Router Device Administration

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

This chapter contains the following topics:

- AAA on Cisco IOS Routers , on page 2
- AAA Policy Page , on page 6
- User Accounts and Device Credentials on Cisco IOS Routers , on page 14
- Accounts and Credentials Policy Page , on page 16
- Bridging on Cisco IOS Routers , on page 19
- Bridging Policy Page , on page 21
- Time Zone Settings on Cisco IOS Routers , on page 23
- Clock Policy Page , on page 24
- CPU Utilization Settings on Cisco IOS Routers , on page 26
- CPU Policy Page , on page 27
- HTTP and HTTPS on Cisco IOS Routers , on page 30
- HTTP Policy Page , on page 32
- Line Access on Cisco IOS Routers , on page 37
- Console Policy Page , on page 44
- VTY Policy Page , on page 52
- Optional SSH Settings on Cisco IOS Routers , on page 65
- Secure Shell Policy Page , on page 67
- SNMP on Cisco IOS Routers , on page 69
- SNMP Policy Page , on page 72
- DNS on Cisco IOS Routers , on page 77
- DNS Policy Page , on page 79
- Hostnames and Domain Names on Cisco IOS Routers , on page 80
- Hostname Policy Page , on page 81
- Memory Settings on Cisco IOS Routers , on page 81
- Memory Policy Page , on page 82
- Secure Device Provisioning on Cisco IOS Routers , on page 84
- Secure Device Provisioning Policy Page , on page 88

- DHCP on Cisco IOS Routers , on page 90
- DHCP Policy Page , on page 95
- NTP on Cisco IOS Routers , on page 100
- NTP Policy Page , on page 102

AAA on Cisco IOS Routers

Note From version 4.17, though Cisco Security Manager continues to support IOS features/functionality, it does not support any bug fixes or enhancements.

Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which you set up access control on your Cisco IOS router. Use the AAA policy in Security Manager to enable AAA functionality on Cisco IOS routers and to configure default AAA settings. The default settings that you define in this policy can be used in other policies, such as HTTP and line access (console and VTY) policies. Enabling AAA functionality is a prerequisite for any device policy that makes use of AAA, including NAC, SDP, and 802.1x.

For more information about AAA, see:

- Supported Authorization Types , on page 2
- Supported Accounting Types , on page 3
- Understanding Method Lists , on page 3

To configure a AAA policy, see:

- Defining AAA Services , on page 4

Related Topics

- Understanding AAA Server and Server Group Objects
- Line Access on Cisco IOS Routers , on page 37

Supported Authorization Types

AAA authorization enables you to limit the services available to an authenticated user. Security Manager supports the following types of authorization:

- Network—Authorizes various types of network connections, such as PPP, SLIP, and ARAP.
- EXEC—Authorizes the launching of EXEC (CLI) sessions.
- Command—Authorizes the use of all EXEC mode commands that are associated with specific privilege levels.

When authorization is enabled, the router uses information retrieved from the user's profile to configure the user session. The profiles are located either in the local user database or on a security server. Users are granted access to a requested service only if the profile allows it.

Related Topics

- Supported Accounting Types , on page 3
- Understanding Method Lists , on page 3
- Defining AAA Services , on page 4
- AAA on Cisco IOS Routers , on page 2

Supported Accounting Types

AAA accounting enables you to track the services the users are accessing and the amount of network resources that they are consuming. Security Manager supports the following accounting types:

- Connection—Records information about all outbound connections made from this device, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin connections.

For example, a RADIUS connection accounting record for an outbound Telnet connection includes such information as the port and IP address of the network access server (NAS), the start and end times of the connection, the identity of the user, and the number of packets that were transmitted during the session.

- EXEC—Records information about user EXEC (CLI) sessions on the devices, including the username, date, start and stop times, and the IP address of the NAS. For dial-in users, the record includes the telephone number from which the call originated.
- Command—Records information about the EXEC commands executed on the device by users with specific privilege levels. Each command accounting record includes a list of the commands executed for that privilege level, the date and time each command was executed, and the name of the user who executed it.

For each accounting type, you can choose whether you want to generate an accounting record at the start and end of each user session or only at the end.

When AAA accounting is enabled, the router sends accounting records of user activity to the TACACS+ or RADIUS security server. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can later be analyzed for network management, client billing, and auditing purposes.

Related Topics

- Supported Accounting Types , on page 3
- Understanding Method Lists , on page 3
- Defining AAA Services , on page 4
- AAA on Cisco IOS Routers , on page 2

Understanding Method Lists

A method list is a sequential list describing the methods to use to perform a particular AAA function. In Security Manager, you define method lists by selecting AAA server groups, which are reusable objects that typically contain one or more AAA servers running the same protocol, such as RADIUS or TACACS+.

Method lists enable you to designate one or more security protocols to be used for each AAA function, thus ensuring a backup system if the initial method fails.

Note Security Manager also contains predefined AAA server group objects for using the enable password or a local database. See Predefined AAA Authentication Server Groups.

For each AAA function, the device initially uses the first method defined in the list. If that method fails to respond, the device selects the next method in the list. This process continues until there is successful communication with a listed method, or all methods defined in the method list are exhausted.

Note The device attempts to communicate with the next listed method only when there is no response from the previous method. If the AAA service fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access or services—the process stops and no other methods are attempted.

Related Topics

- Supported Authorization Types , on page 2
- Supported Accounting Types , on page 3
- Defining AAA Services , on page 4
- AAA on Cisco IOS Routers , on page 2

Defining AAA Services

To define AAA services on a Cisco IOS router, you must first enable AAA functionality on the router. After you do this, you can define the kind of functionality (authentication, authorization, and accounting) that you want the device to implement. You must define a method list for each function, including lists for each type of authorization and accounting that you enable.

For example, if you want to configure EXEC authorization and command authorization, you must define one method list for EXEC authorization and other method lists for each privilege level on which command authorization is performed.

Note If you use RADIUS for authentication, you must use the same RADIUS server group for authorization as well.

Related Topics

- Understanding Method Lists , on page 3
- AAA on Cisco IOS Routers , on page 2
- Understanding AAA Server and Server Group Objects

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Device Admin** > **AAA** from the Policy selector.
- (Policy view) Select **Router Platform** > **Device Admin** > **AAA** from the Policy Type selector. Select an existing policy or create a new one.

The AAA page is displayed. See AAA Policy Page , on page 6 for a description of the fields on this page.

Step 2 Define which login authentication methods to use on users who access the device:

a) On the Authentication tab (see AAA Page—Authentication Tab , on page 7), select the **Enable Device Login Authentication** check box.

b) Enter the names of one or more AAA server group objects (up to four) in the Prioritized Method List field, or click **Select** select the object from a list or to create a new one. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used.

Note
If you select None as a method, it must appear as the last method in the list.

Step 3 (Optional) In the Maximum Number of Attempts field, define the maximum number of unsuccessful authentication attempts to allow before a user is locked out.

Step 4 (Optional) Define which authorization methods to use on users who have been successfully authenticated:

a) Click the **Authorization** tab on the AAA page. See Table 3: AAA Page—Authorization Tab , on page 8 for a description of the fields on this tab.

b) Define method lists for one or more of the following types of authorization:

- Network
- EXEC
- Command—Click the **Add** button to display the Command Authorization dialog box (see Command Authorization Dialog Box , on page 10). From here, you can select a privilege level and the method list to apply to it.

For more information about these authorization types, see Supported Authorization Types , on page 2.

Note
RADIUS uses the same server for authentication and authorization. Therefore, if you use define a RADIUS method list for authentication, you must define the same method list for authorization.

Step 5 (Optional) Define which accounting methods to use on the activities performed by users:

a) Click the **Accounting** tab on the AAA page. See Table 5: AAA Page—Accounting Tab , on page 11 for a description of the fields on this tab.

b) Define method lists for one or more of the following types of accounting:

- Connection
- EXEC
- Command—Click the **Add** button to display the Command Accounting dialog box (see Command Accounting Dialog Box , on page 13). From here, you can select a privilege level and the method list to apply to it.

For more information about these accounting types, see Supported Accounting Types , on page 3.

c) For each accounting type defined above, select a value from the Accounting Process Notices list. This defines when to create an accounting record, at the beginning and end of the user process or only at the end.

d) For each accounting type defined above, select the **Enable broadcast to multiple servers** check box if you want accounting information sent simultaneously to the first server in each AAA server group defined in the method list.

AAA Policy Page

Use the AAA page to define the default authentication, authorization, and accounting methods to use on the router. You do this by configuring method lists, which define which methods to use and the sequence in which to use them.

Note You can use the method lists defined in this policy as default settings when you configure AAA on the router's console port and VTY lines. See Console Policy Page , on page 44 and VTY Policy Page , on page 52.

Navigation Path

- (Device view) Select **Platform > Device Admin > AAA** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > AAA** from the Policy Type selector. Right-click **AAA** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- AAA on Cisco IOS Routers , on page 2
- Understanding AAA Server and Server Group Objects
- Console Policy Page , on page 44
- VTY Policy Page , on page 52

Field Reference

Table 1: AAA Page

Element	Description
Authentication tab	Defines the login authentication methods to use and the sequence in which to use them. See AAA Page—Authentication Tab , on page 7.
Authorization tab	Defines the types of network, EXEC, and command authorization to perform and the methods to use for each type. See AAA Page—Authorization Tab , on page 8.
Accounting tab	Defines types of connection, EXEC, and command accounting to perform and the methods to use for each type. See AAA Page—Accounting Tab , on page 10.

AAA Page—Authentication Tab

Use the Authentication tab of the AAA page to define the methods used to authenticate users who access the device. Authentication methods are defined in a method list, which define the security protocols to use, such as LDAP, RADIUS, and TACACS+.

Note You can use the method list defined in this policy on the console and VTY lines that are used to communicate with the device. See Console Policy Page , on page 44 and VTY Line Dialog Box—Authentication Tab , on page 57.

Navigation Path

Go to the AAA Policy Page , on page 6, then click the **Authentication** tab.

Related Topics

- Defining AAA Services , on page 4
- Understanding Method Lists , on page 3
- AAA Server Group Dialog Box
- Predefined AAA Authentication Server Groups

Field Reference

Table 2: AAA Page—Authentication Tab

Element	Description
Enable Device Login Authentication	When selected, enables the authentication of all users when they log in to the device, using the methods defined in the method list. When deselected, authentication is not performed.
Prioritized Method List	Defines a sequential list of methods to be queried when authenticating a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. Supported methods include Line, Local, Kerberos, LDAP, RADIUS, TACACS+, and None. **Note** If you select None as a method, it must appear as the last method in the list.

Element	Description
Maximum Number of Attempts	The maximum number of unsuccessful authentication attempts before a user is locked out. This feature is disabled by default. Valid values range from 1 to 65535. **Note** From the standpoint of the user, there is no distinction between a normal authentication failure and an authentication failure due to being locked out. The system administrator has to explicitly clear the status of a locked-out user using **clear** commands.

AAA Page—Authorization Tab

Use the Authorization tab of the AAA page to define the type of authorization services to enable on the device and the methods to use for each type. Security Manager supports the following types of authorization:

- Network—Authorizes various types of network connections, such as PPP.
- EXEC—Authorizes the launching of EXEC sessions.
- Command—Authorizes the use of all EXEC mode commands that are associated with specific privilege levels.

Note You can use the method lists defined in this policy on the console and VTY lines that are used to communicate with the device. See Console Policy Page , on page 44 and VTY Line Dialog Box—Authentication Tab , on page 57.

Navigation Path

Go to the AAA Policy Page , on page 6, then click the **Authorization** tab.

Related Topics

- Defining AAA Services , on page 4
- Supported Authorization Types , on page 2
- Understanding Method Lists , on page 3
- AAA Server Group Dialog Box
- Filtering Tables

Field Reference

Table 3: AAA Page—Authorization Tab

Element	Description
Network Authorization settings	

Element	Description
Enable Network Authorization	When selected, enables the authorization of network connections, such as PPP, SLIP, or ARAP connections, using the methods defined in the method list. When deselected, network authorization is not performed.
Prioritized Method List	Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. Supported methods include LDAP, RADIUS, TACACS+, Local, and None. **Note** RADIUS uses the same server for authentication and authorization. Therefore, if you use define a RADIUS method list for authentication, you must define the same method list for authorization. **Note** If you select None as a method, it must appear as the last method in the list.
EXEC Authorization settings	
Enable CLI/EXEC Operations Authorization	When selected, this type of authorization determines whether the user is permitted to open an EXEC (CLI) session, using the methods defined in the method list. When deselected, EXEC authorization is not performed.
Prioritized Method List	Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received.
Command Authorization settings	
Privilege Level	The privilege level to which the command authorization definition applies.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Authorization Dialog Box , on page 10. From here you can configure a command authorization definition.
Edit button	Opens the Command Authorization Dialog Box , on page 10. From here you can edit the command authorization definition.
Delete button	Deletes the selected command authorization definitions from the table.

Command Authorization Dialog Box

Use the Command Authorization dialog box to define which methods to use when authorizing the EXEC commands that are associated with a given privilege level. This enables you to authorize all commands associated with a specific privilege level, from 0 to 15.

Navigation Path

From the AAA Page—Authorization Tab , on page 8, click the **Add** button beneath the Command Authorization table.

Related Topics

- Defining AAA Services , on page 4
- Supported Authorization Types , on page 2
- Understanding Method Lists , on page 3

Field Reference

Table 4: Command Authorization Dialog Box

Element	Description
Privilege Level	The privilege level for which you want to define a command accounting list. Valid values range from 0 to 15.
Prioritized Method List	Defines a sequential list of methods to be used when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. Supported methods include TACACS+, Local, and None. **Note** If you select None as a method, it must appear as the last method in the list.

AAA Page—Accounting Tab

Use the Accounting tab of the AAA page to define the type of accounting services to enable on the device and the methods to use for each type. Security Manager supports the following types of accounting:

- Connection—Records information about all outbound connections made from this device.
- EXEC—Records information about user EXEC sessions on the devices, including the username, date, start and stop times, and the IP address.

- Command—Records information about the EXEC commands executed on the device by users with specific privilege levels.

In addition, you use the Accounting page to determine when accounting records should be generated and whether they should be broadcast to more than one AAA server.

Note You can use the method lists defined in this policy on the console and VTY lines that are used to communicate with the device. See Console Policy Page , on page 44 and VTY Line Dialog Box—Authentication Tab , on page 57.

Navigation Path

Go to the AAA Policy Page , on page 6, then click the **Accounting** tab.

Related Topics

- Defining AAA Services , on page 4
- Supported Accounting Types , on page 3
- Understanding Method Lists , on page 3
- AAA Server Group Dialog Box
- Filtering Tables

Field Reference

Table 5: AAA Page—Accounting Tab

Element	Description
Connection Accounting settings	
Enable Connection Accounting	When selected, enables the recording of information about outbound connections (such as Telnet) made over this device, using the methods defined in the method list. When deselected, connection accounting is not performed.
Generate Accounting Records for	Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the “start” accounting record. • Stop Only—Generates an accounting record at the end of the user process only. • None—Disables this type of accounting.

Element	Description
Prioritized Method List	Defines a sequential list of methods to be queried when creating connection accounting records for a user. Enter the names of one or more AAA server group objects (up to 10 for IOS 12.4(22)T+, otherwise up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. Supported methods include LDAP, RADIUS, and TACACS+.
Enable Broadcast to Multiple Servers	When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.
EXEC Accounting Settings	
Enable CLI/EXEC Operations Accounting	When selected, enables the recording of basic information about user EXEC sessions, using the methods defined in the method list. When deselected, EXEC accounting is not performed.
Generate Accounting Records for	See Table 1.
Prioritized Method List	Defines a sequential list of methods to be queried when creating connection accounting records for a user. Enter the names of one or more AAA server group objects (up to 10 for IOS 12.4(22)T+, otherwise up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it.
Enable Broadcast to Multiple Servers	When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group.
Command Accounting settings	
Privilege Level	The privilege level to which the command authorization definition applies.
Generate Accounting Records for	The points in the process where the device sends an accounting notice to the accounting server.
Enable Broadcast	Whether accounting records are broadcast to multiple servers simultaneously.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Accounting Dialog Box , on page 13. From here you can configure a command accounting definition.

Element	Description
Edit button	Opens the Command Accounting Dialog Box , on page 13. From here you can edit the command accounting definition.
Delete button	Deletes the selected command accounting definitions from the table.

Command Accounting Dialog Box

Use the Command Accounting dialog box to define which methods to use when recording information about the EXEC commands that are executed for a given privilege level. Each accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the name of the user who executed it.

Navigation Path

From the AAA Page—Accounting Tab , on page 10, click the **Add** button beneath the Command Accounting table.

Related Topics

- Defining AAA Services , on page 4
- Supported Accounting Types , on page 3
- Understanding Method Lists , on page 3

Field Reference

Table 6: Command Accounting Dialog Box

Element	Description
Privilege Level	The privilege level for which you want to define a command accounting list. Valid values range from 0 to 15.
Generate Accounting Records for	Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.

Element	Description
Prioritized Method List	Defines a sequential list of methods to be used when creating accounting records for a user. Enter the names of one or more AAA server group objects (up to 10 for IOS 12.4(22)T+, otherwise up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. TACACS+ is the only supported method, but you can select multiple AAA server groups configured with TACACS+. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.

User Accounts and Device Credentials on Cisco IOS Routers

Accounts and credential policies define the contact information for accessing the router, including the privilege level provided to each user account. You can configure as many user accounts as required. However, the user account that Security Manager uses to connect to the router is always the one configured in the Device Properties page.

Additionally, you use device access policies to define the enable or enable secret password required to access privileged EXEC mode. This is the mode required to make any configuration changes on the router.

Note If you use this policy to define a password, be careful later not to unassign this policy without assigning a replacement policy before your next deployment. If you deploy a device access policy that removes this password and the device contains a different type of password not known to Security Manager, such as a line console password, you will not be able to configure this device in the future. This is because the device reverts to this unknown password if Security Manager removes the enable password that it had previously configured.

Related Topics

- Defining Accounts and Credential Policies , on page 15

Defining Accounts and Credential Policies

This procedure describes how to define a device access policy on a Cisco IOS router. If the username that you configured on the Device Properties page to connect to the router (see Viewing or Changing Device Properties) matches one of the user accounts you defined in this policy, Security Manager updates the device credentials according to your policy definition.

If you change the password for the user defined in the device properties, which Security Manager uses to deploy configurations to the device, or change the enable password, Security Manager uses the existing credentials defined in the device properties to log into the device and deploy changes. After successful deployment, the device properties are then changed to use your new settings. For more information on credentials in device properties, see Device Credentials Page.

Note You can discover encrypted passwords, but any password you enter must be in clear text. If you discover an encrypted password and then modify it, the password is saved as clear text.

Related Topics

- User Accounts and Device Credentials on Cisco IOS Routers , on page 14

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Accounts and Credentials** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Accounts and Credentials** from the Policy Type selector. Select an existing policy or create a new one.

The Accounts and Credentials page is displayed. See Table 7: Accounts and Credentials Page , on page 17 for a description of the fields on this page.

Step 2 Enter the password for switching to privileged EXEC mode on the router:

a) Select **Enable Password** or **Enable Secret Password**. The Enable Secret Password option offers better security than the Enable Password option by storing the password using MD5 encryption. This option is useful in environments in which the password crosses the network or is stored on a TFTP server.

Note
After you set an enable secret password, you can switch to an enable password only if the enable secret is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image.

b) Enter a password, then enter it again in the Confirm field. The password that you enter must be in clear text. If you are configuring the enable secret password, the password is encrypted on deployment.

Step 3 (Optional) Select the **Enable Password Encryption Service** check box to encrypt all passwords on the device. This includes, for example, the enable password, username passwords, authentication key passwords, console and VTY line access passwords, and BGP neighbor passwords.

We recommend using this feature to help prevent unauthorized individuals from viewing the passwords in your configuration file.

Note
This option does not provide a high level of security and should not be used as a substitute for additional network security measures.

Step 4 To define new user accounts for the router:

a) Click the **Add** button under the table to display the User Accounts dialog box.
b) Enter the details for the new user. See Table 8: User Account Dialog Box , on page 18 for a description of the available fields.
c) Click **OK** to save your definitions locally on the client and close the dialog box. Your definitions are displayed in the User Accounts table.

Note
To edit a user account, select it from the User Accounts table, then click **Edit**. To remove a user account, select it, then click **Delete**.

Caution
While deleting a user account, Cisco Security Manager times out and deployment fails. To avoid this, you can set up Security Manager to download despite an error. Enable **Allow Download** on **Error** in **Tools > Administrator > Deployments** in the Configuration Manager.

Accounts and Credentials Policy Page

Use the Accounts and Credentials page to define the enable password or enable secret password assigned to the router. In addition, you can define a list of usernames that can be used to access the router.

For more information, see Defining Accounts and Credential Policies , on page 15.

Navigation Path

- (Device view) Select **Platform > Device Admin > Accounts and Credentials** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Accounts and Credentials** from the Policy Type selector. Right-click **Accounts and Credentials** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- User Accounts and Device Credentials on Cisco IOS Routers , on page 14
- User Account Dialog Box , on page 18
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 7: Accounts and Credentials Page

Element	Description
Enable Secret Password	The enable secret password for entering privileged EXEC mode on the router. This option offers better security than the Enable Password option. The enable secret password can contain between 1-25 alphanumeric characters. The first character must be a letter. Spaces are allowed, but leading spaces are ignored. Question marks are also allowed. **Note** You can discover an encrypted password, but any password you enter must be in clear text. If you modify an encrypted password, it is saved as clear text. **Note** After you set an enable secret password, you can switch to an enable password only if the enable secret is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image.
Enable Password	The enable password for entering privileged EXEC mode on the router. The enable password can contain between 1-25 alphanumeric characters. The first character must be a letter. Spaces are allowed, but leading spaces are ignored. Question marks are also allowed. **Note** You must enter the password in clear text.
Enable Password Encryption Service	When selected, encrypts all passwords on the device, including the enable password (which is otherwise saved in clear text). For example, use this option to encrypt username passwords, authentication key passwords, console and VTY line access passwords, and BGP neighbor passwords. This command is primarily used for keeping unauthorized individuals from viewing your passwords in your configuration file. When deselected, device passwords are stored unencrypted in the configuration file. **Note** This option does not provide a high level of network security. You should also take additional network security measures.
User Accounts Table	
Username	The username that can be used to access the router. The username must be a single word up to 64 characters in length. Spaces and quotation marks are not allowed.
Encryption	Indicates whether password information for the user is encrypted using MD5 encryption.
Privilege Level	The privilege level assigned to the user.
Add button	Opens the User Account Dialog Box , on page 18. From here you can define a user account.

Element	Description
Edit button	Opens the User Account Dialog Box , on page 18. From here you can edit the selected user.
Delete button	Deletes the selected user accounts from the table.

User Account Dialog Box

Employ the User Account dialog box to define a username and password combination that can be used by Security Manager to access the router. You can also define the privilege level of the user account, which determines whether you can configure all commands on this router or only a subset of them.

Note Remember—there may be additional user accounts defined on the router using other methods, such as the CLI.

Navigation Path

Go to the Accounts and Credentials Policy Page , on page 16, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Accounts and Credential Policies , on page 15
- User Accounts and Device Credentials on Cisco IOS Routers , on page 14
- Understanding FlexConfig Policies and Policy Objects

Field Reference

Table 8: User Account Dialog Box

Element	Description
Username	The username for accessing the router.
Password	The password for accessing the router with this user account. **Note** You can discover an encrypted password, but any password you enter must be in clear text.
Confirm	Confirms the password for this user account.
Encrypt password using MD5	When selected, uses MD5 encryption to encrypt the password for this user account. This is the default. When deselected, the password is sent to the router unencrypted.

Element	Description
Privilege Level	The privilege level assigned to the user account. Valid values range from 0 to 15: • 0—Grants access to these commands only: **disable**, **enable**, **exit**, **help**, and **logout**. • 1—Enables nonprivileged access to the router (normal EXEC-mode use privileges). • 15—Enables privileged access to the router (traditional enable privileges). **Note** Levels 2-14 are not normally used in a default configuration, but custom configurations can be created by moving commands that are normally at level 15 to a lower level and commands that are normally at level 1 to a higher level. You can configure the privilege levels of commands using the CLI or by defining a FlexConfig.

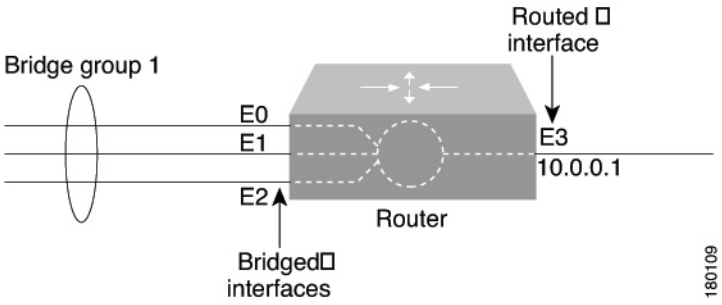
Bridging on Cisco IOS Routers

Bridging policies enable you to perform transparent bridging (as specified in RFC 1286) on selected interfaces that you have configured to function as a bridge group. Security Manager supports integrated routing and bridging, which makes it possible to route a specific protocol between routed interfaces and bridge groups, or route a specific protocol between bridge groups. Local or unroutable traffic can be bridged among the bridged interfaces in the same bridge group, while routable traffic can be routed to other routed interfaces or bridge groups, as shown in Figure 1: Transparent Bridging, on page 19.

Using integrated routing and bridging, you can:

- Switch packets from a bridged interface to a routed interface.
- Switch packets from a routed interface to a bridged interface.
- Switch packets within the same bridge group.

Figure 1: Transparent Bridging



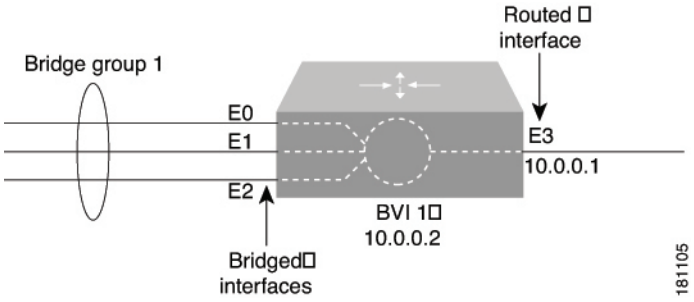
Related Topics

- Defining Bridge Groups , on page 20
- Bridge-Group Virtual Interfaces , on page 20

Bridge-Group Virtual Interfaces

Because bridging takes places at the data link layer and routing takes place at the network layer, they have different protocol configuration models. With IP, for example, bridge group interfaces belong to the same network and have a collective IP network address. In contrast, each routed interface represents a distinct network and has its own IP network address. Integrated routing and bridging uses the concept of a bridge-group virtual interface (BVI) to enable these interfaces to exchange packets for a given protocol. As shown in Figure 2: Bridge-Group Virtual Interface, on page 20, the interface number assigned to the BVI corresponds to the bridge group that the BVI represents. This number serves as the link between the virtual interface and the bridge group.

Figure 2: Bridge-Group Virtual Interface



When you enable routing for a given protocol on the BVI, packets coming from a routed interface that are destined for a host in a bridged domain are routed to the BVI and then forwarded to the corresponding bridged interface. All traffic routed to the BVI is forwarded to the corresponding bridge group as bridged traffic. All routable traffic received on a bridged interface is routed to other routed interfaces as if it is coming directly from the BVI.

Note BVI interfaces are configured using the Interfaces policy. See Defining Basic Router Interface Settings. The BVI interface must have a corresponding bridge group with the same number; otherwise, deployment will fail.

Note When the bridge group contains more than two interfaces, add a BVI interface to the group to help prevent unicast flooding, which is a potential security issue.

Related Topics

- Defining Bridge Groups , on page 20
- Bridging on Cisco IOS Routers , on page 19

Defining Bridge Groups

You define a bridge group by selecting the L3 interfaces that are part of the bridge group and assigning the group a number. All bridge groups in Security Manager perform integrated routing and bridging on IP traffic only and use the standard Spanning Tree Protocol (IEEE 802.1D).

Note Use CLI commands or FlexConfigs to bridge other protocols, such as AppleTalk or IPX, and to use other spanning tree protocols, such as VLAN-Bridge. Concurrent routing and bridging is not supported.

Related Topics

- Bridging on Cisco IOS Routers , on page 19
- Bridge-Group Virtual Interfaces , on page 20

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Bridging** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Bridging** from the Policy Type selector. Select an existing policy or create a new one.

The Bridging page is displayed. See Table 9: Bridging Page , on page 22 for a description of the fields on this page.

Step 2 Click the **Add** button under the table to display the Bridge Group dialog box. See Table 10: Bridge Group Dialog Box , on page 23 for a description of the fields in this dialog box. From here you can define a bridge group.

Step 3 Enter a number to identify the bridge group.

Step 4 Enter the names of the interfaces and interface roles that are part of the bridge group, or click **Select** to select an interface role or to create a new one. For more information, see Specifying Interfaces During Policy Definition.

You can select most Layer 3 interfaces, except X.25 and Integrated Services Digital Network (ISDN) bridged interfaces and certain types of logical interfaces (such as loopback, tunnel, null, and BVI). Each interface can be included in only one bridge group.

You can select a LAN subinterface only if the parent interface is configured with Inter-Switch Link (ISL) or 802.1Q encapsulation.

Step 5 Click **OK** to save your definitions locally on the client and close the dialog box. The bridge group is displayed in the table on the Bridging page.

Note
To edit a bridge group, select it from the Groups table, then click **Edit**. To remove a bridge group, select it, then click **Delete**.

Bridging Policy Page

Use the Bridging page to define bridge groups that can perform integrated routing and bridging on the router. For more information, see Defining Bridge Groups , on page 20.

Navigation Path

- (Device view) Select **Platform** > **Device Admin** > **Bridging** from the Policy selector.
- (Policy view) Select **Router Platform** > **Device Admin** > **Bridging** from the Policy Type selector. Right-click **Bridging** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Bridging on Cisco IOS Routers , on page 19
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 9: Bridging Page

Element	Description
Group Number	The number that identifies the bridge group.
Group Interfaces	The interfaces and interface roles that are included in the bridge group.
Add button	Opens the Bridge Group Dialog Box , on page 22. From here you can define a bridge group.
Edit button	Opens the Bridge Group Dialog Box , on page 22. From here you can edit the bridge group.
Delete button	Deletes the selected bridge groups from the table.

Bridge Group Dialog Box

Use the Bridge Group dialog box to define bridge groups on the router. Each bridge group can contain multiple Layer 3 interfaces of various types, including serial interfaces.

Note All bridge groups use the standard Spanning Tree Protocol (IEEE 802.1D). Use CLI commands or FlexConfigs to bridge other protocols, such as AppleTalk or IPX, and to use other spanning tree protocols, such as VLAN-Bridge.

Navigation Path

Go to the Bridging Policy Page , on page 21, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining Bridge Groups , on page 20

- Bridging on Cisco IOS Routers , on page 19
- Understanding Interface Role Objects

Field Reference

Table 10: Bridge Group Dialog Box

Element	Description
Group Number	The number assigned to the bridge group. Valid values range from 1 to 255.
Group Interfaces	The interfaces that are included in the bridge group. Enter the name of one or more interfaces and interface roles, or click **Select** to select them. If the object that you want is not listed, click the **Create** button to create it. You can select most Layer 3 interfaces, including serial interfaces, provided the serial interface is configured with high-level data link control (HDLC) or Frame Relay encapsulation. Each interface can belong to only one bridge group. You can select a LAN subinterface only if the parent interface is configured with Inter-Switch Link (ISL) or 802.1Q encapsulation. **Note** Certain types of interfaces, such as loopback, tunnel, null, and BVI, cannot be bridged. **Note** Make sure that your bridge group does not prevent Security Manager from communicating with the device.

Time Zone Settings on Cisco IOS Routers

The local time on a Cisco IOS router is typically set using the clock set command in the CLI command or by dynamically deriving the time from an NTP server. You can adjust these time settings by defining the time zone in which the router resides and the start and end dates of Daylight Saving Time (DST) in that time zone.

Related Topics

- Defining Time Zone and DST Settings , on page 23
- NTP on Cisco IOS Routers , on page 100

Defining Time Zone and DST Settings

Security Manager enables you to define the time zone in which a Cisco IOS router is located. You can also define the start and end dates for Daylight Saving Time (DST).

Related Topics

- Defining NTP Servers , on page 101
- Time Zone Settings on Cisco IOS Routers , on page 23

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Clock** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Clock** from the Policy Type selector. Select an existing policy or create a new one.

The Clock page is displayed. See Table 11: Clock Page , on page 25 for a description of the fields on this page.

Step 2 Select the time zone in which the router is located. Time zones are listed according the number of hours behind or ahead of Greenwich Mean Time (GMT).

Step 3 (Optional) Select the method for determining the start and end dates for DST:

- Set by Date—Select this option when DST starts and ends on fixed dates. Continue with Step 4, on page 24.
- Set by Day—Select this option when DST starts and ends on days whose specific dates vary from year to year. Continue with Step 5, on page 24.
- None—Select this option when DST is not used.

Step 4 (When Set by Date is selected) Define the fixed dates when DST starts and ends:

a) Under Start, click the calendar icon, then click the appropriate date.
b) Select the hour and minute from the displayed lists.
c) Repeat steps a and b to configure the end date and time.

Step 5 (When Set by Day is selected) Select the **Specify Recurring Time** check box if you want to define a DST period *other* than the default, which is the period used throughout most of the United States.

Step 6 (When Specify Recurring Time is selected) Define the start and end of DST:

a) Under Start, select the month when DST begins.
b) Select the week of the month (1, 2, 3, 4, first, or last).
c) Select the day of the week.
d) Select the hour and minute from the displayed lists. For example, if DST begins at 1:00 a.m. on the last Sunday of each March, select March, last, Sunday, 1, and 00.
e) Repeat Steps a through d to configure the end date and time.

Clock Policy Page

Use the Clock page to configure the time zone in which the router is located and the settings for Daylight Saving Time (DST). For more information, see Time Zone Settings on Cisco IOS Routers , on page 23.

Tip You can configure the local time on the router by defining an NTP policy or by configuring the **clock set** command using the CLI.

Navigation Path

- (Device view) Select **Platform > Device Admin > Clock** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Clock** from the Policy Type selector. Right-click **Clock** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- NTP Policy Page , on page 102

Field Reference

Table 11: Clock Page

Element	Description
Device Time Zone	The time zone in which the router is located, expressed in relation to GMT (Greenwich Mean Time), also known as UTC (Coordinated Universal Time). **Caution** If you want to use the Command Line Interface (CLI) to configure the time zone on the router, you must use the required Time Zone acronym provided in the Cisco IOS Configuration Fundamentals Command Reference document. If you use any other format for the time zone and then use Security Manager to discover the router, Security Manager will not discover the time zone CLI.
Daylight Savings Time (Summer Time)	The type of DST to apply to the local time on the router: • Set by Date—Enables you to define the exact date and time when DST begins and ends. • Set by Day—Enables you to define the relative recurring date and time when DST begins and ends. For example, you can use this option when DST begins the last Sunday of March and ends the last Sunday of October. • None—Daylight savings time is not used.
Additional Set by Date fields	
Start	The date and time when DST begins: • Date—Click the calendar icon to select the start date. • Hour—Select the start hour. • Minute—Select the start minute.

Element	Description
End	The date and time when DST ends: • Date—Click the calendar icon to select the end date. • Hour—Select the end hour. • Minute—Select the end minute. **Note** Cisco IOS Software supports dates up to and including December 31st, 2035.
Additional Set by Day fields	
Specify Recurring Time	When selected, the router implements DST according to the dates and times specified in this policy. When deselected, the router implements DST according to the schedule used throughout most of the United States.
Start	The relative date and time when daylight savings time begins: • Month—Select the month. • Week—Select the week of the month (1, 2, 3, 4, first, or last). • Weekday—Select the day of the week. • Hour—Select the hour. • Minute—Select the minute. For example, if DST begins at 1:00 a.m. on the last Sunday of each March, select March, last, Sunday, 1, and 00.
End	The relative date and time when daylight savings time ends: • Month—Select the month. • Week—Select the week of the month (1, 2, 3, 4, first, or last). • Weekday—Select the day of the week. • Hour—Select the hour. • Minute—Select the minute.

CPU Utilization Settings on Cisco IOS Routers

The CPU policy configures settings relating to CPU utilization. This policy provides you with methods for monitoring CPU resources and tracking processes that exceed a predetermined level of utilization.

Note The CPU policy is supported on routers running Cisco IOS Software Release 12.3(14)T or later.

Related Topics

- Defining CPU Utilization Settings , on page 27

Defining CPU Utilization Settings

You can use Security Manager to modify the following default CPU utilization settings:

- The size of the CPU history table.
- The size of the extended CPU load history table.
- Whether to enable the automatic CPU Hog profiling.

In addition, you can optionally define:

- The CPU utilization level that causes a process to be included in the history table.
- The types of CPU utilization thresholds to enable. For each type of threshold, you can determine the threshold values that trigger notifications.

Related Topics

- Defining CPU Utilization Settings , on page 27
- Logging on Cisco IOS Routers

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Device Admin** > **CPU** from the Policy selector.
- (Policy view) Select **Router Platform** > **Device Admin** > **CPU** from the Policy Type selector. Select an existing policy or create a new one.

The CPU page is displayed.

Step 2 (Optional) Define the CPU utilization settings of the router, as required. See Table 12: CPU Page , on page 28 for a description of the available fields.

CPU Policy Page

Use the CPU page to configure settings related to router CPU utilization, including the thresholds for sending log messages, the size of the CPU history table, and whether to enable automatic CPU Hog profiling.

For more information, see Defining CPU Utilization Settings , on page 27.

Navigation Path

- (Device view) Select **Platform** > **Device Access** > **CPU** from the Policy selector.

- (Policy view) Select **Router Platform > Device Access > CPU** from the Policy Type selector. Right-click **CPU** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Memory Policy Page , on page 82
- Syslog Logging Setup Policy Page
- Syslog Servers Policy Page

Field Reference

Table 12: CPU Page

Element	Description
CPU Utilization Statistics	Settings related to the history table for CPU utilization statistics: • History Table Entry Limit—The percentage of CPU utilization that a process must use to be included in the history table. • History Table Size—The length of time for which CPU statistics are stored in the history table. Valid values range from 5 to 86400 seconds (24 hours). The default is 600 seconds (10 minutes).
CPU Total Utilization	The thresholds for total CPU utilization that trigger notifications: • Enable CPU Total Utilization—When selected, CPU total utilization thresholds are enabled. When deselected, these thresholds are disabled and do not trigger notifications. This is the default. • Maximum Total Utilization Resources—The percentage of CPU resources that, when usage *exceeds* this level for the defined interval, triggers a notification. • Maximum Total Utilization Violation Duration—The violation interval that triggers a maximum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours). • Minimum Total Utilization Resources—The percentage of CPU resources that, when usage *falls below* this level for the defined interval, triggers a notification. • Minimum Total Utilization Violation Duration—The violation interval that triggers a minimum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours).

Element	Description
CPU Interrupt Utilization	The thresholds for CPU interrupt utilization that trigger notifications: • Enable CPU Interrupt Utilization—When selected, CPU interrupt utilization thresholds are enabled. When deselected, these thresholds are disabled and do not trigger notifications. This is the default. • Maximum Interrupt Utilization Resources—The percentage of CPU resources that, when usage *exceeds* this level for the defined interval, triggers a notification. • Maximum Interrupt Utilization Violation Duration—The violation interval that triggers a maximum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours). • Minimum Interrupt Utilization Resources—The percentage of CPU resources that, when usage *falls below* this level for the defined interval, triggers a notification. • Minimum Interrupt Utilization Violation Duration—The violation interval that triggers a minimum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours).
CPU Process Utilization	The thresholds for CPU process utilization that trigger notifications: • Enable CPU Process Utilization—When selected, CPU process utilization thresholds are enabled. When deselected, these thresholds are disabled and do not trigger notifications. This is the default. • Maximum Process Utilization Resources—The percentage of CPU resources that, when usage *exceeds* this level for the defined interval, triggers a notification. • Maximum Process Utilization Violation Duration—The violation interval that triggers a maximum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours). • Minimum Process Utilization Resources—The percentage of CPU resources that, when usage *falls below* this level for the defined interval, triggers a notification. • Minimum Process Utilization Violation Duration—The violation interval that triggers a minimum CPU threshold notification. Valid values range from 5 to 86400 seconds (24 hours).
Extended CPU History Size	The size of the history to collect for the extended CPU load, in increments of 5 seconds. Valid values range from 2 to 720. The default is 12, which is equivalent to a 1-minute history.
Enable Automatic CPU Hog Profiling	When selected, automatic CPU Hog profiling is enabled. This is the default. When deselected, automatic CPU Hog profiling is disabled. This feature predicts when a process could hog the CPU and begins profiling that process. **Note** To view the CPU Hog profile data, use the **show processes cpu autoprofile hog** command in the CLI.

HTTP and HTTPS on Cisco IOS Routers

Security Manager enables you to configure HTTP and HTTP over Secure Socket Layer (known as HTTP over SSL or HTTPS) server functionality on Cisco IOS routers. This feature provides SSL version 3.0 support for the HTTP 1.1 server.

A secure HTTP connection means that data sent to and received from an HTTP server are encrypted before being sent out over the internet. HTTP with SSL encryption provides a secure connection to allow such functions as configuring a router from a web browser.

In addition to providing access to the device via the Cisco web browser user interface, HTTP and HTTPS are used by device management applications, such as the Cisco Router and Security Device Manager (SDM), to communicate with the device.

Related Topics

- Defining HTTP Policies , on page 30

Defining HTTP Policies

When you define an HTTP policy, you can:

- Enable and disable HTTP and SSL functionality on the router.
- Specify the ports used by each protocol.
- Optionally define a standard, numbered ACL that restricts access to the device using these protocols.

In addition, you can define the methods of AAA authentication and authorization methods to perform on users.

You must use caution when defining an HTTP policy, as your settings may affect communication between Security Manager (as well as other management applications that use these protocols) and the device.

Note As a general rule, Cisco IOS routers that have been discovered by Security Manager already have HTTPS enabled because Security Manager uses SSL as the default protocol for communicating with them. See Setting Up SSL on Cisco IOS Routers.

Before You Begin

- Enable AAA services on the router. See Defining AAA Services , on page 4.

Related Topics

- HTTP and HTTPS on Cisco IOS Routers , on page 30

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Device Access > HTTP** from the Policy selector, then click the **Setup** tab in the work area.
- (Policy view) Select **Router Platform > Device Admin > Device Access > HTTP** from the Policy Type selector. Select an existing policy or create a new one.

The HTTP Setup tab is displayed. See Table 13: HTTP Page—Setup Tab , on page 33 for a description of the fields on this tab.

Step 2 Select the check boxes to enable HTTP and SSL (HTTPS) server functionality on the router.

Note
If SSL is disabled (or if the HTTP policy as a whole is unassigned), Security Manager cannot communicate with the device after deployment unless you change the transport protocol for this device to SSH. This setting can be found in Device Properties. See Managing Device Communication Settings and Certificates.

Tip
We recommend that you disable HTTP when SSL is enabled. This is required to ensure only secure connections to the server.

Step 3 (Optional) Modify the default ports used by HTTP (80) and HTTPS (443).

Step 4 (Optional) In the Allow Connection From field, enter the name of the standard, numbered ACL object that specifies which addresses can use HTTP and HTTPS on this device, or click **Select** to select the ACL object from a list or to create a new one. Use this option to restrict access to these protocols. For more information about creating standard ACL objects, see Creating Standard Access Control List Objects

Note
Make sure that the ACL you select permits the Security Manager server; otherwise, communication with the device is lost.

Step 5 (Optional) On the AAA tab, modify the default type of authentication to perform on users who attempt to access the device using HTTP or HTTPS. Options include AAA, Enable Password (default), Local Database, and TACACS.

If you select AAA, continue with Step 6, on page 31; otherwise, continue with Step 8, on page 32.

Note
The TACACS option applies only to devices using an IOS software version prior to 12.3(8).

See Table 14: HTTP Page—AAA Tab , on page 34 for a description of the fields on the AAA tab.

Step 6 Select the authentication method to perform on users:

- If you want to use the default AAA login authentication methods defined in the device's AAA policy (see Defining AAA Services , on page 4), do *not* select the Enable Device Login Authentication check box. Continue with Step 7, on page 32.
- If you want to define a method list especially for this policy, do the following:

a) Select the **Enable Device Login Authentication** check box.

b) Under Prioritized Method List, enter the names of the AAA server groups to use for authentication, or click **Select** to select the AAA server groups from a list or to create new ones. Use the up and down arrows in the selector to define the order in which you want to apply these authentication methods.

Note
Make sure that Security Manager users are defined on the AAA servers; otherwise communication with the device is lost.

Step 7 Select the authorization method to perform on users who use HTTP or HTTPS to begin an EXEC session:

- If you want to use the default AAA authorization methods defined in the device's AAA policy, do *not* select the Enable CLI/EXEC Operations Authorization check box. Continue with Step 8, on page 32.
- If you want to define a method list especially for this policy, select the **Enable CLI/EXEC Operations Authorization** check box, then define the method list.

Note
If you leave this option deselected, make sure that EXEC authorization is enabled in the router's AAA policy. Otherwise, you will be unable to connect to the device via HTTP or HTTPS (SSL). This applies to Security Manager as well as other applications, such as SDM. See Defining AAA Services , on page 4.

Step 8 (Optional) Create command authorization definitions for specific privilege levels:

a) Click the **Add** button under the Command Authorization Override table. The Command Authorization Override dialog box is displayed. See Table 15: Command Authorization Dialog Box , on page 36 for a description of the fields in this dialog box.
b) Configure the command authorization definition as required.
c) Click **OK**. The dialog box closes and the authorization method is displayed in the Command Authorization Override table.
d) Repeat 8.a, on page 32 through 8.c, on page 32 to create additional command authorization definitions.

HTTP Policy Page

Use the HTTP page to configure HTTP and HTTPS access on the router. You can configure HTTP policies on a Cisco IOS router from the following tabs on the HTTP policy page:

- HTTP Page—Setup Tab , on page 33
- HTTP Page—AAA Tab , on page 34

For more information, see HTTP and HTTPS on Cisco IOS Routers , on page 30.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > HTTP** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > HTTP** from the Policy Type selector. Right-click **HTTP** to create a policy, or select an existing policy from the Shared Policy selector.

HTTP Page—Setup Tab

Use the Setup tab of the HTTP page to enable HTTP and HTTP over Secure Socket Layer (HTTP over SSL or HTTPS) on the router. You can optionally limit access to these protocols to the addresses defined in an access control list.

Note As a general rule, Cisco IOS routers that have been discovered by Security Manager already have HTTPS enabled because Security Manager uses SSL as the default protocol for communicating with them. See Setting Up SSL on Cisco IOS Routers.

Navigation Path

Go to the HTTP Policy Page , on page 32, then click the **Setup** tab.

Related Topics

- HTTP Page—AAA Tab , on page 34
- HTTP and HTTPS on Cisco IOS Routers , on page 30

Field Reference

Table 13: HTTP Page—Setup Tab

Element	Description
Enable HTTP	When selected, an HTTP server is enabled on the router. When deselected, HTTP is disabled on the router. This is the default for devices that were not discovered.
HTTP Port	The port number to use for HTTP. Valid values are 80 or any value from 1024 to 65535. The default is 80.
Enable SSL	When selected, a secure HTTP server (HTTP over SSL or HTTPS) is enabled on the router. When deselected, HTTPS is disabled. This is the default for devices that were not discovered. **Note** If SSL is disabled (or if the HTTP policy as a whole is unassigned), Security Manager cannot communicate with the device after deployment unless you change the transport protocol for this device to SSH. This setting can be found in Device Properties. **Note** We recommend that you disable HTTP when SSL is enabled. This is required to ensure only secure connections to the server.
SSL Port	The port number to use for HTTPS. Valid values are 443 or any value from 1025 to 65535. The default is 443.

Element	Description
Allow Connection From	The name of the standard numbered ACL that restricts use of HTTP and HTTPS on this device. Enter the name of an ACL object, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it. **Note** If you define an ACL, make sure that it includes the Security Manager server. Otherwise, Security Manager cannot communicate with this device using SSL.

HTTP Page—AAA Tab

Use the AAA tab of the HTTP page to define the authentication and authorization methods to perform on users who attempt to access the router using HTTP or HTTPS.

Navigation Path

Go to the HTTP Policy Page , on page 32, then click the **AAA** tab.

Related Topics

- HTTP Page—Setup Tab , on page 33
- HTTP and HTTPS on Cisco IOS Routers , on page 30
- Filtering Tables

Field Reference

Table 14: HTTP Page—AAA Tab

Element	Description
Authenticate Using	The type of authentication to use: • AAA—Performs AAA login authentication. • Enable Password—Uses the enable password configured on the router. This is the default. • Local Database—Uses the local username database configured on the router. • TACACS—Uses the TACACS or XTACACS server configured on the router. Applies only to devices using an IOS software version prior to 12.3(8) or 12.3(8)T.
Login Authentication settings	

Element	Description
Enable Device Login Authentication	Applies only when AAA is selected as the authentication method. When selected, authentication is based on the methods defined in the Prioritized Method List field. When deselected, the default authentication list defined in the router's AAA policy is used. See AAA Page—Authentication Tab , on page 7.
Prioritized Method List	Applies only when the Enable Device Login Authentication check box is selected. Defines a sequential list of methods to be queried when authenticating a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
EXEC Authorization settings	
Enable CLI/EXEC Operations Authorization	Applies only when AAA is selected as the authentication method. When selected, EXEC authorization is based on the methods defined in the Prioritized Method List field. This type of authorization determines whether the user is permitted to open an EXEC (CLI) session. When deselected, the default EXEC authorization list defined in the router's AAA policy is used. See AAA Page—Authorization Tab , on page 8. **Note** If you leave this option deselected, make sure that EXEC authorization is enabled in the router's AAA policy. Otherwise, you will be unable to connect to the device via HTTP or HTTPS (SSL). This applies to Security Manager as well as other applications, such as SDM and the device's web interface.
Prioritized Method List	Applies only when the Enable CLI/EXEC Operations Authorization check box is selected. Defines a sequential list of methods to be queried when authorizing a user to open an EXEC (CLI) session. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.

Element	Description
Command Authorization settings	
Privilege Level	The privilege level to which the command authorization definition applies.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Authorization Override Dialog Box , on page 36. From here you can configure a command authorization definition.
Edit button	Opens the Command Authorization Override Dialog Box , on page 36. From here you can edit the command authorization definition.
Delete button	Deletes the selected command authorization definitions from the table.

Command Authorization Override Dialog Box

Use the Command Authorization Override dialog box to define which methods to use when authorizing the EXEC commands that are associated with a given privilege. This enables you to authorize all commands associated with a specific privilege level, from 0 to 15.

Navigation Path

From the HTTP Page—AAA Tab , on page 34, click the **Add** button beneath the Command Authorization Override table.

Related Topics

- HTTP Policy Page , on page 32
- AAA Policy Page , on page 6

Field Reference

Table 15: Command Authorization Dialog Box

Element	Description
Privilege Level	The privilege level for which you want to define a command accounting list. Valid values range from 0 to 15.

Element	Description
Prioritized Method List	Defines a sequential list of methods to be used when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. Supported methods include TACACS+, Local, and None. **Note** If you select None as a method, it must appear as the last method in the list.

Line Access on Cisco IOS Routers

Security Manager enables you to configure command line access (also called EXEC access) to a router using the following methods:

- Console port—Physical connection via a standard RS232 cable for local access. For more information, see:
  - Defining Console Port Setup Parameters , on page 37
  - Defining Console Port AAA Settings , on page 39
- VTY lines—Virtual terminal lines for remote access, typically using protocols such as Telnet, SSH, or rlogin. For more information, see:
  - Defining VTY Line Setup Parameters , on page 40
  - Defining VTY Line AAA Settings , on page 42

After you configure and deploy these policies, you can use these lines to communicate with individual devices directly when you want to configure or diagnose them using the CLI.

Defining Console Port Setup Parameters

The console port on a router is generally used for local system access by an administrator with physical access to the device. By default, the console port is set up as follows:

- All permitted users have privileged access to the router, including all configuration commands (privilege level 15).
- The line is disconnected after 10 minutes without user input.
- Incoming connections are not permitted.
- Outgoing connections support Telnet only.

In addition to modifying any of the default settings, you can optionally define the following settings:

- The password for accessing the console.
- Whether to disable all EXEC sessions on the console.
- Incoming and outgoing ACLs that restrict the connections that are permitted on the console.
- Whether VRF connections are permitted on the console.

Related Topics

- Line Access on Cisco IOS Routers , on page 37

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Device Access > Line Access > Console** from the Policy selector, then click the **Setup** tab in the work area.
- (Policy view) Select **Router Platform > Device Admin > Device Access > Line Access > Console** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Setup** tab.

The Console Setup tab is displayed. See Table 16: Console Page—Setup Tab , on page 45 for a description of the fields on this tab.

Step 2 (Optional) Enter the password for accessing the console port, then enter it again in the Confirm field.

Step 3 (Optional) Modify the default (15) granted to users of the console port. See Console Page—Authorization Tab , on page 47.

Step 4 (Optional) Select the **Disable all the EXEC sessions to the router via this line** check box to prevent any incoming connections via the console.

Note
Selecting this option blocks all access to the device via the console port.

Step 5 (Optional) Modify the default timeout after which the line is disconnected if no user input is detected.

Note
Setting this value to 0 disables the timeout. Disabling the timeout could compromise the security of your network.

Step 6 (Optional) Specify which protocols can be used for outbound connections on the console port:

- All—All supported protocols are permitted.
- None—No protocols are permitted.
- Protocol—Enables one or more of the following protocols: SSH, Telnet, and rlogin.

Note
You must configure AAA authentication on devices where the console port permits the SSH and rlogin protocols. See Defining Console Port AAA Settings , on page 39.

Step 7 (Optional) Enter the names of ACLs that restrict incoming and outgoing connections between the device and the addresses in these lists, or click **Select** to select the ACL object or to create a new one. At the top of the selector, in the Type field, select the ACL type as either Standard or Extended.

Step 8 (Optional) Click the **AAA** tab to define authentication, authorization, and accounting settings for the console port. See Defining Console Port AAA Settings , on page 39.

Defining Console Port AAA Settings

By default, authentication, authorization, and accounting are not performed on the console port. When you configure one or more of these access control options, you can either make use of the default method lists defined in the device's AAA policy or define a custom method list containing one or more AAA methods.

Related Topics

- Defining Console Port Setup Parameters , on page 37
- Line Access on Cisco IOS Routers , on page 37

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Device Access > Line Access > Console** from the Policy selector, then click the **Authentication** tab in the work area.
- (Policy view) Select **Router Platform > Device Admin > Device Access > Line Access > Console** from the Policy Type selector. Select an existing policy or create a new one, and then click the **Authentication** tab.

The Console Authentication tab is displayed.

Step 2 (Optional) Select the authentication method to perform on users who attempt to access the console line.

See Table 17: Console Page—Authentication Tab , on page 47 for a description of the fields on the Authentication tab.

Note
If you select local authentication, preview the full configuration before deployment to make sure that the **aaa new-model** command is not configured by another policy (for example, by configuring a method list in the AAA policy) or is already configured on the device itself.

Step 3 (Optional) On the Authorization tab, select the authorization method to perform on users who access the console line and begin an EXEC session.

See Table 18: Console Page—Authorization Tab , on page 48 for a description of the fields on the Authorization tab.

Note
RADIUS uses the same server for authentication and authorization. Therefore, if you use define a RADIUS method list for authentication, you must define the same method list for authorization.

Step 4 (Optional) Create command authorization definitions for specific privilege levels:

a) Click the **Add** button under the Commands Authorization table. The Command Authorization dialog box is displayed. See Table 26: Command Authorization Dialog Box—Line Access , on page 63 for details.
b) Configure the command authorization definition as required.
c) Click **OK**. The dialog box closes and the authorization method is displayed in the Commands Authorization table.
d) Repeat 6.a, on page 40 through 6.c, on page 40 to create additional command authorization definitions.

Step 5 (Optional) On the Accounting tab, select the EXEC and connection accounting methods to perform on users who access the console line.

See Table 19: Console Page—Accounting Tab , on page 49 for a description of the fields on this tab.

Step 6 (Optional) Create command accounting definitions for specific privilege levels:

a) Click the **Add** button under the Commands Accounting table. The Command Accounting Dialog Box—Line Access , on page 64 is displayed.
b) Configure the command accounting definition as required.
c) Click **OK**. The dialog box closes and the accounting method is displayed in the Commands Accounting table.
d) Repeat 6.a, on page 40 through 6.c, on page 40 to create additional command accounting definitions.

Defining VTY Line Setup Parameters

All Cisco IOS routers are configured by default with five VTY lines (labeled 0-4) that have the following settings:

- All permitted users have privileged access to the router, including all configuration commands (privilege level 15).
- VTY lines are disconnected after 10 minutes without user input.
- Incoming connections are not permitted.
- Outgoing connections support Telnet only.

You can use Security Manager to modify the default settings on these five VTY lines or to configure additional lines (up to a maximum of 16). In addition, you can optionally configure the following settings on each line:

- The password for accessing the line.
- Whether to disable all EXEC sessions on the line.
- Incoming and outgoing ACLs that restrict the connections that are permitted on the line.
- Whether VRF connections are permitted on the line.

Defining Groups of VTY Lines

You can configure multiple VTY lines as a contiguous group, which enables you to define identical settings for all the lines in the group with one procedure. All the lines within the group must fall within one of two ranges, 0-4 or 6-15. The group cannot overlap these two ranges.

The rules for configuring VTY line 5 are as follows. Line 5 can be part of the same definition as lines 0-4 only when there are no lines configured above line 5. If there are lines configured above line 5, you cannot include line 5 in the definition for lines 0-4, even if their configurations are the same. Line 5 *can* be included in the definition of the lines above line 5 if their configurations are the same.

For example, if lines 0-5 all share one configuration and lines 6-9 have a different configuration, you need to create three definitions—one definition for lines 0-4, a second definition for line 5, and a third definition for lines 6-9.

Note When you configure VTY lines, bear in mind that users are assigned a line at random when they connect to the device.

Note You can create only one definition per VTY line. An error is displayed if you create a VTY line definition that overlaps an existing definition.

Note If you use Security Manager to configure the default VTY lines (0-4), your definition overrides the default settings on the device. If you later delete this definition from Security Manager, the input protocol settings are retained and the other default settings are restored. This ensures that you always have VTY lines available for remote access to the device.

Note You can use the CLI or FlexConfigs to configure additional VTY lines on devices that support more than 16 lines.

Related Topics

- Line Access on Cisco IOS Routers , on page 37

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Device Access > Line Access > VTY** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > Line Access > VTY** from the Policy Type selector. Select an existing policy or create a new one.

The VTY page is displayed. See Table 20: VTY Lines Page , on page 52 for a description of the fields on this page.

Step 2 Click the **Add** button beneath the Lines table, or select a line definition and then click the **Edit** button. The Setup tab of the VTY Lines dialog box is displayed. See Table 21: VTY Line Dialog Box , on page 54 for a description of the fields on this tab.

Step 3 Enter the relative line number of the VTY line. If you are configuring a group of VTY lines, enter the first and last numbers of the group in the fields provided.

Step 4 (Optional) Enter the password for accessing the console line, then enter it again in the Confirm field.

Step 5 (Optional) Modify the default Privilege (15) granted to users of this VTY line (or group of lines).

Step 6 (Optional) Select the **Disable all the EXEC sessions to the router via this line** check box to prevent any incoming connections over this VTY line (or group of lines).

Step 7 (Optional) Modify the default timeout after which the line is disconnected if no user input is detected.

Note
Setting this value to 0 to disables the timeout. Disabling the timeout could cause abandoned sessions to block available VTY lines. It can also compromise the security of your network.

Step 8 (Optional) Specify which protocols can be used for inbound and outbound connections on this VTY line (or group of lines):

- All—All supported protocols are permitted.
- None—No protocols are permitted.
- Protocol—Enables one or more of the following protocols: SSH, Telnet, and rlogin.

Caution
Setting the inbound connections setting to None might prevent Security Manager from connecting to the device after deployment.

Note
You must configure AAA authentication when the VTY line permits the SSH and rlogin protocols. See Defining VTY Line AAA Settings , on page 42.

Step 9 (Optional) Enter the names of ACLs that restrict incoming and outgoing connections between the device and the addresses in these lists, or click **Select** to select an ACL object from a list or to create a new one. You can choose from standard or extended ACLs.

Tip
Defining an inbound ACL is a good way to reserve a VTY line for administrative access only.

Step 10 (Optional) Click the **AAA** tab to define authentication, authorization, and accounting settings for this VTY line (or group of lines). See Defining VTY Line AAA Settings , on page 42.

Step 11 Click **OK** to save your definitions locally on the client and close the dialog box. Your definitions are displayed in the Lines table.

Note
To remove a VTY line definition, select it, then click **Delete**. If you delete a VTY line from an IOS device, any subsequent lines are also deleted. For example, if the device contains lines 0-9 and you delete line 5, lines 6-9 are deleted as well. If you delete the definition for lines 0-4 from Security Manager, the router retains the inbound protocol definition and restores the other default settings for these lines on the device. This ensures that five VTY lines are always available.

Defining VTY Line AAA Settings

By default, authentication, authorization, and accounting are not performed on VTY lines. When you configure one or more of these access control options, you can either make use of the default method lists defined in the device's AAA policy or define a custom method list containing one or more AAA methods.

Before You Begin

- Define the basic parameters of the VTY line or group of VTY lines. See Defining VTY Line Setup Parameters , on page 40.

Related Topics

- Defining VTY Line Setup Parameters , on page 40

- Line Access on Cisco IOS Routers , on page 37

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Device Admin** > **Device Access** > **Line Access** > **VTY** from the Policy selector.
- (Policy view) Select **Router Platform** > **Device Admin** > **Device Access** > **Line Access** > **VTY** from the Policy Type selector. Select an existing policy or create a new one.

The VTY page is displayed. See Table 20: VTY Lines Page , on page 52 for a description of the fields on this page.

Step 2 Select a VTY line definition in the Lines tables, click the **Edit** button to display the VTY Line dialog box, then click the **Authentication** tab.

Step 3 (Optional) Select the authentication method to perform on users who attempt to access the VTY line.

See Table 23: VTY Line Dialog Box—Authentication Tab , on page 58 for a description of the fields on this tab.

Note
If you select local authentication, preview the full configuration before deployment to make sure that the **aaa new-model** command is not configured by another policy (for example, by configuring a method list in the AAA policy) or is already configured on the device itself.

Step 4 (Optional) On the Authorization tab, select the authorization method to perform on users who access the VTY line and begin an EXEC session.

See Table 24: VTY Line Dialog Box—Authorization Tab , on page 59 for a description of the fields on the Authorization tab.

Note
RADIUS uses the same server for authentication and authorization. Therefore, if you use define a RADIUS method list for authentication, you must define the same method list for authorization.

Step 5 (Optional) Create command authorization definitions for specific privilege levels:

a) Click the **Add** button under the Commands Authorization table. The Command Authorization Override Dialog Box , on page 36 is displayed.
b) Configure the command authorization definition as required.
c) Click **OK**. The dialog box closes and the authorization method is displayed in the Commands Authorization table.
d) Repeat 5.a, on page 43 through 5.c, on page 43 to create additional command authorization definitions.

Step 6 (Optional) On the Accounting tab, select the EXEC and connection accounting methods to perform on users who attempt to access the VTY line.

See Table 25: VTY Line Dialog Box—Accounting Tab , on page 60 for a description of the fields on the Accounting tab.

Step 7 (Optional) Create command accounting definitions for specific privilege levels:

a) Click the **Add** button under the Commands Accounting table. The Command Accounting Dialog Box—Line Access , on page 64 is displayed.
b) Configure the command accounting definition as required.
c) Click **OK**. The dialog box closes and the accounting method is displayed in the Commands Accounting table.

d) Repeat 7.a, on page 43 through 7.c, on page 43 to create additional command accounting definitions.

Console Policy Page

Use the Console page to configure access to the router over the console port. You can configure console policies on a Cisco IOS router from the following tabs on the Console policy page:

- Console Page—Setup Tab , on page 44
- Console Page—Authentication Tab , on page 46
- Console Page—Authorization Tab , on page 47
- Console Page—Accounting Tab , on page 49

For more information, see Line Access on Cisco IOS Routers , on page 37.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Line Access > Console** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > Line Access > Console** from the Policy Type selector. Right-click **Console** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- VTY Policy Page , on page 52

Console Page—Setup Tab

Use the Setup tab of the Console page to define the basic parameters of the console port. This includes the password for accessing the port, the privilege level assigned to users, the protocols that are permitted, and the ACLs that limit access.

Navigation Path

Go to the Console Policy Page , on page 44, then click the **Setup** tab.

Related Topics

- Console Page—Authentication Tab , on page 46
- Console Page—Authorization Tab , on page 47
- Console Page—Accounting Tab , on page 49
- VTY Line Dialog Box—Setup Tab , on page 54

Field Reference

Table 16: Console Page—Setup Tab

Element	Description
Password	The password for accessing the console port. The password is case sensitive and can contain up to 80 alphanumeric characters. The first character cannot be a number. Spaces are not allowed. Enter the password again in the Confirm field.
Privilege Level	The privilege level assigned to users connected to the console port. Valid values range from 0 to 15: • 0—Grants access to these commands only: **disable**, **enable**, **exit**, **help**, and **logout**. • 1—Enables nonprivileged access to the router (normal EXEC-mode use privileges). • 15—Enables privileged access to the router (traditional enable privileges). **Note** Levels 2-14 are not normally used in a default configuration, but custom configurations can be created by moving commands that are normally at level 15 to a lower level and commands that are normally at level 1 to a higher level. You can configure the privilege levels of commands using the CLI or by defining a FlexConfig. **Note** If you do not define a value, level 1 is assigned by default. This value does not appear in the device configuration.
Disable all the EXEC sessions to the router via this line	When selected, disables EXEC sessions over this line. Select this option when you want to allow only an outgoing connection on the console. This option is useful for keeping the console port free from unsolicited incoming data that can tie up the line. When deselected, EXEC sessions are enabled on the console port. This is the default. **Note** Selecting this option blocks all access to the device via the console port.
Exec Timeout	The amount of time (in seconds) that the EXEC command interpreter waits to detect user input on the console port. If no input is detected, the line is disconnected. Valid values range from 0 to 2147483. The default is 600 (10 minutes). Setting the value to 0 disables the timeout. **Note** Although the timeout is defined in seconds, it appears in the CLI in the format [mm ss].

Element	Description

Output Protocols	The protocols that you can use for outgoing connections on the console port:
	• All—All supported protocols are permitted. Supported protocols include LAT, MOP, NASI, PAD, rlogin, SSH, Telnet, and V.120.
	• None—No protocols are permitted. This makes the port unusable by outgoing connections.
	• Protocol—Enables one or more of the following protocols:
	  • SSH—Secure Shell protocol.
	  • Telnet—Standard TCP/IP terminal emulation protocol.
	  • rlogin—UNIX rlogin protocol.
	Note
	SSH and rlogin require that you configure AAA authentication. See Console Page—Authentication Tab , on page 46.
	Note
	Not all IOS Software Versions support rlogin as an output protocol.

Inbound Access List	The name of the ACL object that restricts incoming connections on the console port. Enter the name of the ACL object, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it.
Permit VRF Interface Connections	Applies only when an inbound ACL is defined on the console port. When selected, accepts incoming connections from interfaces that belong to a VRF. When deselected, rejects incoming connections from interfaces that belong to a VRF.
Outbound Access List	The name of the ACL object that restricts outgoing connections on the console port. Enter the name of an ACL object, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it.

Console Page—Authentication Tab

Use the Authentication tab of the Console page to define the AAA authentication methods to perform on users who attempt to access the console port.

Navigation Path

Go to the Console Policy Page , on page 44, then click the **Authentication** tab.

Related Topics

- Console Page—Setup Tab , on page 44
- Console Page—Authorization Tab , on page 47
- Console Page—Accounting Tab , on page 49

- VTY Line Dialog Box—Authentication Tab , on page 57

Field Reference

Table 17: Console Page—Authentication Tab

Element	Description
Authenticate Using	Authentication settings for the console port: • None—Authentication is not performed. This is the default. • Local Database—Uses the local username database for authentication. • AAA Policy Default List—Uses the default authentication method list that is defined in the device's AAA policy. See AAA Page—Authentication Tab , on page 7. • Custom Method List—Uses the authentication methods specified in the Authentication Method List field. **Note** If you select local authentication, preview the full configuration before deployment to make sure that the **aaa new-model** command is not configured by another policy (for example, by configuring a method list in the AAA policy) or is already configured on the device itself.
Prioritized Method List	Applies only when Custom Method List is selected as the authentication method. Defines a sequential list of methods to be queried when authenticating a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.

Console Page—Authorization Tab

Use the Authorization tab of the Console page to define the EXEC and command authorization methods to perform on users who access the console port.

Note You must enable AAA services on the router to use this feature; otherwise, deployment will fail. See Defining AAA Services , on page 4.

Navigation Path

Go to the Console Policy Page , on page 44, then click the **Authorization** tab.

Related Topics

- Console Page—Setup Tab , on page 44
- Console Page—Authentication Tab , on page 46
- Console Page—Accounting Tab , on page 49
- VTY Line Dialog Box—Authorization Tab , on page 58
- Filtering Tables

Field Reference

Table 18: Console Page—Authorization Tab

Element	Description
EXEC Authorization settings	
Authorize EXEC Operations Using	The authorization method that determines whether a user is allowed to run an EXEC session: • None—Authorization is not performed. This is the default. • AAA Policy Default List—Uses the default authorization method list that is defined in the device's AAA policy. See AAA Page—Authorization Tab , on page 8. • Custom Method List—Uses the authorization methods specified in the EXEC Method List field.
Prioritized Method List	Applies only when Custom Method List is selected as the EXEC method. Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list. **Note** RADIUS uses the same server for authentication and authorization. Therefore, if you use define a RADIUS method list for authentication, you must define the same method list for authorization.
Command Authorization settings	

Element	Description
Privilege Level	The privilege level to which the command authorization definition applies.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Authorization Dialog Box—Line Access , on page 63. From here you can configure a command authorization definition.
Edit button	Opens the Command Authorization Dialog Box—Line Access , on page 63. From here you can edit the command authorization definition.
Delete button	Deletes the selected command authorization definitions from the table.

Console Page—Accounting Tab

Use the Accounting tab of the Console page to define the EXEC, connection, and command accounting methods to perform on users who access the console port.

Note You must enable AAA services on the router to use this feature; otherwise, deployment will fail. See Defining AAA Services , on page 4.

Navigation Path

Go to the Console Policy Page , on page 44, then click the **Accounting** tab.

Related Topics

- Console Page—Setup Tab , on page 44
- Console Page—Authentication Tab , on page 46
- Console Page—Authorization Tab , on page 47
- VTY Line Dialog Box—Accounting Tab , on page 60
- Filtering Tables

Field Reference

Table 19: Console Page—Accounting Tab

Element	Description
EXEC Accounting settings	

Element	Description
Perform EXEC Accounting Using	The accounting method to use for recording basic information about user EXEC sessions: • None—Accounting is not performed. This is the default. • AAA Policy Default List—Uses the default EXEC accounting method list that is defined in the device's AAA policy. See AAA Page—Accounting Tab , on page 10. • Custom Method List—Uses the accounting methods specified in the EXEC Method List field. EXEC accounting records basic details about EXEC sessions, such as the username, date, start and stop times, and the access server IP address.
Generate Accounting Records for	Applies only when Custom Method List is selected as the EXEC method. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.
Prioritized Method List	Applies only when Custom Method List is selected as the EXEC method. Defines a sequential list of methods to be queried when creating accounting methods for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Method List is selected as the EXEC method. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.
Connection Accounting settings	

Element	Description
Perform Connection Accounting Using	The accounting method to use for recording information about outbound connections made over the console line: • None—Accounting is not performed. This is the default. • AAA Policy Default List—Uses the default connection accounting method list that is defined in the device's AAA policy. See AAA Page—Accounting Tab , on page 10. • Custom Method List—Uses the accounting methods specified in the Connection Method List field. Connection accounting records details about outgoing connections over the line, such as Telnet and rlogin connections.
Generate Accounting Records for	Applies only when Custom Method List is selected as the connection method. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.
Prioritized Method List	Applies only when Custom Method List is selected as the connection method. Defines a sequential list of methods to be queried when creating accounting methods for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Custom Method List is selected as the connection method. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.
Command Accounting settings	

Element	Description
Privilege Level	The privilege level to which the command authorization definition applies.
Generate Accounting Records for	The points in the process where the device sends an accounting notice to the accounting server.
Enable Broadcast	Whether accounting records are broadcast to multiple servers simultaneously.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Accounting Dialog Box—Line Access , on page 64. From here you can configure a command accounting definition.
Edit button	Opens the Command Accounting Dialog Box—Line Access , on page 64. From here you can edit the command accounting definition.
Delete button	Deletes the selected command accounting definitions from the table.

VTY Policy Page

Use the VTY page to configure up to 16 VTY lines for remote access to the router. In addition to configuring individual lines, you can configure a group of lines that share the same definition.

For more information, see Line Access on Cisco IOS Routers , on page 37.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Line Access > VTY** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > Line Access > VTY** from the Policy Type selector. Right-click **VTY** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Console Policy Page , on page 44
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 20: VTY Lines Page

Element	Description
Line	The relative line number of the VTY line. This field may also contain multiple VTY lines configured as a contiguous group.

Element	Description
Line/Line Group Parameters	
Input Protocols	The protocols that you can use for incoming connections on the VTY line.
Output Protocols	The protocols that you can use for outgoing connections on the VTY line.
Privilege Level	The privilege level assigned to users.
Exec Timeout	The amount of time the EXEC command interpreter waits until user input is detected.
Inbound ACL	The ACL used to limit inbound traffic.
Outbound ACL	The ACL used to limit outbound traffic.
Authentication	The type of AAA authentication used.
Authorization	The types of AAA authorization used.
Accounting	The types of AAA accounting used.
VTY Line Page Buttons	
Add button	Opens the VTY Line Dialog Box , on page 53. From here you can define a VTY line or line group.
Edit button	Opens the VTY Line Dialog Box , on page 53. From here you can edit the VTY line or line group.
Delete button	Deletes the selected VTY lines from the table. If you delete a VTY line from an IOS device, any subsequent lines are also deleted. For example, if the device contains lines 0-9 and you delete line 5, lines 6-9 are deleted as well. **Note** If you delete any of the default VTY lines (0-4) on the device, the input protocol settings are retained and the other default settings are restored. This helps prevent you from cutting off remote access to the device.

VTY Line Dialog Box

Use the VTY Line dialog box to configure one or more VTY lines (up to 16) that enable remote users to access the router. When you configure a VTY line, you can define the type of authentication and authorization to perform on users who access the lines.

Navigation Path

Go to the VTY Policy Page , on page 52, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Line Access on Cisco IOS Routers , on page 37
- Console Policy Page , on page 44

Field Reference

Table 21: VTY Line Dialog Box

Element	Description
Setup tab	Defines the basic configuration of the VTY line or line group. See VTY Line Dialog Box—Setup Tab , on page 54.
Authentication tab	Defines the type of AAA authentication to perform on users who access the VTY line. See VTY Line Dialog Box—Authentication Tab , on page 57.
Authorization tab	Defines the types of AAA authorization to perform on users who access the VTY line. See VTY Line Dialog Box—Authorization Tab , on page 58.
Accounting tab	Defines the types of AAA accounting to perform on users who access the VTY line. See VTY Line Dialog Box—Accounting Tab , on page 60.

VTY Line Dialog Box—Setup Tab

Use the Setup tab of the VTY Line dialog box to define the basic parameters of the VTY line. This includes the password for accessing the line, the privilege level assigned to users, the protocols that are permitted on the line, and the ACLs that limit access.

Navigation Path

Go to the VTY Line Dialog Box , on page 53, then click the **Setup** tab.

Related Topics

- Defining VTY Line Setup Parameters , on page 40
- VTY Line Dialog Box—Authentication Tab , on page 57
- VTY Line Dialog Box—Authorization Tab , on page 58
- VTY Line Dialog Box—Accounting Tab , on page 60
- Console Page—Setup Tab , on page 44

Field Reference

Table 22: VTY Line Dialog Box—Setup Tab

Element	Description
Starting VTY Line Number	The relative line number of the VTY line. If you are configuring a group of VTY lines, enter the number of the first line in the group. Valid values range from 0 to 15. **Note** Although different routers support a different number of VTY lines (from four to several thousand), Security Manager supports a maximum of 16 lines per device. You cannot configure the same line number more than once.
Ending VTY Line Number	Applies only when configuring a group of lines. The relative line number of the last VTY line in the group. **Note** When you configure a group of lines, all the lines in the group must fall within one of two ranges, 0-4 or 6-15.
Password	The password for accessing this VTY line. The password is case sensitive and can contain up to 80 alphanumeric characters. The first character cannot be a number. Spaces are not allowed. Enter the password again in the Confirm field.
Privilege Level	The privilege level assigned to users on this VTY line. Valid values range from 0 to 15: • 0—Grants access to these commands only: **disable**, **enable**, **exit**, **help**, and **logout**. • 1—Enables nonprivileged access to the router (normal EXEC-mode use privileges). • 15—Enables privileged access to the router (traditional enable privileges). **Note** Levels 2-14 are not normally used in a default configuration, but custom configurations can be created by moving commands that are normally at level 15 to a lower level and commands that are normally at level 1 to a higher level. You can configure the privilege levels of commands using the CLI or by defining a FlexConfig. **Note** If you do not define a value, level 1 is assigned by default. This value does not appear in the device configuration.
Disable all the EXEC sessions to the router via this line	When selected, EXEC sessions are disabled over this line. Select this option when you want to allow only an outgoing connection on this line. This option is useful for keeping a particular line free from unsolicited incoming data that can tie up the line. When deselected, EXEC sessions are enabled over this line. This is the default.

Element	Description
Exec Timeout	The amount of time (in seconds) that the EXEC command interpreter waits to detect user input on the line. If no input is detected, the line is disconnected. Valid values range from 0 to 2147483. The default is 600 (10 minutes). Setting the value to 0 disables the timeout. **Note** Although the timeout is defined in seconds, it appears in the CLI in the format [mm ss].
Input Protocols	The protocols that you can use for incoming connections on this line: • All—All supported protocols are permitted. Supported protocols include LAT, MOP, NASI, PAD, rlogin, SSH, Telnet, and V.120. • None—No protocols are permitted. This makes the port unusable by incoming SSH, Telnet, and rlogin connections. **Note** Setting the input protocols setting to None might prevent Security Manager from connecting to the device after deployment. The device can still be managed using SSL, if SSL is enabled in the HTTP policy. See HTTP Page—Setup Tab , on page 33. • Protocol—Enables one or more of the following protocols: • SSH—Secure Shell protocol. • Telnet—Standard TCP/IP terminal emulation protocol. • rlogin—UNIX rlogin protocol. **Note** SSH and rlogin require that you configure AAA authentication. See VTY Line Dialog Box—Authentication Tab , on page 57. **Note** Not all IOS Software Versions support rlogin as an input protocol.

Element	Description

Output Protocols	The protocols that you can use for outgoing connections on this line:
	• All—All supported protocols are permitted. Supported protocols include LAT, MOP, NASI, PAD, rlogin, SSH, Telnet, and V.120.
	• None—No protocols are permitted. This makes the port unusable by outgoing connections.
	• Protocol—Enables one or more of the following protocols:
	  • SSH—Secure Shell protocol.
	  • Telnet—Standard TCP/IP terminal emulation protocol.
	  • rlogin—UNIX rlogin protocol.
	Note
	SSH and rlogin require that you configure AAA authentication. See VTY Line Dialog Box—Authentication Tab , on page 57.
	Note
	Not all IOS Software Versions support rlogin as an output protocol.

Inbound Access List	The name of the ACL object that restricts incoming connections on this line. Enter the name of the ACL object, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it.
Permit VRF Interface Connections	Applies only when an inbound ACL is defined on this line. When selected, accepts incoming connections from interfaces that belong to a VRF. When deselected, rejects incoming connections from interfaces that belong to a VRF.
Outbound Access List	The name of the ACL object that restricts outgoing connections on this line. Enter the name of the ACL object, or click **Select** to select it. If the object that you want is not listed, click the **Create** button to create it.

VTY Line Dialog Box—Authentication Tab

Use the Authentication tab of the VTY Line dialog box to define the authentication methods to perform on users who attempt to access the selected VTY line or group of lines.

Navigation Path

Go to the VTY Line Dialog Box , on page 53, then click the **Authentication** tab.

Related Topics

- Defining VTY Line AAA Settings , on page 42
- VTY Line Dialog Box—Setup Tab , on page 54
- VTY Line Dialog Box—Authorization Tab , on page 58
- VTY Line Dialog Box—Accounting Tab , on page 60

- Console Page—Authentication Tab , on page 46

Field Reference

Table 23: VTY Line Dialog Box—Authentication Tab

Element	Description
Authenticate Using	Authentication settings for the VTY line: • None—Authentication is not performed. This is the default. • Local Database—Uses the local username database for authentication. • AAA Policy Default List—Uses the default authentication method list that is defined in the device's AAA policy. See AAA Page—Authentication Tab , on page 7. • Custom Method List—Uses the authentication methods specified in the Prioritized Method List field. **Note** If you select local authentication, preview the full configuration before deployment to make sure that the **aaa new-model** command is not configured by another policy (for example, by configuring a method list in the AAA policy) or is already configured on the device itself.
Prioritized Method List	Applies only when Custom Method List is selected as the authentication method. Defines a sequential list of methods to be queried when authenticating a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authenticate users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.

VTY Line Dialog Box—Authorization Tab

Use the Authorization tab of the VTY Line dialog box to define the EXEC and command authorization methods to perform on users who access the selected VTY line or group of lines.

Note You must enable AAA services on the router to use this feature; otherwise, deployment will fail. See Defining AAA Services , on page 4.

Navigation Path

Go to the VTY Line Dialog Box , on page 53, then click the **Authorization** tab.

Related Topics

- Defining VTY Line AAA Settings , on page 42
- VTY Line Dialog Box—Setup Tab , on page 54
- VTY Line Dialog Box—Authentication Tab , on page 57
- VTY Line Dialog Box—Accounting Tab , on page 60
- Console Page—Authentication Tab , on page 46
- Filtering Tables

Field Reference

Table 24: VTY Line Dialog Box—Authorization Tab

Element	Description
EXEC Authorization settings	
Authorize EXEC Operations Using	The authorization method that determines whether a user is allowed to run an EXEC session: • None—Authorization is not performed. This is the default. • AAA Policy Default List—Uses the default authorization method list that is defined in the device's AAA policy. See AAA Page—Authorization Tab , on page 8. • Custom Method List—Uses the authorization methods specified in the Prioritized Method List field.
Prioritized Method List	Applies only when Custom Method List is selected as the EXEC method. Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list. **Note** RADIUS uses the same server for authentication and authorization. Therefore, if you use define a RADIUS method list for authentication, you must define the same method list for authorization.
Command Authorization settings	
Privilege Level	The privilege level to which the command authorization definition applies.

Element	Description
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Authorization Dialog Box—Line Access , on page 63. From here you can configure a command authorization definition.
Edit button	Opens the Command Authorization Dialog Box—Line Access , on page 63. From here you can edit the command authorization definition.
Delete button	Deletes the selected command authorization definitions from the table.

VTY Line Dialog Box—Accounting Tab

Use the Accounting tab of the VTY Line dialog box to define the EXEC, connection, and command accounting methods to perform on users who access the selected VTY line or group of lines.

Note You must enable AAA services on the router to use this feature; otherwise, deployment will fail. See Defining AAA Services , on page 4.

Navigation Path

Go to the VTY Line Dialog Box , on page 53, then click the **Accounting** tab.

Related Topics

- Defining VTY Line AAA Settings , on page 42
- VTY Line Dialog Box—Setup Tab , on page 54
- VTY Line Dialog Box—Authentication Tab , on page 57
- Console Page—Accounting Tab , on page 49
- Filtering Tables

Field Reference

Table 25: VTY Line Dialog Box—Accounting Tab

Element	Description
EXEC Accounting settings	

Element	Description
Perform EXEC Accounting Using	The accounting method to use for recording basic information about user EXEC sessions: • None—Accounting is not performed. This is the default. • AAA Policy Default List—Uses the default EXEC accounting method list that is defined in the device's AAA policy. See AAA Page—Accounting Tab , on page 10. • Custom Method List—Uses the accounting methods specified in the Prioritized Method List field. EXEC accounting records basic details about EXEC sessions, such as the username, date, start and stop times, and the access server IP address.
Generate Accounting Records for	Applies only when Custom Method List is selected as the EXEC method. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.
Prioritized Method List	Applies only when Custom Method List is selected as the EXEC method. Defines a sequential list of methods to be queried when creating accounting methods for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Method List is selected as the EXEC method. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.
Connection Accounting settings	

Element	Description
Perform Connection Accounting Using	The accounting method to use for recording information about outbound connections made over the VTY line: • None—Accounting is not performed. This is the default. • AAA Policy Default List—Uses the default connection accounting method list that is defined in the device's AAA policy. See AAA Page—Accounting Tab , on page 10. • Custom Method List—Uses the accounting methods specified in the Prioritized Method List field. Connection accounting records details about outgoing connections over the line, such as Telnet and rlogin connections.
Generate Accounting Records for	Applies only when Custom Method List is selected as the connection method. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.
Prioritized Method List	Applies only when Custom Method List is selected as the connection method. Defines a sequential list of methods to be queried when creating accounting methods for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Custom Method List is selected as the connection method. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.
Command Accounting settings	

Element	Description
Privilege Level	The privilege level to which the command authorization definition applies.
Generate Accounting Records for	The points in the process where the device sends an accounting notice to the accounting server.
Enable Broadcast	Whether accounting records are broadcast to multiple servers simultaneously.
Prioritized Method List	The method list to use when authorizing users with this privilege level.
Add button	Opens the Command Accounting Dialog Box—Line Access , on page 64. From here you can configure a command accounting definition.
Edit button	Opens the Command Accounting Dialog Box—Line Access , on page 64. From here you can edit the command accounting definition.
Delete button	Deletes the selected command accounting definitions from the table.

Command Authorization Dialog Box—Line Access

Use the Command Authorization dialog box to define which methods to use when authorizing the EXEC commands that are associated with a given privilege. This enables you to authorize all commands associated with a specific privilege level, from 0 to 15.

Navigation Path

From the Console Page—Authorization Tab , on page 47 or the VTY Line Dialog Box—Authorization Tab , on page 58, click the **Add** button beneath the Command Authorization table.

Related Topics

- Console Policy Page , on page 44
- VTY Policy Page , on page 52

Field Reference

Table 26: Command Authorization Dialog Box—Line Access

Element	Description
Privilege Level	The privilege level for which you want to define a command authorization list. Valid values range from 0 to 15. **Note** If you do not define a value, level 1 is assigned by default. This value does not appear in the device configuration.
AAA Policy Default List	Select this option to apply the default authorization list defined in the device's AAA policy to the EXEC commands associated with this privilege level. See Command Accounting Dialog Box , on page 13.
Custom Method List	Select this option to define an authorization method list for this privilege level.

Element	Description
Prioritized Method List	Applies only when the Custom Method List option is selected. Defines a sequential list of methods to be queried when authorizing a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to authorize users using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.

Command Accounting Dialog Box—Line Access

Use the Command Accounting dialog box to define which methods to use when recording information about the EXEC commands that are executed for a given privilege. Each accounting record includes a list of the commands executed for that privilege level, as well as the date and time each command was executed, and the name of the user who executed it.

Navigation Path

From the Console Page—Accounting Tab , on page 49 or the VTY Line Dialog Box—Accounting Tab , on page 60, click the **Add** button beneath the Command Accounting table.

Related Topics

- Console Policy Page , on page 44
- VTY Policy Page , on page 52

Field Reference

Table 27: Command Accounting Dialog Box—Line Access

Element	Description
Privilege Level	The privilege level for which you want to define a command accounting list. Valid values range from 0 to 15. **Note** If you do not define a value, level 1 is assigned by default. This value does not appear in the device configuration.
AAA Policy Default List	Select this option to apply the default accounting list defined in the device's AAA policy to the EXEC commands executed for this privilege level.
Custom Method List	Select this option to define an accounting method list for this privilege level.

Element	Description
Generate Accounting Records for	Applies only when Custom Method List is selected. Defines when the device sends an accounting notice to the accounting server: • Start and Stop—Generates accounting records at the beginning and the end of the user process. The user process begins regardless of whether the accounting server receives the "start" accounting record. This is the default. • Stop Only—Generates an accounting record at the end of the user process only. • None—No accounting records are generated.
Prioritized Method List	Applies only when the Custom Method List option is selected. Defines a sequential list of accounting methods to be used when creating accounting records for a user. Enter the names of one or more AAA server group objects (up to four), or click **Select** to select them. Use the up and down arrows in the object selector to define the order in which the selected server groups should be used. If the object that you want is not listed, click the **Create** button to create it. The device tries initially to perform accounting using the first method in the list. If that method fails to respond, the device tries the next method, and so on, until a response is received. **Note** If you select None as a method, it must appear as the last method in the list.
Enable Broadcast to Multiple Servers	Applies only when Custom Method List is selected. When selected, enables the sending of accounting records to multiple AAA servers. Accounting records are sent simultaneously to the first server in each AAA server group defined in the method list. If the first server is unavailable, failover occurs using the backup servers defined within that group. When deselected, accounting records are sent only to the first server in the first AAA server group defined in the method list.

Optional SSH Settings on Cisco IOS Routers

Secure Shell (SSH) is an application and a protocol that uses encryption to provide secure communication between a client and server. You can use SSH to connect remotely to a Cisco IOS router over a VTY line and establish an EXEC session. SSH is the recommended replacement for other protocols, such as Telnet and rlogin, in environments where security is a concern.

All Cisco IOS routers are required to have SSH configured before they can be added to Security Manager. This is because Security Manager uses SSH (in addition to SSL) to communicate with them. The SSH policy provides a way to modify selected default settings and configure selected optional settings.

Related Topics

• Defining Optional SSH Settings , on page 66
• Understanding Device Communication Requirements

- Setting Up SSH

Defining Optional SSH Settings

SSH is configured by default with the following settings:

- Both SSH version 1 and SSH version 2 are supported.
- The negotiation phase is terminated if not completed successfully after 120 seconds.
- The router tries 3 times to authenticate SSH clients before disconnecting.

You can use Security Manager to modify these default settings and optionally configure the following settings:

- The source interface for SSH packets.
- The name of the RSA key pair to use.
- Whether to regenerate the key during the next deployment.

Before You Begin

- Make sure that SSH is enabled on the router. See Understanding Device Communication Requirements.
- Make sure that the VTY lines on the router allow inbound SSH traffic. See Defining VTY Line Setup Parameters , on page 40.
- Make sure that a hostname and domain name are configured on the router (unless you plan to use a different RSA key pair). You can use the CLI or the Hostname policy in Security Manager for this purpose. See Hostnames and Domain Names on Cisco IOS Routers , on page 80.

Related Topics

- Optional SSH Settings on Cisco IOS Routers , on page 65
- Setting Up SSH

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Device Admin** > **Device Access** > **Secure Shell** from the Policy selector.
- (Policy view) Select **Router Platform** > **Device Admin** > **Device Access** > **Secure Shell** from the Policy Type selector. Select an existing policy or create a new one.

The Secure Shell page is displayed. See Secure Shell Policy Page , on page 67 for a description of the fields on this page.

Step 2 (Optional) Modify the following default settings:

a) The version of SSH to support.
b) The timeout for completing the negotiation phase of the SSH connection.
c) The number of times to attempt authentication of the SSH client.

Step 3 (Optional) In the Source Interface field, enter the name of the interface or interface role whose address should be used as the source interface for all SSH packets sent to SSH clients, or click **Select** to select an interface role object from a list or to create a new one. The source interface must have an IP address.

If you do not enter a value in this field, the address of the closest interface to the destination is used.

Step 4 (Optional) Enter the name of the RSA key pair to use for SSH connections. If you do not enter a value in this field, the router uses the key pair that is based on the hostname and domain name.

Tip
Use the CLI command show crypto key mypubkey rsa to display the names and values of each key pair configured on the device.

Step 5 (Optional) Select the **Regenerate Key During Deployment** check box if you want the router to regenerate the RSA key pair used for SSH. This option is useful if you believe that the secrecy of the keys might be compromised. Enter the size of the modulus to use to regenerate the keys.

Note
You must remember to return to this policy after deployment to deselect the check box. If you do not do this, a new key is generated during each deployment.

Note
This option requires interaction with the device during deployment. Therefore, you should use it only when deploying to live devices, not when deploying to a file.

Note
A key pair must already exist on the device *before* you select this option; otherwise, deployment will fail. (This will typically be the case, since IOS routers must have SSH enabled to be added to Security Manager.)

Secure Shell Policy Page

Use the Secure Shell page to change the default SSH settings on the router and to define additional optional settings, if required.

For more information, see Optional SSH Settings on Cisco IOS Routers , on page 65.

Note You must configure SSH on the device using CLI commands before adding the device to Security Manager. This is because Security Manager uses SSH (as well as SSL) to communicate with Cisco IOS routers. For more information, see Setting Up SSH.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Secure Shell** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > Secure Shell** from the Policy Type selector. Right-click **Secure Shell** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Understanding Device Communication Requirements
- VTY Policy Page , on page 52
- Console Policy Page , on page 44

Field Reference

Table 28: Secure Shell Page

Element	Description
SSH Version	The version of SSH to use when connecting to the router: • 1 and 2—SSH version 1 and SSH version 2. This is the default. • 1—SSH version 1 only. • 2—SSH version 2 only.
Timeout	The amount of time the router should wait for the SSH client to respond during the negotiation phase before disconnecting. The default value (and the maximum) is 120 seconds. **Note** After negotiation finishes and the EXEC session begins, the timeout configured for the VTY line applies. See VTY Line Dialog Box—Setup Tab , on page 54.
Authentication Retries	The number of times the router attempts to authenticate SSH clients. Valid values range from 0 to 5. The default is 3.
Source Interface	The source address for all SSH packets sent to the SSH client. If you do not define a value in this field, the address of the closest interface to the destination (that is, the output interface through which SSH packets are sent) is used. Enter the name of an interface or interface role, or click **Select** to select the object from a list or to create a new one.
RSA Key Pair	The name of the RSA key pair to use for SSH connections. If you do not enter a value, the router uses the RSA key pair generated from its hostname and domain name. This is the default. **Tip** Use the CLI command **show crypto key mypubkey rsa** to display the names and values of each key pair configured on the device. These are the valid names that can be entered in this field.

Element	Description
Regenerate Key During Deployment	When selected, regenerates the RSA key pair on the router during the next deployment. This option is useful if you are concerned that the secrecy of the keys might be compromised. When deselected, a new key pair is not generated. **Note** This check box is *not* deselected automatically after deployment. If you do not return to this policy to deselect the check box, the key is regenerated each time you deploy. **Note** This option requires interaction with the device during deployment. Therefore, you should use it only when deploying to live devices, not when deploying to a file. **Note** A key pair must already exist on the device *before* you select this option; otherwise, deployment will fail. (This will typically be the case, since IOS routers must have SSH enabled in order to be added to Security Manager.)
Modulus Size	Applies only when the Regenerate Key check box is selected. The size of the modulus used to generate a new key pair. A larger modulus is more secure but takes longer to generate. Valid values range from 360 to 2048 bits. The default is 1024 bits.

SNMP on Cisco IOS Routers

Simple Network Management Protocol (SNMP) defines a standard way for network management stations or workstations to monitor the health and status of many types of devices, including switches, routers, and firewall devices. It comprises a protocol, a database-structure specification, and a set of management data objects. Each SNMP device or member is part of a *community* , which determines the access that each device has (read-only or read-write).

SNMP obtains information from the managed device through a Management Information Base (MIB). The MIB is a database of code blocks called MIB objects, each of which controls one specific function. The MIB object comprises MIB variables, which define the MIB object name, description, default value, and so forth. MIB objects are structured hierarchically in a MIB tree.

SNMP policies enable you to configure the behavior of the SNMP agent running on the router. The agent sends unsolicited information back to the SNMP host as events occur. These unsolicited messages, which are generated in response to significant, predetermined events on the router, are called traps.

The following topics describe the tasks you perform to create SNMP policies on Cisco IOS routers:

- Defining SNMP Agent Properties , on page 69
- Enabling SNMP Traps , on page 71

Defining SNMP Agent Properties

When you define the properties of the SNMP agent, you must define the community string and community string type, as well as the address and properties of the SNMP host that receives the traps.

SNMP community strings are embedded passwords to MIBs, which store data about the router's operation and are meant to be available to authenticated remote users. Two types of community strings exist: "public" community strings, which provide read-only access to all objects in the MIB (except community strings themselves), and "private" community strings, which provide read-write access to all objects in the MIB (except community strings).

SNMP hosts receive the traps generated by the router. You must define the address, password, and port number for accessing the SNMP host, as well as the SNMP version being used. Security Manager supports SNMP version 1, version 2c (also called "community-based SNMP") and version 3, which offers authentication and encryption.

Related Topics

- SNMP on Cisco IOS Routers , on page 69

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Device Admin** > **Device Access** > **SNMP** from the Policy selector.
- (Policy view) Select **Router Platform** > **Device Admin** > **Device Access** > **SNMP** from the Policy Type selector. Select an existing policy or create a new one.

The SNMP page is displayed. See Table 29: SNMP Page , on page 72 for a description of the fields on this page.

Step 2 Define the community string needed to access the MIB:

a) Under Permissions, click **Add** to display the Permission dialog box.
b) Define the string. See Table 30: Permission Dialog Box , on page 74 for a description of the available fields.
c) Click **OK** to save your definitions locally on the client and close the dialog box. Your definitions are displayed in the Permissions table.

Note
A warning is displayed if you attempt to edit or delete a community string that is in use by an SNMP host. If you continue with the operation, the device creates a private, read-only string that matches the definition for the host in the Trap Receiver table.

Step 3 Define the SNMP host that receives the traps generated by the SNMP agent:

a) Under Trap Receiver, click **Add** to display the Trap Receiver dialog box.
b) Define the host. See Trap Receiver Dialog Box , on page 74 for a description of the available fields.
c) Click **OK** to save your definitions locally on the client and close the dialog box. Your definitions are displayed in the Trap Receiver table.

Step 4 Under SNMP Server Properties, enter the location and contact information for the administrator responsible for routers configured with this SNMP policy.

This definition, which is text-only and does not affect the operation of the router, provides useful information to the manager of the SNMP host when the manager investigates a particular trap.

Step 5 Click **Configure Traps** to display the SNMP Traps dialog box, which is used to select which traps to enable on the router. For more information, see Enabling SNMP Traps , on page 71.

Enabling SNMP Traps

The router immediately sends notifications, also called SNMP traps, to the designated SNMP host (management station) when a defined condition occurs, such as a link up, link down, or a syslog event.

To enable SNMP traps, select the check box next to each relevant trap. Certain check boxes activate multiple, related traps.

Note Each trap that you enable consumes system resources. To lessen the impact on system performance, select only those traps that you need for network monitoring.

Related Topics

- SNMP on Cisco IOS Routers , on page 69

Procedure

Step 1 Open the SNMP page for defining SNMP server policies on Cisco IOS routers, as described in Defining SNMP Agent Properties , on page 69.

Step 2 On the SNMP page, click **Configure Traps**. The SNMP Traps dialog box is displayed.

Step 3 Select the check box next to each type of trap to enable. The traps are divided into the following four categories:

- Standard SNMP traps (for example, Authentication, Cold Start, and Warm Start).
- ISAKMP traps (related to Phase 1 of the IPsec process).
- IPsec traps (related to Phase 2 of the IPsec process).
- Other traps (includes syslog messages, protocol-related notifications, and CPU usage warnings).

See Table 32: SNMP Traps Dialog Box , on page 76 for a description of the available traps.

Note
You must add command-line interface (CLI) commands to fully implement the IP multicast and CPU traps. One method available for entering these commands is by using FlexConfigs. See Understanding FlexConfig Policies and Policy Objects.

Tip
Click **Select All** to enable all traps displayed in the dialog box or **Deselect All** to disable all the traps.

Step 4 Click **OK** to save your definitions locally on the client and close the dialog box.

Tip
To configure SNMP traps not included in this dialog box, define a FlexConfig.

SNMP Policy Page

Use the SNMP page to configure the parameters necessary to send traps from the router to a designated SNMP host. These traps are unsolicited messages that notify the SNMP host of important events occurring on the router.

For more information, see Defining SNMP Agent Properties , on page 69.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > SNMP** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Device Access > SNMP** from the Policy Type selector. Right-click **SNMP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- SNMP on Cisco IOS Routers , on page 69
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 29: SNMP Page

Element	Description
Permissions table	
Community String	The community string used for accessing the router's MIB.
Type	The community string type—read-only or read-write.
ACL	The standard ACL that defines the IP addresses permitted to access the router's MIB.
Add button	Opens the Permission Dialog Box , on page 73. From here you can enter the community string and type required to generate traps.
Edit button	Opens the Permission Dialog Box , on page 73. From here you can edit the selected permissions profile.
Delete button	Deletes the selected permissions profiles from the table.
Trap Receiver table	
Host IP Address	The IP address of the SNMP host receiving the traps generated by the router.
SNMP Version	The SNMP version being used by the router.
UDP Port	The UDP port that is being used by the SNMP host.

Element	Description
Add button	Opens the Trap Receiver Dialog Box , on page 74. From here you can define the SNMP host that receives the traps generated by the router.
Edit button	Open the Trap Receiver Dialog Box , on page 74. From here you can edit the selected SNMP host.
Delete button	Deletes the selected SNMP hosts from the table.
Additional fields and buttons	
SNMP Server Properties	The name and contact information of the system administrator responsible for the SNMP server/agent (that is, the router). The person managing the SNMP host can use this information when tracking down the source of unusual events. The maximum length of each of these properties is 255 characters, including spaces. **Note** The values entered in these fields are text-only and do not affect the operation of the router.
Configure Traps button	Opens a dialog box for selecting which SNMP traps the router should generate. See SNMP Traps Dialog Box , on page 75.

Permission Dialog Box

Use the Permission dialog box to define the community string and string type required by the SNMP policy. The community string is an embedded password for accessing the Management Information Base (MIB) that stores operational data about the router.

Navigation Path

Go to SNMP Policy Page , on page 72, then click the **Add** or **Edit** button beneath the Permissions table.

Related Topics

- SNMP Policy Page , on page 72
- Trap Receiver Dialog Box , on page 74
- SNMP Traps Dialog Box , on page 75
- Defining SNMP Agent Properties , on page 69
- SNMP on Cisco IOS Routers , on page 69

Field Reference

Table 30: Permission Dialog Box

Element	Description
Community String	The community string for accessing the router's MIB. String length ranges from 1 to 128 characters.
Access Control Lists	Applies only to routers running Cisco IOS Software Release 12.3(2)T and up (T-train) or any 12.4 version. The standard ACL containing the IP addresses that can access the router's MIB. Defining an ACL provides an additional layer of security by limiting the source addresses that can make use of the community string. Enter the name of a standard ACL object, or click **Select** to select the object from a list or to create a new one.
Read-Write	This community string type provides read-write access to all objects in the MIB (except community strings).
Read-Only	This community string type provides read-only access to all objects in the MIB (except community strings). This is the default.

Trap Receiver Dialog Box

Use the Trap Receiver dialog box to define the SNMP hosts that receive traps generated by the router. This includes defining the version of SNMP to use.

Navigation Path

Go to the SNMP Policy Page , on page 72, then click the **Add** or **Edit** button beneath the Trap Receiver table.

Related Topics

- SNMP Policy Page , on page 72
- Permission Dialog Box , on page 73
- SNMP Traps Dialog Box , on page 75
- Defining SNMP Agent Properties , on page 69
- SNMP on Cisco IOS Routers , on page 69

Field Reference

Table 31: Trap Receiver Dialog Box

Element	Description
Host IP Address	The IP address of the SNMP host receiving the traps generated by the router. Enter an IP address or the name of a network/host object, or click **Select** to select the object from a list or to create a new one.
SNMP Version	The version of SNMP to use—version 1, version 2c, or version 3.
Community String	Applies only when version 1 or version 2c is selected. The password required to access the SNMP host. Enter the string again in the Confirm field. **Note** We recommend that you use one of the strings defined in the Permissions table as the password to the SNMP host. You may, however, enter a different password. String length ranges from 1 to 128 characters. Your entry does not appear in the Permissions table and is read-only.
User Name	Applies only when version 3 is selected. The password required to access the SNMP host. Enter the string again in the Confirm field. **Note** We recommend that you use one of the strings defined in the Permissions table as the password to the SNMP host. You may, however, enter a different password. String length ranges from 1 to 128 characters. Your entry does not appear in the Permissions table and is read-only.
SNMPv3 Security	Applies only when version 3 is selected. The level of security to apply to SNMP traffic: • No MD5, No DES—No packet authentication. • MD5 (auth)—MD5 authentication, but no encryption. • DES (priv)—MD5 authentication and DES encryption.
UDP Port	The port number for the SNMP host. The default is 162. Valid values range from 0 to 65535.

SNMP Traps Dialog Box

Use the SNMP Traps dialog box to select the events in the router that should generate SNMP traps. To lessen possible degradation of system performance, select only those traps that are needed for network monitoring purposes.

Tip You can configure SNMP traps not included in this dialog box by defining FlexConfigs. For more information, see Understanding FlexConfig Policies and Policy Objects.

Navigation Path

Go to the SNMP Policy Page , on page 72, then click **Configure Traps**.

Related Topics

- SNMP Policy Page , on page 72
- Permission Dialog Box , on page 73
- Trap Receiver Dialog Box , on page 74
- Enabling SNMP Traps , on page 71
- SNMP on Cisco IOS Routers , on page 69

Field Reference

Table 32: SNMP Traps Dialog Box

Element	Description
Standard SNMP Traps	Enables or disables standard SNMP traps. Options are: • Cold start—Sends a trap when the router reinitializes in a way that could change the configuration of the SNMP agent (or any other trap-receiving entity). • Warm start—Sends a trap when the router reinitializes in a way that does not change the configuration of the SNMP agent (or any other trap-receiving entity). • Authentication—Sends a trap if an SNMP request from the SNMP host fails because of an invalid community string.
IPsec Traps	Enables or disables individual IPsec-related traps. Options are: • Cryptomap—Sends a trap when a crypto map entry is added to, or removed from, the device's crypto map set. Additionally, this option sends a trap when a crypto map set is attached to, or detached from, an active interface. • Too Many SAs—Sends a trap if an attempt is made to create a security association (SA) when there is insufficient memory on the device. • Tunnel—Sends a trap when an IPsec Phase 2 tunnel becomes active or inactive. For more information, see Understanding IPsec Proposals for Site-to-Site VPNs.

Element	Description
ISAKMP Traps	Enables or disables individual Internet Security Association and Key Exchange Protocol (ISAKMP) traps. Options are: • Policy—Sends a trap when an ISAKMP policy is created or deleted. • Tunnel—Sends a trap when a Phase 1 IKE tunnel becomes active or inactive. For more information, see Understanding IKE.
Other Traps	Enables or disables additional SNMP traps. Options are: • Syslog—Sends syslog messages to the SNMP host. • TTY—Sends Cisco-specific notifications when a Transmission Control Protocol (TCP) connection closes. • BGP—Sends notifications when Border Gateway Protocol (BGP) state changes occur. See BGP Routing on Cisco IOS Routers. • IP Multicast—(Applicable to multicast routers only) Sends a trap if the router fails to receive a defined number of heartbeat packets from heartbeat sources within a defined time interval. If you select IP Multicast, you must also manually configure the **ip multicast heartbeat** command on the device to configure the multicast address and heartbeat limits. You can use FlexConfigs to do this. • CPU—Sends a trap when CPU usage rises and remains above an upper threshold or falls and remains below a lower threshold. If you select CPU, you must also manually configure the **process cpu threshold type** command on the device to configure the thresholds. You can use FlexConfigs to do this. • HSRP—Sends Hot Standby Routing Protocol (HSRP) notifications.
Select All button	Enables all the SNMP traps displayed in the dialog box.
Deselect All button	Disables all the SNMP traps displayed in the dialog box.

DNS on Cisco IOS Routers

The Domain Name System (DNS) is a distributed database in which you can map hostnames to IP addresses through the DNS protocol from a DNS server. Each unique IP address can have an associated hostname. DNS is what makes it possible to connect to hosts without having to know the 32-bit IP address of that host. The DNS server takes the provided hostname and translates it into the appropriate IP address.

In addition to the translation provided by remote DNS servers, you can configure Cisco IOS routers with a local host table containing static mappings of hosts to IP addresses. When commands such as connect, telnet, and ping are used, the router checks this host table before querying the DNS servers, which speeds the translation process.

By default, the DNS feature is enabled on all Cisco IOS routers.

Related Topics

- Defining DNS Policies , on page 78

Defining DNS Policies

When you define a DNS policy in Security Manager, you can specify the remote DNS servers used by the router for hostname-to-address translations. In addition, you can define a static host table that contains local translations used exclusively by this device. Having selected addresses in this type of cache can speed the translation process by eliminating the need to query the DNS servers.

Related Topics

- DNS on Cisco IOS Routers , on page 77

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Device Admin** > **DNS** from the Policy selector.
- (Policy view) Select **Router Platform** > **Device Admin** > **DNS** from the Policy Type selector. Select an existing policy or create a new one.

The DNS page is displayed. See Table 33: DNS Page , on page 79 for a description of the fields on this page.

Step 2 In the Servers field, enter the addresses of the DNS servers (up to 6) that can perform hostname-to-address translations for the router. You can use a combination of addresses and network/host objects, or click **Select** to display a selector. For more information, see Specifying IP Addresses During Policy Definition.

Tip
If the network you want is not listed in the selector, click the **Create** button or the **Edit** button in the selector to display the Add or Edit Network/Host Dialog Box. From here you can create a network/host object to use in the policy.

Step 3 (Optional) In the Hosts field, enter the static host mappings that you want to define in the router's host table:

a) Click **Add** to display the IP Host Dialog Box , on page 79.
b) Enter the hostname to translate.
c) Enter up to three addresses or network/host objects, or click **Select** to display a selector. These are the addresses to which the router translates the hostname.
d) Click **OK**. The mapping is displayed in the Hosts field on the DNS page.
e) Repeat 3.a, on page 78 through 3.d, on page 78 to add more hosts to the host table.

Note
To edit a host mapping, select the definition from the Hosts field, then click **Edit**. To remove a host mapping, select it, then click **Delete**.

Step 4 (Optional) Deselect the **Domain Lookup** check box to disable DNS functionality on the router.

DNS Policy Page

Use the DNS policy page to define the local IP host table and the Domain Name System (DNS) servers that the router should use for translating hostnames to IP addresses. You can also prevent the router from performing DNS lookups by disabling the DNS feature.

Navigation Path

- (Device view) Select **Platform > Device Admin > DNS** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > DNS** from the Policy Type selector. Right-click **DNS** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- DNS on Cisco IOS Routers , on page 77

Field Reference

Table 33: DNS Page

Element	Description
Servers	The DNS servers used by the router to perform DNS lookups. Enter one or more addresses or network/host objects, or click **Select** to select an object from a list or to create a new one. You can define a maximum of six DNS servers.
Hosts	The local host table configured on the router. When a user types in a hostname, the router checks this table first before querying the DNS servers defined in the Servers field. Click **Add** to display the IP Host Dialog Box , on page 79. From here you can define a hostname and the IP addresses to associate with that hostname. **Note** To edit an entry in the host table, select it, then click **Edit**. To remove an entry, select it, then click **Delete**.
Domain Lookup	When selected, the router performs lookups on the defined DNS servers. This is the default. When deselected, lookups on remote DNS servers are disabled.

IP Host Dialog Box

Use the IP Host dialog box to configure the host table on the router. This is the table of static, local mappings that the router uses to translate hostnames to IP addresses. If the router does not find the required entry in the host table, it queries the DNS servers that are defined on the DNS page.

Navigation Path

Go to the DNS Policy Page , on page 79, then click **Add** under Hosts.

Related Topics

- DNS on Cisco IOS Routers , on page 77

Field Reference

Table 34: IP Host Dialog Box

Element	Description
Host Name	The hostname to include in the router's local host table.
Addresses	The addresses to associate with the hostname. Enter one or more addresses or network/host objects, or click **Select** to select an object from a list or to create a new object. You can define a maximum of three addresses per hostname.

Hostnames and Domain Names on Cisco IOS Routers

The Hostname policy configures the hostname and domain name of the selected router. After you deploy this policy, any changes that you made to the hostname and domain name are reflected in the Device Properties page (see Viewing or Changing Device Properties).

Related Topics

- Defining Hostname Policies , on page 80

Defining Hostname Policies

When you define a hostname policy, Security Manager updates the hostname and domain name fields in the Device Properties dialog box after deployment. See Viewing or Changing Device Properties.

Related Topics

- Hostnames and Domain Names on Cisco IOS Routers , on page 80

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform** > **Device Admin** > **Hostname** from the Policy selector.
- (Policy view) Select **Router Platform** > **Device Admin** > **Hostname** from the Policy Type selector. Select an existing policy or create a new one.

The Hostname page is displayed. See Table 35: Hostname Page , on page 81 for a description of the fields on this page.

Step 2 Enter the hostname for the router. Names must start with a letter, end with a letter or digit, and include only letters, digits, and hyphens. The maximum length is 63 characters.

Step 3 Enter the domain name for the router. The router uses this domain name for RSA key generation and in policies when you do not enter the fully-qualified domain name.

Hostname Policy Page

Use the Hostname page to define the hostname and domain name assigned to the router. For more information, see Defining Hostname Policies , on page 80.

Navigation Path

- (Device view) Select **Platform > Device Admin > Hostname** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Hostname** from the Policy Type selector. Right-click **Hostname** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Hostnames and Domain Names on Cisco IOS Routers , on page 80

Field Reference

Table 35: Hostname Page

Element	Description
Host Name	The hostname of the router. Names must start with a letter, end with a letter or digit, and include only letters, digits, and hyphens. The maximum length is 63 characters.
Domain Name	The default domain name of the router. The maximum length is 63 characters. The router uses this domain name for RSA key generation and in policies when you do not enter the fully-qualified domain name (FQDN).

Memory Settings on Cisco IOS Routers

The Memory policy configures settings relating to router memory. This policy provides you with methods for monitoring memory consumption, including the ability to generate notification messages when available memory drops below predefined thresholds.

Note The Memory policy is supported on routers running Cisco IOS Software Release 12.3(14)T or later.

Related Topics

- Defining Router Memory Settings , on page 82

Defining Router Memory Settings

You can use Security Manager to modify the following default memory settings:

- The number of hours that the router maintains the log of memory consumption.
- Whether to enable the Memory Allocation Lite feature.
- The amount of memory to reserve for critical system log messages.

In addition, you can define:

- The lower thresholds for processor and I/O memory. Log messages are sent when available memory drops below these thresholds.
- The types of sanity checks to perform.

Related Topics

- Memory Settings on Cisco IOS Routers , on page 81
- Logging on Cisco IOS Routers

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Memory** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Memory** from the Policy Type selector. Select an existing policy or create a new one.

The Memory page is displayed.

Step 2 (Optional) Define the memory settings of the router, as required. See Table 36: Memory Page , on page 83 for a description of the available fields.

Memory Policy Page

Use the Memory page to define settings related to router memory, including:

- The amount of time to retain the memory log.
- The thresholds for available processor and I/O memory.
- The amount of memory reserved for critical log messages.
- Whether to perform sanity checks on buffers and queues.
- Whether to enable the “memory-allocation lite” feature.

For more information, see Defining Router Memory Settings , on page 82.

Navigation Path

- (Device view) Select **Platform > Device Admin > Memory** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Memory** from the Policy Type selector. Right-click **Memory** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- Memory Settings on Cisco IOS Routers , on page 81
- CPU Policy Page , on page 27
- Syslog Logging Setup Policy Page
- Syslog Servers Policy Page

Field Reference

Table 36: Memory Page

Element	Description
Maintain Memory Log	The number of hours that the router should maintain the log containing the history of memory consumption on the device. Valid values range from 12 to 72 hours. The default is 24 (1 day). **Note** The memory log is enabled by default and cannot be disabled.
Processor Threshold	The processor memory threshold in kilobytes. When available processor memory falls below this threshold, a notification message is triggered. Valid values range from 1 to 4294967295 kilobytes (4096 gigabytes). **Note** Another notification message is generated when available free memory rises to 5% above the threshold.
I/O Threshold	The I/O memory threshold in kilobytes. When available processor memory falls below this threshold, a notification message is triggered. Valid values range from 1 to 4294967295 kilobytes (4096 gigabytes). **Note** Another notification message is generated when available free memory rises to 5% above the threshold.
Memory Allocation Lite	When selected, the “memory-allocation lite” (malloc_lite) feature on the router is enabled. This feature avoids excessive memory allocation overhead for situations where less than 128 bytes are required. This is the default. When deselected, the “memory-allocation lite” feature is disabled. **Note** This feature is supported for processor memory pools only.

Element	Description
Memory Region For Critical Notifications	The amount of memory (in kilobytes) reserved for critical system log messages. Valid values range from 1 to 4294967295 kilobytes (4096 gigabytes), but the value you specify cannot exceed 25% of total memory. This option reserves a region of memory on the router so that the router can issue critical system log messages even when system resources are overloaded.
Perform Sanity Checks	The types of sanity checks to perform: • Buffer—When selected, performs sanity checks on all buffers. Sanity checks are performed when a packet buffer is allocated and when the packet buffer is returned to the buffer pool. • Queue—When selected, performs sanity checks on all queues. • All—When selected, performs sanity checks on all buffers and queues. **Note** Enabling any of these options may result in a slight degradation of router performance.

Secure Device Provisioning on Cisco IOS Routers

Secure Device Provisioning (SDP) offers an integrated solution for streamlining VPN and network security deployment. SDP (previously called Easy Secure Device Deployment, or EzSDD) enables remote-site users to securely bootstrap their VPN device through an easy-to-use web interface, thereby easing the deployment burden, lowering costs, and shortening the network development cycle. For example, a telecommuter or small branch office user can remove a new device from its shipping package, plug it in, open a simple web management interface, and establish VPN connectivity, all within a period of just a few minutes.

For more information about SDP, see *Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI* , which can be found in *Cisco IOS Security Configuration Guide, Release 12.4T* .

Note SDP requires Cisco IOS Software Release 12.3(8)T or later. Attempting to deploy this policy to a router running an earlier version could result in deployment failure. You also cannot configure the policy on NO-VPN router models (those that do not allow VPN configurations, such as the 3845 NOVPN).

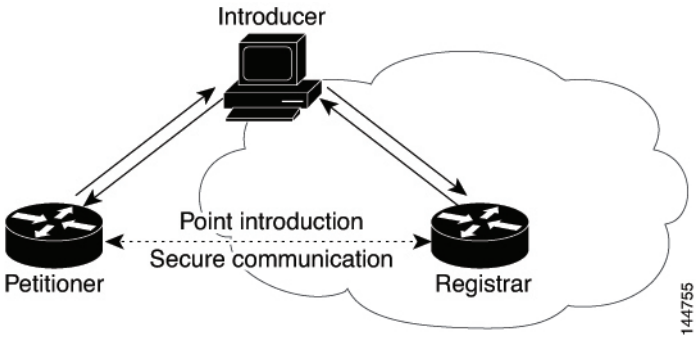
Trusted Transitive Introduction (TTI) is the protocol that acts as the primary mechanism for implementing SDP. As shown in Figure 3: Secure Device Provisioning, on page 85, TTI comprises the following three entities:

- Introducer—A mutually trusted device that introduces the petitioner to the registrar. Introducers can be end users who use SDP to deploy VPN devices associated with themselves to the PKI network, or an administrator/management system that uses SDP to deploy many VPN devices to the PKI network. This latter type is known as an administrative introducer. For more information, see Configuring a AAA Server Group for Administrative Introducers , on page 88.

- Petitioner—A remote-site device that is joined to the secure domain. The petitioner serves web pages to the introducer and receives the bootstrap configuration from the introducer's web browser. The petitioner component is enabled by default on all Cisco IOS devices.
- Registrar—A server that authorizes the petitioner by communicating directly with an authentication, authorization, and accounting (AAA) server to verify user credentials, permit or deny enrollment, and retrieve user-specific configuration information.

Use the SDP policy in Security Manager to configure the router as a registrar.

Figure 3: Secure Device Provisioning



For more information about Secure Device Provisioning, see:

- Contents of Bootstrap Configuration , on page 85
- Secure Device Provisioning Workflow , on page 86
- Defining Secure Device Provisioning Policies , on page 86

Contents of Bootstrap Configuration

The bootstrap configuration provided by SDP typically does the following:

- Sets the petitioner's hostname.
- Synchronizes the petitioner's system clock with the registrar.
- Sets the petitioner's trustpoint.
- Sets the petitioner's authentication and authorization mechanism.
- Pushes the CA certificate.
- Enrolls the petitioner with the PKI server.
- Sets other VPN configurations, such as the configuration required to establish a management tunnel.
- Sets Cisco Networking Services (CNS) configuration.
- Sets the petitioner's DHCP pool.

Related Topics

- Secure Device Provisioning Workflow , on page 86

- Secure Device Provisioning on Cisco IOS Routers , on page 84

Secure Device Provisioning Workflow

The following illustrates the steps required to use SDP to register a remote-site device in a secure network:

1. Unpack the router and connect the power, LAN, and WAN cables.
2. Turn on a computer (introducer) that is assigned an IP address from the DHCP server on the router, open a web browser, and go to the petitioner URL (http://device/ezsdd/welcome) on the router. The router responds with a registration page (also called the local login dialog box).
3. Enter the username and password, then click **OK**. On the welcome page, enter the URL for the registrar. The following actions occur:
   a. The browser opens an HTTPS-secured session to the central-site registrar, which verifies the username with the AAA server and returns the appropriate bootstrap configuration to the browser.
   b. The browser feeds the bootstrap configuration to the remote-site router, configuring PKI trustpoint enrollment and IPsec VPN connectivity, and provisioning system attributes and other information.
   c. You are notified that bootstrap configuration is complete.

Related Topics

- Contents of Bootstrap Configuration , on page 85
- Secure Device Provisioning on Cisco IOS Routers , on page 84

Defining Secure Device Provisioning Policies

The petitioner component is automatically enabled on all Cisco IOS routers. The SDP policy in Security Manager enables the registrar. To define an SDP policy you must define:

- The AAA server group containing the AAA server that the registrar uses to authenticate and authorize the introducer.
- The CA server to which the petitioner enrolls during the bootstrap process.
- The location of the introduction page that is displayed after authorization was performed.
- The location of the bootstrap configuration to be provided to the petitioner.

Related Topics

- Secure Device Provisioning Workflow , on page 86
- Configuring a AAA Server Group for Administrative Introducers , on page 88
- Secure Device Provisioning on Cisco IOS Routers , on page 84

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Secure Device Provisioning** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Secure Device Provisioning** from the Policy Type selector. Select an existing policy or create a new one.

The Secure Device Provisioning page is displayed. See Table 37: Secure Device Provisioning Page , on page 89 for a description of the fields on this page.

Step 2 Under Introducer Authentication, enter the name of the AAA server group containing the relevant AAA server, or click **Select** to select it from a list or to create a new object.

The selected AAA server determines whether the username and password supplied by the introducer represent an authorized user. The AAA server must use TACACS+, RADIUS, or be local.

Note
Each AAA server in the selected group must be configured to communicate with an interface that exists on the router; otherwise, validation fails. If you want to configure a different AAA server group for authenticating and authorizing administrative introducers, see Configuring a AAA Server Group for Administrative Introducers , on page 88.

Step 3 Under Petitioner Authentication, define the CA server that authenticates the identity of the petitioner by doing one of the following:

- Select **Local CA Server**, then enter the local CA name in the field provided. If you have already configured the CA server locally on the registrar, a trustpoint is generated automatically.

Note
If you have not configured the router as the CA server, enter the command **Crypto pki server [name]** using the CLI or FlexConfigs. This command is mandatory when you deploy an SDP policy configured with a local CA server.

- Select Remote CA Server, then enter the name of a PKI enrollment object, or click **Select** to select it from a list or to create a new object.

The PKI enrollment object defines the external CA server used in the SDP policy.

Step 4 Select the source of the introduction page that is displayed after you log in to the registrar. The introduction page indicates whether authorization was successfully completed and contains a button for completing the process of obtaining the bootstrap configuration.

If you do not select the default welcome page, you must enter the URL required to access a different welcome page that you prepared elsewhere.

Step 5 Select the source of the bootstrap configuration provided to the petitioner to implement its first-time configuration:

- If the source of the bootstrap configuration is a non-Security Manager URL, enter the URL and also the username and password for accessing the URL, if required.
- If the source of the configuration file is a Security Manager URL:
  - Enter the name of a FlexConfig, or click **Select** to select it from a list or to create a new object. The FlexConfig contains the device commands required to retrieve the appropriate bootstrap configuration. For more information, see Add or Edit FlexConfig Dialog Box.

- Enter the device name formula required by the FlexConfig to derive the device name of the petitioner from the username submitted by the introducer. (The two names typically have a fixed relationship.) The default formula is $n, which uses the introducer name to determine the device name.

The device name determines which bootstrap configuration the petitioner should receive. The resulting URL contains the name of the FlexConfig you selected, as well as the parameters and formula you defined.

- Enter a username and password for accessing the Security Manager server containing the FlexConfig. The password can contain alphanumeric characters, but cannot consist of a single digit.

Configuring a AAA Server Group for Administrative Introducers

Administrative introducers are administrators or management systems that introduce many devices to the PKI network. You can configure a AAA server group for authenticating and authorizing administrative introducers by appending the following FlexConfig to the configuration of the router:

```
aaa new-model
radius-server host 1.2.3.4 auth-port 1645 acct-port 1646 key key
aaa group server radius default-radius-group2
server 1.2.3.4 auth-port 1645 acct-port 1646
exit
aaa authentication login CSM_SDP2 group default-radius-group2
crypto provisioning registrar
administrator authentication list CSM_SDP2
administrator authorization list CSM_SDP2
exit
```

This FlexConfig serves two functions—it configures the AAA server group to use and it associates this server group with the SDP crypto.

For more information about administrative introducers, see *Administrative Secure Device Provisioning Introducer* on Cisco.com at this URL:
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtadintr.html

Related Topics

- Secure Device Provisioning on Cisco IOS Routers , on page 84
- Defining Secure Device Provisioning Policies , on page 86
- Understanding FlexConfig Policies and Policy Objects

Secure Device Provisioning Policy Page

Secure Device Provisioning (SDP) policies (formerly known as Easy Secure Device Deployment or EzSDD) enable you to configure a Cisco IOS router as a *registrar* . This is the SDP component that retrieves bootstrap configurations for *petitioners* , which are remote-site devices that are enrolling in the network security infrastructure. These devices uses the bootstrap configuration for first-time configuration purposes. The registrar also verifies the identity of the *introducer* , which is the user who introduces the petitioner to the registrar.

For more information, see Defining Secure Device Provisioning Policies , on page 86.

Navigation Path

- (Device view) Select **Platform > Device Admin > Secure Device Provisioning** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Secure Device Provisioning** from the Policy Type selector. Create a new policy or select an existing one.

Related Topics

- Secure Device Provisioning on Cisco IOS Routers , on page 84
- Secure Device Provisioning Workflow , on page 86
- Understanding AAA Server and Server Group Objects
- Understanding FlexConfig Policies and Policy Objects

Field Reference

Table 37: Secure Device Provisioning Page

Element	Description
Introducer Authentication (AAA)	The AAA server group that authenticates the username and password supplied by the introducer. Enter the name of a AAA server group object, or click **Select** to select it from a list or to create a new object. **Note** To configure a separate AAA server group for authenticating administrative introducers, see Configuring a AAA Server Group for Administrative Introducers , on page 88.
Petitioner Authentication	The CA server that authenticates the identity of the petitioner: • Local CA Server—Select this option when the router itself is already configured to act as the CA server. Enter the name of the local CA in the field provided. **Note** If you have not configured the router as the CA server, enter the command **Crypto pki server [name]** using the CLI or FlexConfigs. This command is mandatory when you deploy an SDP policy configured with a local CA server. • Remote CA Server—Select this option when using an external CA server. Enter the name of a a PKI enrollment object, or click **Select** to select it from a list or to create a new object. For more information about PKI enrollment objects, see PKI Enrollment Dialog Box.

Element	Description
Introduction Page	The source of the introduction page to display to the introducer after authorization is performed: • Use default introduction page—Uses a default page provided with Security Manager. • Specify introduction page URL—Uses the introduction page specified in the URL field. Supported protocols include: FTP, HTTP, HTTPS, null, NVRAM, RCP, SCP, system, TFTP, Webflash, and XMODEM.
Bootstrap Configuration	The source of the bootstrap configuration to provide to the petitioner for first-time configuration: • Non-Security Manager URL—Used when the bootstrap configuration is located externally to Security Manager. Enter its location in the URL field. If required, enter a username and password to access the server containing the bootstrap configuration. • Security Manager URL—Used when Security Manager is providing the bootstrap configuration. Enter information in the following fields: • FlexConfig—The FlexConfig that contains the basic CLI structure required to create the bootstrap configuration. Enter the name of a FlexConfig object, or click **Select** to display a selector. After selecting the FlexConfig, you must enter a username and password to access the Security Manager server that contains the FlexConfig. • Device name formula—The formula required by Security Manager to determine the device name of the petitioner from the username that the introducer supplied. Typically a fixed relationship exists between the username and the device name, which enables a formula like this to be established. The default formula is $n, which uses the introducer name to determine the device name. The device name is required to determine the configuration file that the petitioner should receive. If required, enter a username and password to access the server containing the bootstrap configuration. The password can contain alphanumeric characters, but cannot consist of a single digit.

DHCP on Cisco IOS Routers

In Security Manager, certain security features, such as Easy VPN and 802.1x, require Dynamic Host Configuration Protocol (DHCP) client/server configuration. DHCP is widely used in LAN environments to dynamically assign host IP addresses from a centralized server, which significantly reduces the overhead of administering IP addresses.

DHCP servers assign and manage IP addresses from specified address pools within a router to DHCP clients. If the DHCP server cannot satisfy a DHCP request from its own database, it can forward the request to one or more secondary DHCP servers defined by the network administrator.

Security Manager enables you to configure a Cisco IOS device as a DHCP server for clients (hosts) that are connected to the device's inside interface. When you configure a DHCP server, you use IP pools (a range of IP addresses reserved for a DHCP server). The IP pools you select determine the range of IP addresses the server can use. These addresses are provided to client devices for a defined period of time called a lease. When this lease expires, the address is returned to the address pool, enabling the DHCP server to assign it to a different device.

For more information about DHCP, see:

- Understanding DHCP Database Agents , on page 91
- Understanding DHCP Relay Agents , on page 91
- Understanding DHCP Option 82 , on page 92
- Understanding Secured ARP , on page 92

To configure a DHCP policy, see:

- Defining DHCP Policies , on page 93
- Defining DHCP Address Pools , on page 94

Understanding DHCP Database Agents

A DHCP database agent is any external host—for example, an FTP, TFTP, or RCP server—that stores the DHCP bindings database. You can include one or more DHCP database agents in each DHCP policy, as well as configure the interval between database updates to the agent.

Note If you configure an external DHCP database agent, it is not necessary to define IP address pools, but you may do so. For more information about IP address pools, see Defining DHCP Address Pools , on page 94.

Related Topics

- Understanding DHCP Relay Agents , on page 91
- Understanding DHCP Option 82 , on page 92
- Understanding Secured ARP , on page 92
- Defining DHCP Policies , on page 93
- DHCP on Cisco IOS Routers , on page 90

Understanding DHCP Relay Agents

A DHCP relay agent is any host that forwards DHCP packets between clients and servers when they do not reside on the same physical subnet. Relay agents receive DHCP messages and then generate a new DHCP message to send on another interface. You can configure a reforwarding policy that determines what the DHCP relay agent should do if a forwarded message already contains relay information.

DHCP relay options in Security Manager include:

- Drop—The relay agent discards messages with existing relay information if Option 82 information is also present.
- Keep—The relay agent retains existing relay information.
- Replace—The relay agent overwrites existing information with its own relay information.

For example, you can have the DHCP relay agent replace the forwarded message with a new relay message. Additionally, you can choose whether to have the relay agent check the validity of relay information contained within forwarded BOOTREPLY messages.

Related Topics

- Understanding DHCP Database Agents , on page 91
- Understanding DHCP Option 82 , on page 92
- Understanding Secured ARP , on page 92
- Defining DHCP Policies , on page 93
- DHCP on Cisco IOS Routers , on page 90

Understanding DHCP Option 82

DHCP option 82 enables the DHCP relay agent to include information about itself and its attached client when it forwards requests from a DHCP client to a DHCP server. The DHCP server can use this information to assign IP addresses, perform access control, and set quality of service (QoS) and security policies for each of its subscribers. When the DHCP option 82 feature is enabled, a subscriber is identified by the switch port through which it connects to the networks, instead of by its MAC address. Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified. Option 82 also enhances security on access switches by providing the ability to use a user's IP address to locate the port on which a user is attached.

Related Topics

- Understanding DHCP Database Agents , on page 91
- Understanding DHCP Relay Agents , on page 91
- Understanding Secured ARP , on page 92
- Defining DHCP Policies , on page 93
- DHCP on Cisco IOS Routers , on page 90

Understanding Secured ARP

The DHCP Secure IP Address Assignment feature (also called DHCP Authorized ARP) enables you to secure Address Resolution Protocol (ARP) table entries to DHCP leases in the DHCP database. This feature secures and synchronizes the client's MAC address to the DHCP binding, preventing unauthorized clients or hackers from spoofing the DHCP server and taking over a DHCP lease of an authorized client.

When you enable this feature and the DHCP server assigns an IP address to the DHCP client, the DHCP server adds a secure ARP entry to the ARP table with the assigned IP address and the MAC address of the client. These ARP entries cannot be updated by any other dynamic ARP packets, and they exist in the ARP table for as long as the lease is active.

Secure ARP entries can be deleted only by an explicit termination message from the DHCP client or by the DHCP server when the binding expires. To detect when a client has logged out, Secured ARP sends periodic ARP messages to which only authorized users can respond. Unauthorized responses are blocked at the DHCP server, providing an additional level of security.

Note Secured ARP disables dynamic ARP learning on an interface.

Related Topics

- Understanding DHCP Database Agents , on page 91
- Understanding DHCP Relay Agents , on page 91
- Understanding DHCP Option 82 , on page 92
- Defining DHCP Policies , on page 93
- DHCP on Cisco IOS Routers , on page 90

Defining DHCP Policies

When you configure a DHCP policy, you must define the IP address pools for the server to use to provide addresses to DHCP clients. In addition, you can optionally define the following:

- External DHCP database agent.
- IP ranges to exclude from DHCP.
- DHCP relay parameters.

Note When configuring DHCP on a Cisco IOS router, make sure that the router does not contain an access rule denying Bootstrap Protocol (BootP) traffic. Having such a rule blocks DHCP traffic from being transmitted.

Related Topics

- DHCP on Cisco IOS Routers , on page 90

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Server Access > DHCP** from the Policy selector.

- (Policy view) Select **Router Platform** > **Device Admin** > **Server Access** > **DHCP** from the Policy Type selector. Select an existing policy or create a new one.

The DHCP Policy page is displayed. See Table 38: DHCP Policy Page , on page 95 for a description of the fields on this page.

Step 2 (Optional) Under Databases, click the **Add** button to display the DHCP Database Dialog Box , on page 97. From here you can define external DHCP database agents. For more information, see Understanding DHCP Database Agents , on page 91.

Step 3 (Optional) Under Excluded IPs, enter the IP addresses or address ranges within a DHCP address pool that should not be made available to DHCP clients. You can use a combination of addresses and network/host objects, or click **Select** to display a selector. For more information, see Specifying IP Addresses During Policy Definition.

Tip
If the network you want is not listed in the selector, click the **Create** button to display the Add or Edit Network/Host Dialog Box. From here you can create a network/host object.

Step 4 Under IP Pools, click the **Add** button to display the IP Pool Dialog Box , on page 98. From here you can define the address pools to be used by the DHCP server. For more information, see Defining DHCP Address Pools , on page 94.

Step 5 (Optional) When you use a relay agent to manage requests from DHCP clients located on a different subnet from the DHCP server, define the following DHCP relay options:

a) Select the relay agent information reforwarding policy (Drop, Keep, or Replace). DHCP relay agents implement this policy when they receive messages already containing relay information.
b) Select the **Option** check box to enable the insertion of Option 82 data in requests that the relay agent forwards to the DHCP server.
c) Select the **Check** check box to validate DHCP Option 82 reply packets sent by the DHCP server.

When you enable this option, invalid messages are dropped. Valid messages are stripped of the option-82 field before they are forwarded to the DHCP client. When you disable this option, the option-82 field is removed from the packet without being checked first for validity.

See Understanding DHCP Relay Agents , on page 91 for more information.

Defining DHCP Address Pools

When you configure a DHCP policy that does not include an external database agent, you must define at least one IP address pool. This pool contains the addresses that the DHCP server can dynamically assign to DHCP clients. Additionally, you can define the following IP pool-specific options:

- The default routers, DNS servers, WINS servers, and domain used by DHCP clients.
- Whether to use the Secured ARP feature.
- Whether to import information regarding IP pool options from a centralized DHCP server.
- The length of the lease.
- The location of the TFTP server that IP telephony devices require to use addresses from this pool.

Related Topics

- Defining DHCP Policies , on page 93

- DHCP on Cisco IOS Routers , on page 90

Procedure

Step 1 On the DHCP page, click the **Create** button under IP Pools. The IP Pool dialog box is displayed.

Step 2 Define the address pool. See Table 40: IP Pool Dialog Box , on page 98 for a description of the available fields.

Step 3 Click **OK** to save your definitions locally on the client and close the dialog box. The IP pool appears in the table displayed under IP Pools on the DHCP page.

Step 4 Repeat Step 1, on page 95 through Step 3, on page 95 to define additional address pools, if required.

Note
To edit an IP pool, select it from the table, then click the **Edit** button. To delete an IP pool, select it from the table, then click the **Delete** button. You cannot delete a pool whose addresses have been assigned to DHCP clients.

DHCP Policy Page

Use the DHCP policy page to define a DHCP server policy on the selected router. This includes specifying the address pools used by the DHCP server when assigning addresses to requesting clients.

For more information, see Defining DHCP Policies , on page 93.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > DHCP** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Server Access > DHCP** from the Policy Type selector. Right-click **DHCP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- DHCP on Cisco IOS Routers , on page 90
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 38: DHCP Policy Page

Element	Description
Databases Table	
Database URL	The URL of the external DHCP database agent.
Timeout	The amount of time to wait (in seconds) for a response from the external DHCP database agent before aborting a database transfer.

Element	Description
Write Delay	The interval (in seconds) between DHCP assignment updates sent to the external DHCP database agent.
Add button	Opens the DHCP Database Dialog Box , on page 97. From here you can define a DHCP database agent.
Edit button	Opens the DHCP Database Dialog Box , on page 97. From here you can edit the selected DHCP database agent.
Delete button	Deletes the selected DHCP database agents.
Excluded IPs	
Excluded IPs or IP Ranges	The IP addresses or address ranges to exclude from DHCP. These addresses are not assigned by the DHCP server to DHCP clients requesting addresses. Enter one or more network addresses or network/host objects, or click **Select** to select an object from a list or to create a new object. For more information, see Specifying IP Addresses During Policy Definition.
IP Pools Table	
Name	The name of the IP pool.
Network	The IP address and subnet mask of the IP pool.
Default Router	The IP addresses of the default routers used by DHCP clients.
DNS Server	The IP addresses of the DNS servers used by DHCP clients.
NetBIOS (WINS) Server	The IP addresses of the Windows Internet Naming Service (WINS) servers used by Microsoft DHCP clients.
Domain Name	The domain name for DHCP clients.
Import All	Indicates whether the remote DHCP server imports certain DHCP options from a centralized DHCP server.
Secured ARP	Indicates whether secured ARP is enabled on this IP pool to help prevent IP spoofing by unauthorized users.
Lease	The duration of the lease for each IP address assigned by the DHCP server from this IP pool.
Option 150	The IP address of the TFTP server required by IP phones for configuration, as defined using DHCP option 150.
Option 66	The IP address of the TFTP server required by IP phones for configuration, as defined using DHCP option 66.
Add button	Opens the IP Pool Dialog Box , on page 98. From here you can define a DHCP IP address pool.

Element	Description
Edit button	Opens the IP Pool Dialog Box , on page 98. From here you can edit the selected IP pool.
Delete button	Deletes the selected IP pools.
Relay parameters	
Policy	The policy that DHCP relay agents implement when they receive messages already containing relay information: • Drop—The relay agent discards messages with existing relay information if option-82 information is also present. • Keep—The relay agent retains existing relay information. • Replace—The relay agent overwrites existing information with its own relay information.
Option	When selected, enables DHCP Option 82 data insertion in message requests forwarded from the DHCP client to the server. DHCP Option 82 provides the DHCP server with both the switch and port ID of the requesting client. This option makes it possible to locate where a user is physically connected to the network and prevent spoofing. See Understanding DHCP Relay Agents , on page 91. When deselected, DHCP Option 82 is disabled.
Check	When selected, DHCP Option 82 reply packets received from the DHCP server are validated. Invalid messages are dropped; valid messages are stripped of the option-82 field before being forwarded to the DHCP client. When deselected, the option-82 field is removed from the packet without being checked first for validity.

DHCP Database Dialog Box

Use the DHCP Database dialog box to define external DHCP database agents that contain the automatic bindings. Each database URL that you define must be unique.

For more information, see Understanding DHCP Database Agents , on page 91.

Navigation Path

Go to the DHCP Policy Page , on page 95, then click the **Add** or **Edit** button beneath the Databases table.

Related Topics

- Defining DHCP Policies , on page 93
- DHCP on Cisco IOS Routers , on page 90
- IP Pool Dialog Box , on page 98

Field Reference

Table 39: DHCP Database Dialog Box

Element	Description
Database URL	The URL of the external DHCP database agent containing the automatic bindings. The URL can be in HTTP, FTP, TFTP, or RCP format. **Note** If you define a URL, it is not necessary to define an IP address pool. However, you may do so.
Timeout	The amount of time (in seconds) the DHCP server should wait for a response from the external DHCP database agent before aborting a database transfer. The default is 300 seconds (5 minutes). **Note** A value of 0 disables the timeout.
Write Delay	The interval (in seconds) between updates sent from the DHCP server to the external DHCP database agent. The minimum delay is 60 seconds. The default is 300 seconds (5 minutes).

IP Pool Dialog Box

Use the IP Pool dialog box to define one or more address pools, which the DHCP server uses to assign dynamic addresses to DHCP clients. You must define at least one address pool, unless you have defined an external DHCP database agent.

Navigation Path

Go to the DHCP Policy Page , on page 95, then click the **Add** or **Edit** button beneath the IP Pools table.

Related Topics

- Defining DHCP Address Pools , on page 94
- Understanding DHCP Database Agents , on page 91
- DHCP Database Dialog Box , on page 97
- DHCP on Cisco IOS Routers , on page 90

Field Reference

Table 40: IP Pool Dialog Box

Element	Description
Pool Name	The name of the IP pool.

Element	Description
Network	The IP address and subnet mask of the IP pool. This subnet contains the range of available IP addresses that the DHCP server may assign to clients. Enter an address and mask or the name of a network/host object, or click **Select** to select an object from a list or to create a new one. **Tip** You can exclude specific addresses within the range by defining them in the Excluded IPs field. See DHCP Policy Page , on page 95.
Default Router Addresses	The IP addresses of the default routers for DHCP clients using this IP pool. After a DHCP client is booted, it begins sending packets to this router, which should be located on the same subnet as the client. Enter up to eight (8) network addresses or network/host objects, or click **Select** to select an object from a list or to create a new one.
DNS Server Addresses	The IP addresses of the DNS servers that DHCP clients using this IP pool should query when they need to correlate hostnames to IP addresses. Enter up to eight (8) network addresses or network/host objects, or click **Select** to select an object from a list or to create a new one.
NetBIOS (WINS) Server Addresses	The IP addresses of the Windows Internet Naming Service (WINS) servers used by Microsoft DHCP clients to correlate hostnames to IP addresses within a general grouping of networks. Enter up to eight (8) network addresses or network/host objects, or click **Select** to select an object from a list or to create a new one.
Domain Name	The domain name for DHCP clients using this IP pool. This name places these clients in the general grouping of networks that make up the domain.
Import All	When selected, enables remote DHCP servers to import specific DHCP options (such as the DNS server) from a centralized server. Use this option to enable configuration information to be updated automatically. When deselected, all DHCP options are local to this specific server.
Secured ARP	When selected, enables the DHCP Authorized ARP feature, which limits the leasing of IP addresses to authorized mobile users. This feature helps prevent IP spoofing by unauthorized users. See Understanding Secured ARP , on page 92. When deselected, the DHCP Authorized ARP feature is disabled. **Note** This feature also disables dynamic ARP learning on an interface.
Lease Never Expires	When selected, the DHCP server permanently assigns IP addresses to its clients. When deselected, addresses are leased for a predefined amount of time, as defined in the Time Length field.

Element	Description
Time Length (DD:HH:MM)	Applies only when the Lease Never Expires check box is deselected. The duration of the lease provided to each IP address assigned from this IP pool (using the format DD:HH:MM). After the lease expires, the assigned IP address is no longer valid and is returned to the pool.
Option 66 (IP Addresses)	The IP address of the TFTP server used to provide configuration files to IP phones. These configuration files define parameters required by IP phones to connect to Cisco CallManager. Enter up to eight (8) network addresses or network/host objects, or click **Select** to select an object from a list or to create a new one. **Note** This option is functionally similar to option 150. Either or both options may be used.
Option 150 (IP Addresses)	The IP address of the TFTP server used to provide configuration files to IP phones. These configuration files define parameters required by IP phones to connect to Cisco CallManager. Enter up to eight (8) network addresses or network/host objects, or click **Select** to select an object from a list or to create a new one. **Note** This option is functionally similar to option 66. Either or both options may be used.

NTP on Cisco IOS Routers

The Network Time Protocol (NTP) is the standard for time synchronization between network devices. Synchronized time enables you to correlate syslog and other debug output to specific events, which is essential for troubleshooting, fault analysis, and security incident tracking. Time comparisons are not possible without precise time synchronization between the logging, management, and AAA functions occurring in your network.

NTP uses the concept of a stratum to describe how far removed a machine is from an authoritative time source. For example, a stratum 1 time server is directly attached to a radio or atomic clock. NTP then distributes the time from this authoritative time source across the network. A stratum 2 time server synchronizes with a stratum 1 time server; a stratum 3 time server synchronizes with a stratum 2 time server and so on. One NTP transaction per minute is sufficient to synchronize two machines to within a millisecond.

NTP runs over the User Datagram Protocol (UDP) using port 123. Security Manager supports NTP version 3, as defined in RFC 1305.

Related Topics

- Defining NTP Servers , on page 101

Defining NTP Servers

This procedure describes how to define the NTP servers that the routers users to synchronize time. After the NTP policy is deployed, the router uses an algorithm (based on factors such as delay, dispersion, and jitter) to determine which NTP server is the most accurate and synchronizes to that one.

At the global level, you can enable MD5 authentication and specify a source address to use on all NTP packets sent from the router.

To add an NTP server to the policy, all you need to do is enter its IP address. In addition, you can optionally define authentication parameters and determine whether a particular server should be preferred over other NTP servers of similar accuracy.

Related Topics

- Defining NTP Servers , on page 101

Procedure

Step 1 Do one of the following:

- (Device view) Select **Platform > Device Admin > Server Access > NTP** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Server Access > NTP** from the Policy Type selector. Select an existing policy or create a new one.

The NTP page is displayed. See Table 41: NTP Page , on page 103 for a description of the fields on this page.

Step 2 (Optional) In the Source Interface field, enter the name of the interface or interface role whose address should be used as the source interface for all NTP packets sent from the router, or click **Select** to select an interface role from a list or to create a new one. The source interface must have an IP address.

This option is useful when the NTP server cannot reach the address from which the connection originated (for example, due to a firewall). If you do not enter a value in this field, the address of the outgoing interface is used.

Note
You can override this global setting for individual NTP servers, as described in Step 5, on page 101.

Step 3 (Optional) Select the **Enable NTP Authentication** check box to authenticate all associations between this router and the NTP servers defined in this policy.

Step 4 Click the **Add** button under the Servers table to display the NTP Server dialog box. From here you can define an NTP server.

Step 5 Define an NTP server. See Table 42: NTP Server Dialog Box , on page 104 for a description of the available fields.

Step 6 (Optional) Define authentication parameters for this NTP server.

Note
If you modify the value of a previously defined authentication key, the change affects all NTP servers that share this key.

Note
When you define an authentication key in Security Manager, the value 0 is automatically appended to the end of the CLI command. This value, which represents the default authentication key encryption type, can be modified using the CLI.

Step 7 Repeat Step 5, on page 101 and Step 6, on page 101 to define additional NTP servers.

Step 8 Click **OK** to save your definitions locally on the client and close the dialog box. Your definitions are displayed in the Servers table.

Note
To edit an NTP server, select it from the Servers table, then click **Edit**. To remove an NTP server, select it, then click **Delete**. If the key defined on the server you delete is not defined on a different NTP server, the key is also deleted.

NTP Policy Page

Use the NTP page to define one or more NTP servers that the router can use for time synchronization. This includes enabling authentication, if required, and defining a global source interface for all traffic sent to these servers.

For more information, see Defining NTP Servers , on page 101.

Navigation Path

- (Device view) Select **Platform > Device Admin > Server Access > NTP** from the Policy selector.
- (Policy view) Select **Router Platform > Device Admin > Server Access > NTP** from the Policy Type selector. Right-click **NTP** to create a policy, or select an existing policy from the Shared Policy selector.

Related Topics

- NTP on Cisco IOS Routers , on page 100
- Understanding Interface Role Objects
- Table Columns and Column Heading Features
- Filtering Tables

Field Reference

Table 41: NTP Page

Element	Description
Source Interface	The source address for all packets sent to an NTP server. This setting might be necessary when the NTP server cannot respond to the address from which the packet originated (for example, due to a firewall). The source interface must have an IP address. If you do not define a value in this field, the address of the outgoing interface is used. Enter the name of an interface or interface role, or click **Select** to select the object from a list or to create a new one. **Note** The source interface defined in this field is a global setting that you can override for individual NTP servers. For more information, see NTP Server Dialog Box , on page 104.
Enable NTP Authentication	When selected, enables authentication using MD5 when connecting to an NTP server. When deselected, authentication is disabled.
Servers Table	
IP Address	The IP address of the NTP server.
Source Interface	The source address for all packets sent to this NTP server. This setting overrides the global setting defined at the top of the page.
Preferred	Indicates whether this NTP server is preferred over other NTP servers of similar accuracy. **Note** By default, preferred servers are listed first in the table.
Key Number	The ID number of the key used for authentication with this NTP server.
Trusted	Indicates whether the authentication key defined for this NTP server is a trusted key.
Add button	Opens the NTP Server Dialog Box , on page 104. From here you can define an NTP server.
Edit button	Opens the NTP Server Dialog Box , on page 104. From here you can edit the selected NTP server.
Delete button	Deletes the selected NTP server from the table. If the key defined on the server you delete is not defined on a different NTP server, the key is also deleted.

NTP Server Dialog Box

Use the NTP Server dialog box to define the address of an NTP server that the router can use to perform time synchronization. In addition, you can use this dialog box to define a default source interface for NTP packets sent to this server and authentication parameters.

Navigation Path

Go to the NTP Policy Page , on page 102, then click the **Add** or **Edit** button beneath the table.

Related Topics

- Defining NTP Servers , on page 101
- NTP on Cisco IOS Routers , on page 100
- Understanding Interface Role Objects

Field Reference

Table 42: NTP Server Dialog Box

Element	Description
IP Address	The IP address of the NTP server. Enter an address or the name of a network/host object, or click **Select** to select the object from a list or to create a new one.
Source Interface	The source address for all packets sent to this NTP server. This setting might be necessary when the NTP server cannot respond to the address from which the packet originated (for example, due to a firewall). The source interface must have an IP address. If you do not define a value in this field and there is no global setting, the address of the outgoing interface is used. **Note** This setting overrides the global setting you defined on the NTP Policy Page , on page 102. Enter the name of an interface or interface role, or click **Select** to select the object from a list or to create a new one.
Preferred	When selected, this NTP server is preferred over other NTP servers of similar accuracy. If this server is used for synchronization, the time offset used to correct the local clock is calculated from this server only. **Note** If a different NTP server is significantly more accurate than the preferred server (for example, stratum 2 versus stratum 3), the router synchronizes to the more accurate server. When deselected, this NTP server is not given preference over other NTP servers of similar accuracy. The time offset used to correct the local clock is calculated by taking the combined offset of all NTP servers. We recommend that you configure an NTP server as preferred only when multiple servers have the same stratum and you can rely on the accuracy of the preferred server.

Element	Description
Authentication Key	The MD5 key that is used to authenticate associations with the NTP server. • Key Number—The ID number of the authentication key. Enter the key number or select a previously defined number from the list. • Key Value—An arbitrary string of up to 32 characters that defines the authentication key. Enter the string again in the Confirm field. • Trusted—When selected, this key authenticates the identity of systems attempting to synchronize with this server. When deselected, this key is not used for authentication. If you select a key number from the list and then change the key value, you are warned that saving this change affects any other NTP servers using the same authentication key. **Note** To use authentication, you must enable it from the NTP Policy Page , on page 102.