN.</p> <p>Click  and do one of the following:</p> <ul style="list-style-type: none"> <li>• Select <b>Select VLAN</b> to open the VLAN Selector dialog box. See <a href="#">VLAN Selector, page 3-9</a> for more information.</li> <li>• Select <b>Create VLAN</b> to open the Create VLAN dialog box. See <a href="#">Create VLAN Dialog Box, page 3-9</a> for more information.</li> </ul> <p>You can select <b>Clear VLAN</b> to clear the VLAN that is specified in this field.</p>
IP Address field	Enter the IP address of the interface VLAN.
Mask list	Select the subnet mask of the interface VLAN from the list or enter it in the field.

GUI Element	Action/Description
VPN Outside Interface pane	
Connection Mode radio button	<p>Specify the connection mode; you can select the Access/Trunk radio button to specify an access port or trunk port as the outside port, or you can select the Routed Port radio button to specify a routed port as the outside port.</p> <p>If you select the Access/Trunk radio button, do the following:</p> <ol style="list-style-type: none"> <li>Specify an outside VLAN. You can create a VLAN or choose an available VLAN. From the Outside VLAN field, click <input type="button" value="▽..."/> and do one of the following: <ul style="list-style-type: none"> <li>Select <b>Select VLAN</b> to open the VLAN Selector dialog box. See <a href="#">VLAN Selector, page 3-9</a> for more information.</li> <li>Select <b>Create VLAN</b> to open the Create VLAN dialog box. See <a href="#">Create VLAN Dialog Box, page 3-9</a> for more information.</li> </ul> <p>You can select <b>Clear VLAN</b> to clear the VLAN that is specified in this field.</p> </li> <li>Specify the VPN Outside interface from the Port Selector in Step 1 of the Site-to-Site VPN Wizard page. For more information, see <a href="#">Configuring the Crypto Connection, page 2-3</a>.</li> </ol> <p>If you select the Routed Port radio button, you must select a routed port. From the Routed Port field, click <input type="button" value="..."/> to open the Select Routed Ports dialog box. For more information, see <a href="#">Select Routed Port Dialog Box, page 3-12</a>.</p>

## Configuring IKE Information (Optional)

In Step 2 of the Site-to-Site VPN Connection Setup wizard, you configure your Internet Key Exchange (IKE) information. For more information about configuring IKE settings, see [Configuring IKE Settings, page 5-53](#).

Define the following.

GUI Element	Action/Description
Add New IKE Policy check box	<p>Select this check box to create a new IKE policy. Then, edit the appropriate values:</p> <ul style="list-style-type: none"> <li>Priority field—Enter the IKE policy priority value. Each policy is uniquely identified by the priority number you assign. The range of values is 1 to 10000.</li> <li>Encryption list—Select, from the list, the protocol to be used for encrypting data. Available values are DES, 3DES, AES_128, AES_192, and AES_256.</li> <li>Hash list—Select, from the list, the hash algorithm to be used (MD5 of SHA_1).</li> <li>Authentication—Select, from the list, the method used for authenticating data (PRE_SHARE). CVDM-VPNSM supports only preshared keys.</li> <li>D-H Group list—Select, from the list, the Diffie-Hellman (D-H) group for the policy. Value can be group1, group2, or group5.</li> </ul> <p>A D-H key is an algorithm that allows two VPN peers who have agreed to policies to exchange information over untrusted and unencrypted networks and develop a shared key.</p>
View Existing IKE Policies button	Select to view the IKE policies that are configured. Click  to open the IKE policy dialog box. See <a href="#">IKE Policy List Dialog Box, page 2-7</a> for more information.

## IKE Policy List Dialog Box

This dialog box can be launched from several pages and contains information about your configured IKE policies. This dialog box contains a table that displays the following information:

Column	Description
Priority	IKE policy priority value; this value uniquely identifies the policy. The range of values is 1 to 10000.
Encryption	Protocol used for encrypting data (DES, 3DES, AES, AES_128, AES_192, and AES_256).
Hash	Hash algorithm used (MD5 or SHA_1).
D-H Group	D-H group used (group1, group2, or group5).

Column	Description
Authentication	Algorithm used for authenticating data (PRE_SHARE).
Lifetime	Lifetime, in seconds, before the security association (SA) between the device and the peer expires. When the SA expires, the IPSec tunnel between the devices is deleted. The range of values is 60 to 86400.

## Configuring Remote Peer Information

In Step 3 of the Site-to-Site VPN Connection Setup wizard, you configure a peer whose IP address is the address of the remote site. You also configure a preshared key for the remote peer for IKE authentication.

Preshared keys allow for one or more peers to use individual shared secrets to authenticate encrypted tunnels to a gateway. The same preshared key must be set on the remote peer and any other participating peers.

Define the following.

GUI Element	Action/Description
<b>Peer Information pane</b>	
Peer IP Address field	Enter the IP address of the peer.
Preshared Key field	Enter the preshared key used for the peers. If a preshared key has previously been configured for the peer, this field is populated with that information, and you cannot edit this field.
Reenter Preshared Key field	Re-enter the preshared key used for the peers.
Add>> button	After entering a peer IP address, click to add to the <a href="#">Peer List table</a> .
<<Remove button	To remove an entry from the <a href="#">Peer List table</a> , select the entry and click << <b>Remove</b> .
Peer List table	Displays all peers participating in the VPN tunnel.

## Configuring a Transform Set

In Step 4 of the Site-to-Site VPN Connection Setup wizard, you configure the transform set that will be used to protect the traffic on this network. A transform set is a combination of security protocols, algorithms, and other settings to apply to IPSec-protected traffic. In this step, you can select from available transform sets or create a new one. For more information on transform sets, see [Configuring Transform Sets, page 5-47](#).

Define the following.

GUI Element	Action/Description
Create New Transform Set radio button	<p>Select this radio button to create a new transform set. Then, edit the appropriate values.</p> <ul style="list-style-type: none"> <li>• Create New Transform Set field—Enter a name for the transform set.</li> <li>• Encryption (ESP)—Select the ESP protocol (DES, 3DES, Null, AES, AES-192, or AES-256) used for encrypting data. Use ESP encryption when ESP authentication is selected.</li> <li>• Authentication (ESP)—Select the ESP algorithm (SHA or MD5) used for ensuring data integrity.</li> </ul> <p><b>Note</b> Tunnel mode is the default mode for the VPN tunnel. In tunnel mode, both the data sent by VPN clients and the inside IP address of the client are encrypted.</p>
Use Existing Transform Set radio button	<p>Select this radio button to select from available transform sets. Then, click <input type="button" value="..."/> to open the Transform Set List dialog box. See <a href="#">Transform Set List Dialog Box, page 2-9</a> for more information.</p>

### Transform Set List Dialog Box

This dialog box can be launched from several pages and contains information about your configured transform sets. It contains a table that displays the following information:

Column	Description
Name	Name of the transform set.
ESP Encryption	ESP protocol (DES, 3DES, Null, AES, AES-192, or AES-256) used for data encryption.
ESP Authentication	ESP algorithm (SHA or MD5) used for data authentication.
AH Authentication	AH algorithm (SHA or MD5) used for data authentication. AH allows for data integrity, but it does not offer data encryption.
Mode	Method of data transport (tunnel or transport). In tunnel mode, both the data sent by VPN clients and the inside IP address of the client are encrypted. In transport mode, only the data sent by VPN clients is encrypted.

## Configuring Traffic to Be Protected

In Step 5 of the Site-to-Site VPN Connection Setup wizard, you specify how the traffic on the VPN is protected. You can specify the subnets on which all traffic is protected, or you can specify an IPSec rule to be used for protecting traffic.

Define the following.

GUI Element	Action/Description
Protect all traffic between the following subnets radio button	<p>Select this radio button to specify two subnets between which traffic is protected. Only traffic between the source and destination on the tunnel is protected. Then, do the following:</p> <ul style="list-style-type: none"> <li>• In the Local Site pane, specify the local site from which the protected traffic originates. Then: <ul style="list-style-type: none"> <li>– In the IP Address field, enter the IP address of the source.</li> <li>– From the Subnet list, select the subnet mask address of the source.</li> </ul> </li> <li>• In the Remote Site pane, specify the remote site on which protected traffic terminates. Then: <ul style="list-style-type: none"> <li>– In the IP Address field, enter the IP address of the destination.</li> <li>– From the Subnet list, select the subnet mask address of the destination.</li> </ul> </li> </ul> <p>CVDM-VPNSM automatically creates the rule that permits all IP traffic from the local site network to the remote site network.</p>
Protect traffic specified by IPsec rule radio button	<p>Select this radio button to specify an IPsec rule to be applied for traffic protection. Click <input type="button" value="▽..."/> and select <b>Select ACL...</b> to select from available IPsec rules. The Select a Rule dialog box appears. See <a href="#">Select a Rule Dialog Box, page 2-11</a> for more information.</p> <p>You can also clear the entry in this field by selecting <b>Clear Selection...</b></p> <p>For more information about IPsec rules, see <a href="#">Configuring Access and IPsec Rules, page 5-33</a>.</p>

## Select a Rule Dialog Box

This dialog box can be launched from several pages and allows you to select an IPsec rule. It displays the following information.

GUI Element	Action/Description
Rule Type list	Select, from the list, the type (IPSec Rules or Default Rules) of rule. Default rules are those that have been preconfigured on the CVDM-VPNSM application. If you select a default rule for use, CVDM-VPNSM copies the default rule and creates a new IPSec rule from that copy.
<b>IPSec Rules pane</b>	
Name/Number	Name and number of the IPSec rule.
Used by	Crypto maps on which the rule is applied.
<b>Details pane</b>	
Rule Entry column	Displays the name of the IPSec rule entries configured on the selected IPSec rule.

## Site-to-Site VPN Connection Setup Wizard Summary

The summary page of the wizard shows you the information that you entered.

Click **Finish** to send the commands to the device. The Deliver Configuration to Switch/Module(s) dialog box appears if you have configured CVDM-VPNSM to display the accumulated CLI commands after you have completed a wizard (for information on configuring this option, see [Editing Preferences, page 1-19](#)).

For more information on the Deliver Configuration to Switch/Module(s) dialog box, see [Delivering CLI Commands to the Device, page 1-22](#).

## Using the Secure GRE Tunnel Setup Wizard

In the Secure GRE Tunnel Setup wizard, you create and configure secure GRE tunnels between your device and a remote peer. Generic routing encapsulation (GRE) is a tunneling protocol that can encapsulate different protocol packet types inside encrypted IP packets. The device and the peer must be configured with the same information for the GRE tunnel to work.

For more information about GRE tunnels, see [Configuring GRE Tunnels, page 3-19](#).

- 
- Step 1** Click **Setup** at the top of the window and click **Wizard** in the left-most pane. The main VPN Wizard page appears.
  - Step 2** Select the Configure Secure GRE Tunnel radio button.
  - Step 3** Click **Launch the Selected Task**.
- 

## Configuring the Crypto Connection

In Step 1 of the Secure GRE Tunnel Setup wizard, you configure a crypto connection between the device and the peer. For more information on crypto connections, see [Configuring Crypto Connections, page 3-2](#).



### Note

You can click the **Advance...** button to display the Add Crypto Connection dialog box. This dialog box provides more detailed options for defining a crypto connection. For more information, see [Add Crypto Connection Dialog Box, page 2-4](#).

---

To create a crypto connection using the fields on this page, define the following.

GUI Element	Action/Description
VPN Module list	<p>Select, from the list, the slot on the device where the VPN module is located (if there are multiple VPN modules in the chassis).</p> <p>If there is only one VPN module in the chassis, the VPN Module field displays the slot on the device where the VPN module is located. You cannot edit this field.</p>
<b>IP Address pane</b>	
IP address field	<p>Enter the IP address of the interface VLAN, which is the Layer 3 VLAN that contains only the VPN module inside port. This IP address is used by the remote peer to connect to this site.</p> <p><b>Note</b> The interface VLAN is removed from all trunk ports on the switch.</p>
Mask list	Enter the subnet mask address of the interface VLAN.
<b>VPN Outside Interface pane</b>	
Available Ports Table	<p>Select the VPN outside interface. The outside interface is used to connect to the device. You can only select one port. If you require additional ports, you must add and configure a site-to-site VPN from the <b>Setup &gt; Site-to-Site</b> page. For more information, see <a href="#">Chapter 3, “Configuring Site-to-Site VPNs.”</a></p> <p>This table contains the port selector, which allows you to select ports. For more information, see <a href="#">Port Selector, page 3-9</a>.</p>
Advance... button	Click to display the Add Crypto Connection dialog box. This dialog box provides more detailed options for defining a crypto map. For more information, see <a href="#">Add Crypto Connection Dialog Box, page 2-4</a> .

## Configuring Tunnel Parameters

In Step 2 of the Secure GRE Tunnel Setup wizard, you define the parameters for the GRE tunnel. For more information about GRE tunnels, see [Configuring GRE Tunnels, page 3-19](#).

Define the following:


GUI Element	Action/Description
<b>Tunnel Parameters pane</b>	
IP Address field	Enter the IP address of the tunnel source.
Mask list	Select, from the list, the subnet mask of the tunnel source.
Keepalive field	Optionally, enter the tunnel keepalive value, in seconds; this is the number of seconds that the device waits between sending keepalive packets on the tunnel.  The default value is 10. The range of values you can use is 0 to 32767.
MTU field	Optionally, enter the maximum transmission unit (MTU) value, in bytes, of the data packets that can be sent on the tunnel.  The default value is 1514. The range of values you can use is 256 to 1000000.
Destination Address field	Enter the IP address of the tunnel destination.
<b>Static Routing pane</b>	
IP Address field	Optionally, enter the IP address of the network destination for the static route through this tunnel.
Mask list	Optionally, select, from the list, the subnet mask address of the network destination for the static route through this tunnel.

GUI Element	Action/Description
<b>IPSec Authentication pane</b>	
Preshared Key field	Enter the preshared key for the tunnel destination IP address. The tunnel destination is used as the peer IP address.
Reenter Preshared Key field	Re-enter the preshared key for the tunnel destination IP address.

## Configuring IKE Information (Optional)

In Step 3 of the Secure GRE Tunnel Setup wizard, you configure your Internet Key Exchange (IKE) information. For more information about configuring IKE settings, see [Configuring IKE Settings, page 5-53](#).

Define the following.

GUI Element	Action/Description
Add New IKE Policy check box	<p>Select this check box to create a new IKE policy. Then, edit the appropriate values:</p> <ul style="list-style-type: none"> <li>• Priority field—Enter the IKE policy priority value. Each policy is uniquely identified by the priority number you assign. The range of values is 1 to 10000.</li> <li>• Encryption list—Select, from the list, the protocol to be used for encrypting data. Available values are DES, 3DES, AES_128, AES_192, and AES_256.</li> <li>• Hash list—Select, from the list, the hash algorithm to be used (MD5 or SHA_1).</li> <li>• Authentication—Select, from the list, the method used for authenticating data (PRE_SHARE). CVDM-VPNSM supports only preshared keys.</li> <li>• D-H Group list—Select, from the list, the Diffie-Hellman (D-H) group for the policy. Value can be group1, group2, or group5.</li> </ul> <p>A D-H key is an algorithm that allows two VPN peers who have agreed to policies to exchange information over untrusted and unencrypted networks and develop a shared key.</p>
View Existing IKE Policies button	Select to view the IKE policies that are configured. Click  to open the IKE policy dialog box. See <a href="#">IKE Policy List Dialog Box, page 2-7</a> for more information.

## Configuring a Transform Set

In Step 4 of the Secure GRE Tunnel Setup wizard, you configure the transform set that will be applied to the traffic flowing on this tunnel. A transform set is a combination of security protocols, algorithms, and other settings to apply to IPsec protected traffic. In this step, you can select from available transform sets or create a new one. For more information on transform sets, see [Configuring Transform Sets, page 5-47](#).

Define the following.

GUI Element	Action/Description
Create New Transform Set radio button	<p>Select this radio button to create a new transform set. Then, edit the appropriate values.</p> <ul style="list-style-type: none"> <li>• Create New Transform Set field—Enter a name for the transform set.</li> <li>• Encryption (ESP)—Select the ESP protocol (DES, 3DES, Null, AES, AES-192, or AES-256) used for encrypting data. Use ESP encryption when ESP authentication is selected.</li> <li>• Authentication (ESP)—Select the ESP algorithm (SHA, or MD5) used for ensuring data integrity.</li> </ul> <p><b>Note</b> Transport mode is the default mode for the GRE tunnel. In transport mode, only the data sent by VPN clients is encrypted.</p>
Use Existing Transform Set radio button	<p>Select this radio button to select from available transform sets. Then, click <input type="button" value="..."/> to open the Transform List dialog box. See <a href="#">Transform Set List Dialog Box, page 2-9</a> for more information.</p>

After you have made your configurations in the Secure GRE Tunnel Setup wizard, CVDM-VPNSM creates IPsec rules that protect the traffic flowing from an interface IP address and terminating on a tunnel destination IP address.

## Secure GRE Tunnel Setup Wizard Summary

The summary page of the wizard shows you the information that you entered.

Click **Finish** to send the commands to the device. The Deliver Configuration to Switch/Module(s) dialog box appears if you have configured CVDM-VPNSM to display the accumulated CLI commands after you have completed a wizard (for information on configuring this option, see [Editing Preferences, page 1-19](#)).

For more information on the Deliver Configuration to Switch/Module(s) dialog box, see [Delivering CLI Commands to the Device, page 1-22](#).

## Using the Remote Access Server Setup Wizard

In the Remote Access Server Setup wizard, you configure the settings for the server that establishes and manages secure connections between remote users and this device.

For more information about configuring remote access connections, see [Chapter 4, “Remote Access Configuration.”](#)

- 
- Step 1** Click **Setup** at the top of the window and click **Wizards** in the left-most pane. The main VPN Wizard page appears.
  - Step 2** Select the Configure Remote Access Server radio button.
  - Step 3** Click **Launch the Selected Task**.
- 

## Configuring Connection Parameters

In Step 1 of the Remote Access Server Setup wizard, you configure the connection a remote device will use to establish a VPN connection with the module. For more information on crypto connection configuration, see [Configuring Crypto Connections, page 4-2](#).

**Note**

You can click the **Advance...** button to display the Add Crypto Connection dialog box. This dialog box provides more detailed options for defining a crypto connection. For more information, see [Add Crypto Connection Dialog Box, page 2-4](#).

To create a crypto connection using the fields on this page, define the following.


GUI Element	Action/Description
VPN Module list or field	<p>Select, from the list, the slot on the device where the VPN module is located (if there are multiple VPN modules in the chassis).</p> <p>If there is only one VPN module in the chassis, the VPN Module field displays the slot on the device where the VPN module is located. You cannot edit this field.</p>
<b>IP Address pane</b>	
IP Address field	<p>Enter the IP address of the interface VLAN, which is the Layer 3 VLAN that contains only the VPN module inside port. This IP address is used by the remote peer to connect to this site.</p> <p><b>Note</b> The interface VLAN is removed from all trunk ports on the switch.</p>
Mask list	Select, from the list, the subnet mask address of the interface VLAN.

GUI Element	Action/Description
<b>VPN Outside Interface pane</b>	
Available Ports Table	<p>Select the VPN outside interface. The outside interface is used to connect to the device. You can only select one port. If you require additional ports, you must add and configure a remote access VPN from the <b>Setup &gt; Remote Access</b> page. For more information, see <a href="#">Chapter 4, “Remote Access Configuration.”</a></p> <p>This table contains the port selector, which allows you to select ports. For more information, see <a href="#">Port Selector, page 3-9.</a></p>
Advance... button	<p>Click to display the Add Crypto Connection dialog box. This dialog box provides more detailed options for defining a crypto connection. For more information, see <a href="#">Add Crypto Connection Dialog Box, page 2-4.</a></p>

## Configuring IKE Policies

In Step 2 of the Remote Access Server Setup wizard, you configure your Internet Key Exchange (IKE) information. For more information about configuring IKE settings, see [Configuring IKE Settings, page 5-53.](#)

Define the following.

GUI Element	Action/Description
Add New IKE Policy check box	<p>Select this check box to create a new IKE policy. Then, edit the appropriate values:</p> <ul style="list-style-type: none"> <li>• Priority field—Enter the IKE policy priority value. Each policy is uniquely identified by the priority number you assign. The range of values is 1 to 10000.</li> <li>• Encryption list—Select, from the list, the protocol to be used for encrypting data. Available values are DES, 3DES, AES_128, AES_192, and AES_256.</li> <li>• Hash list—Select, from the list, the hash algorithm to be used (MD5 or SHA_1).</li> <li>• Authentication—Select, from the list, the method used for authenticating data (PRE_SHARE). CVDM-VPNSM supports only preshared keys.</li> <li>• D-H Group list—Select, from the list, the Diffie-Hellman (D-H) group for the policy. Value can be group1, group2, or group5.</li> </ul> <p>A D-H key is an algorithm that allows two VPN peers who have agreed to policies to exchange information over untrusted and unencrypted networks and develop a shared key.</p>
View Existing IKE Policies button	<p>Select to view the IKE policies that are configured. Click  to open the IKE policy dialog box. See <a href="#">IKE Policy List Dialog Box, page 2-7</a> for more information.</p>

## Configuring Transform Sets

In Step 3 of the Remote Access Server Setup wizard, you configure the transform set that will be used to protect the traffic on this network. A transform set is a combination of security protocols, algorithms, and other settings to apply to IPSec-protected traffic. In this step, you can select from available transform sets or create a new one. For more information on transform sets, see [Configuring Transform Sets, page 5-47](#).



### Note

By default, the configured transform set runs in tunnel mode.

Define the following.

GUI Element	Action/Description
Create New Transform Set radio button	<p>Select this radio button to create a new transform set. Then, edit the appropriate values.</p> <ul style="list-style-type: none"> <li>• Create New Transform Set field—Enter a name for the transform set.</li> <li>• Encryption (ESP)—Select the ESP protocol (DES, 3DES, Null, AES, AES-192, or AES-256) used for encrypting data. Use ESP encryption when ESP authentication is selected.</li> <li>• Authentication (ESP)—Select the ESP algorithm (SHA or MD5) used for ensuring data integrity.</li> </ul> <p><b>Note</b> Tunnel mode is the default mode for the VPN tunnel. In tunnel mode, both the data sent by VPN clients and the inside IP address of the client are encrypted.</p>
Use Existing Transform Set radio button	<p>Select this radio button to select from available transform sets. Then, click <input type="button" value="..."/> to open the Transform Set List dialog box. See <a href="#">Transform Set List Dialog Box, page 2-9</a> for more information.</p>

## Configuring Group Policies

In Step 4 of the Remote Access Server Setup wizard, you configure the parameters for a new group policy.



### Note


This step is optional if a group policy has already been configured for the remote access server and a local database has not been selected for authorization purposes.

Define the following.

GUI Element	Action/Description
Create a New Group Policy check box	Select to enable the fields in this page of the wizard.
Group Name field	Enter a name for the new group policy.
Key field	Enter the key used to communicate with the device.
Confirm Key field	Re-enter the key used to communicate with the device.
Create a new pool radio button	Select to create a new IP address pool. In the IP Address Range fields, enter the IP addresses that begin and end the desired address range.
Select from an existing pool radio button	Select this radio button to select an IP address pool that has already been configured on the device. See <a href="#">Selecting an IP Pool, page 2-24</a> for more information.
View Group Policies button	Click to launch the List of Group Policies dialog box. See <a href="#">Viewing Group Policy Information, page 2-24</a> for more information.

## Selecting an IP Pool

From this dialog box, you can assign an IP pool to a new group policy by selecting one from the list of IP pools that have already been configured on the device.

- 
- Step 1** In Step 4 of the Remote Access Server Setup wizard, select the Select from an existing pool radio button.
- Step 2** Click  to launch the Select an IP Pool dialog box.
- Step 3** Select an IP pool and click **OK**.
- 

## Viewing Group Policy Information

From the List of Group Policies dialog box, you can view detailed information about the group policies that have already been configured on the device. The following information is provided.

GUI Element	Action/Description
<b>Group Policies pane</b>	
Name column	Name of a group policy.
Address Pool column	Name of the address pool associated with a group policy.
Key column	Preshared key used for group policy attribute definition.
Domain Name column	Name of the domain to which a group policy belongs.
Split Tunnel ACL column	IPSec rule to be applied for traffic protection.
DNS column	DNS servers associated with a group policy. <b>Note</b> You can specify up to two DNS servers.

GUI Element	Action/Description
<b>Details: X pane</b>	
Access Restrict field	Indicates the interfaces that clients in the group policy are restricted from accessing.
Group Lock field	Indicates whether the group lock feature is enabled. By default, the feature is disabled.
WINS field	IP address of the group policy's WINS server.
Max. Users per Group field	Maximum number of users in a group.
Max. Logins per User field	Maximum number of logins for users in a group.
Split DNS field	Indicates the IPSec rule to be applied for traffic protection.
Backup Server(s) field	IP address of the group's backup gateway.
Firewall, Are You There? field	Indicates whether the Firewall Are-You-There attribute, which restricts VPN connections to clients running Black Ice or Zone Alarm personal firewalls, is enabled. By default, the feature is disabled.
Save Password field	Indicates whether extended authentication usernames and passwords are saved locally on your Easy VPN client. By default, the feature is disabled.
Include Local LAN field	Indicates whether the Include-Local-LAN attribute, which allows a non-split tunneling connection to access the local subnet at the same time as the client, is enabled. By default, the feature is disabled.

GUI Element	Action/Description
Perfect Forwarding Secrecy (PFS) field	Indicates whether Perfect Forwarding Secrecy (PFS) is enabled.  <b>Note</b> By default, the feature is disabled.  PFS is a property of some asymmetric key agreement protocols that allows for the use of different keys at different times during a session. This ensures that the compromising of any single key will not compromise the session as a whole.
Address Pool field	Name of the address pool configured for a group policy.
Cache Size field	Number of IP addresses that an address pool's cache contains.
Start IP Address column	Lowest IP address in an address range configured for an address pool.
End IP Address column	Highest IP address in an address range configured for an address pool.

## Configuring RADIUS Servers

In Step 5 of the Remote Access Server Setup wizard, you configure the parameters for a new Remote Authentication Dial-In User Service (RADIUS) server. This server handles authentication, authorization, and accounting (AAA) for remote users who want to access the module.



### Note

This step is optional if either a RADIUS server has already been configured or a RADIUS server is not used for AAA.

Define the following.

GUI Element	Action/Description
Create a new RADIUS Server check box	Select to enable the fields in this page of the wizard.
IP Address field	Enter the IP address of the RADIUS server.
Type field	Indicates that you are configuring a RADIUS server. This field cannot be edited.
Key field	Enter the key used to communicate with the server.
Confirm Key field	Re-enter the key used to communicate with the server.
Accounting Port field	Enter the server port used for accounting requests. The default is 1646.
Authentication Port field	Enter the server port used for authentication requests. The default is 1645.
Timeout (sec) field	Enter the number of seconds that the router should attempt to contact this server before going on to another server. The default is 5 seconds.
View RADIUS Servers button	Click to launch the List of Servers dialog box. See <a href="#">Viewing RADIUS Server Information, page 2-27</a> for more information.

## Viewing RADIUS Server Information

From the List of Servers dialog box, you can view detail information for the RADIUS servers that have already been configured on the device. The following information is provided.

Column	Description
IP Address	IP address of the AAA server.
Authentication Port	Server port used for authentication requests. The default is 1645.
Accounting Port	Server port used for accounting requests. The default is 1646.
Key	Key used when contacting the AAA server.
Timeout (sec)	Number of seconds that the router should attempt to contact this server before going on to the next server in the group list. The default is 5 seconds.
Type	The type of server. Only the RADIUS option is supported.


## Configuring Group Policy Lookup

In Step 6 of the Remote Access Server Setup wizard, you select one of the methods described in the following table for the lookup of group policies.

GUI Element	Action/Description
Use local database of group policies for lookup radio button	Select to look into the local database for group authorization.
Use RADIUS and local database of group policies for lookup radio button	Select to first look into the RADIUS server and then the local database for group authorization.
Use existing list, whose methods will be used for lookup radio button	Select to use an existing list for group authorization. <ol style="list-style-type: none"> <li>Click <input type="button" value="..."/> to launch the Select an Authorization List dialog box.</li> <li>Select a list and then click <b>OK</b>.</li> </ol>

## Configuring Extended Authentication

In Step 7 of the Remote Access Server Setup wizard, you select one of the Extended Authentication (Xauth) methods described in the following table.

GUI Element	Action/Description
Use RADIUS and local database for Xauth radio button	Select to first look into the RADIUS server and then the local database for group authentication.
Use local database for Xauth radio button	Select to look into the local database for group authentication.
Use existing list, whose methods will be used for Xauth radio button	Select to use an existing list for group authentication. <ol style="list-style-type: none"> <li>1. Click  to launch the Select an Authentication List dialog box.</li> <li>2. Select a list and then click <b>OK</b>.</li> </ol>
Configure Xauth User button	Click to launch the Add Xauth User dialog box. See <a href="#">Adding an Xauth User, page 2-30</a> for more information.

## Adding an Xauth User

In this dialog box, you can configure the parameters for a new Extended Authentication (Xauth) user.

**Step 1** In Step 7 of the Remote Access Server Setup wizard, click **Configure Xauth User**.

**Step 2** Define the following:

GUI Element	Action/Description
Username field	Enter the username for a new Xauth user.
Privilege Level list	Select the privilege level for the new Xauth user. Privilege levels range from 0 to 15, where 15 is the highest level.
Password field	Enter the password for the new Xauth user.
Confirm Password field	Re-enter the password for the new Xauth user.
Encrypt Password check box	Select to encrypt the password configured for the Xauth user.

**Step 3** Click **OK**.

## Configuring Accounting Information

In Step 8 of the Remote Access Server Setup wizard, you select one of the methods described in the following table for the accounting of network-related service requests.

GUI Element	Action/Description
No accounting is needed radio button	Select to disable accounting. <b>Note</b> By default, this option is selected.
Use RADIUS for accounting radio button	Select to use the RADIUS server configured in Step 5 of the wizard for accounting purposes.
Use existing list, whose methods will be used for accounting radio button	Select this radio button to select an accounting list that has already been configured on the device. <ol style="list-style-type: none"> <li>1. Click <input type="text" value="..."/> to launch the Select an Accounting List dialog box.</li> <li>2. Select an accounting list and then click <b>OK</b>.</li> </ol>

## Remote Access Server Wizard Summary

The summary page of the wizard shows you the information that you entered.

Click **Finish** to send the commands to the device. The Deliver Configuration to Switch/Module(s) dialog box appears if you have configured CVDM-VPNSM to display the accumulated CLI commands after you have completed a wizard (for information on configuring this option, see [Editing Preferences, page 1-19](#)).

For more information on the Deliver Configuration to Switch/Module(s) dialog box, see [Delivering CLI Commands to the Device, page 1-22](#).

