Configuring Device Access Settings on Firewall Devices

The Device Access section, located under the Device Admin folder in the Policy selector, contains pages for defining access to firewall devices.

This chapter contains the following topics:

- Configuring Console Timeout, page 49-1
- HTTP Page, page 49-2
- Configuring ICMP, page 49-4
- Configuring Management Access, page 49-6
- Configuring Management Session Quota Limits, page 49-7
- Configuring Secure Shell Access, page 49-7
- Configuring SSL - Basic and Advanced tabs, page 49-9
- Reference Identities, page 49-13
- Configuring SNMP, page 49-14
- Telnet Page, page 49-29

Configuring Console Timeout

Use the Console page to specify a timeout value for inactive console sessions. When the time limit you specify is reached, the console session is closed.

In the **Console Timeout** field, enter the number of minutes a console session can remain idle before the device closes it. Valid values are 0 to 60 minutes. To prevent a console session from timing out, enter 0.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Console** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > Console** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Chapter 49, "Configuring Device Access Settings on Firewall Devices"

HTTP Page

Use the table on the HTTP page to manage the interfaces configured to access the HTTP server on a device, as well as HTTP redirect to HTTPS on those interfaces. You also can enable or disable the HTTP server on the device from this page. Administrative access by the specific device manager requires HTTPS access.

Note To redirect HTTP, the interface requires an access list that permits HTTP. Otherwise, the interface cannot listen to port 80, or to any other port that you configure for HTTP.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > HTTP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > HTTP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 49-1 HTTP Page

Element	Description
HTTP Interface table	Use the Add Row, Edit Row, and Delete Row buttons below this table to manage device interfaces on which HTTP-to-HTTPS redirect is configured. Add Row and Edit Row open the HTTP Configuration Dialog Box, page 49-3.
Fetch user name from certificate settings	Select this option to set the rules for extracting a username from the certificate. Enter the following: • Enable HTTP username from certificate—Check this box to get the HTTP username from the certificate for authentication. • Pre-fill user name—Check the Pre-fill Username checkbox to enable the use of this name for authentication. When enabled, this username, along with the password entered by the user, are used for authentication. Choose one of the following options: **Note** This feature is supported only in devices running ASA software version 9.4(1) or later. • Use the Entire DN as the username—Select this option if you want to use the entire DN as the username. This option is disabled by default.

Table 49-1 HTTP Page (continued)

Element	Description
Fetch user name from certificate settings (contd..)	• Specify individual DN fields as the username—Choose from the Primary DN Field and Secondary DN Field drop-down values to specify which attributes and additional attributes to use to derive the username. This option is enabled by default. – C—Country: the two-letter country abbreviation which conforms to the ISO 3166 country abbreviations. – CN—Common Name: the name of a person, system, or other entity. Not available as a secondary attribute. – DNQ—Domain Name Qualifier. – EA—Email address. – GENQ—Generational qualifier. – GN—Given name. – I—Initials. – L—Locality: the city or town where the organization is located. – N—Name. – O—Organization: the name of the company, institution, agency, association, or other entity. – OU—Organizational Unit: the subgroup within the organization (O). – SER—Serial number. – SN—Surname. – SP—State/Province: the state or province where the organization is located. – T—Title. – UID—User Identifier. – UPN—User Principal Name. • Use LUA Script generated by ASDM—Choose this option if you want to use the LUA script that is generated by ASDM. This option is disabled by default.
Enable HTTP Server	Enables or disables the HTTP server on the device. When enabled, you can specify a communications **Port** for the server. The Port range is 1 to 65535; the default is 443.

HTTP Configuration Dialog Box

Use the HTTP Configuration dialog box to add or edit a host or network that will be allowed to access the HTTP server on the device via a specific interface; you also can enable and disable HTTP redirect.

Navigation Path

You can access the HTTP Configuration dialog box from the HTTP Page, page 49-2.

Field Reference

Table 49-2 HTTP Configuration Dialog Box

Element	Description
Interface Name	Enter or Select the interface on which access to the HTTP server on the device is allowed. **Note** Beginning with Cisco Security Manager version 4.17, you can configure BVI interface for HTTP on ASA 9.9.2 devices and above. However, in multi-context, "Transparent" mode security context only supports BVI interface.
IP Address/Netmask	Enter the IP address and netmask, separated by a forward slash ("/") of the host or network that is permitted to establish an HTTP connection with the device. Alternately, you can click Select to select a Networks/Hosts object. **Note** Beginning with version 4.13, Cisco Security Manager supports policies—Groups, Hosts, Address Range, and Network for IPv6 devices.
Enable Authentication Certificate	Select this option to require user certificate authentication in order to establish an HTTP connection. On ASA and PIX 8.0(2)+ devices, you can specify the authentication **Port**.
Certificate Maps	Select the Certificate Map name that you configured in Remote Access VPN > certificate to Connection Profile Maps > Rules. For more information, see Map Rule Dialog Box (Upper Table), page 31-39. None is selected by default. This feature is available beginning with Security Manager version 4.12 for ASA 9.6(2) or later devices. This option is supported for single, multi, routed and transparent contexts for ASA devices.
Redirect port	The port on which the security appliance listens for HTTP requests, which it then redirects to HTTPS. To disable HTTP redirect, ensure that this field is blank.

Configuring ICMP

Use the table on the ICMP page to manage Internet Control Message Protocol (ICMP) rules, which specify the addresses of all hosts or networks that are allowed or denied ICMP access to specific interfaces on the security device.

Note Starting from ASA 8.2(1) ICMP IPv6 was supported in the transparent firewall mode.

The ICMP rules control ICMP traffic that terminates on any device interface. If no ICMP control list is configured, the device accepts all ICMP traffic that terminates at any interface, including the outside interface. However, by default, the device does not respond to ICMP echo requests directed to a broadcast address.

It is recommended that permission is always granted for the ICMP Unreachable message (type 3). Denying ICMP Unreachable messages disables ICMP Path MTU discovery, which can halt IPsec and PPTP traffic. See RFC 1195 and RFC 1435 for details about Path MTU Discovery.

If an ICMP control list is configured, the device uses a first match to the ICMP traffic, followed by an implicit deny all. That is, if the first matched entry is a permit entry, the processing of the ICMP packet continues. If the first matched entry is a deny entry, or an entry is not matched, the device discards the ICMP packet and generates a syslog message. If an ICMP control list is not configured, a permit rule is assumed in all cases.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > ICMP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > ICMP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Note ICMP IPv6 support is not available for PIX and FWSM devices.

Field Reference

Table 49-3 ICMP Page

Element	Description
ICMP Rules Table	Use the Add Row, Edit Row, and Delete Row buttons below this table to manage ICMP rules. Add Row opens the Add ICMP dialog box, while Edit Row opens the Edit ICMP dialog box. See Add and Edit ICMP Dialog Boxes, page 49-5 for information about these dialog boxes.
ICMP Unreachable Parameters	
Rate Limit	For ICMP traffic that terminates at an interface on this device, the maximum number of ICMP Unreachable messages the device can transmit per second. This value can be between 1 and 100 messages per second; the default is 1 message per second.
Burst Size	The burst size for ICMP Unreachable messages; this can be a value between 1 and 10. **Note** This parameter is not currently used by the system, so you can choose any value.

Add and Edit ICMP Dialog Boxes

Use the Add ICMP dialog box to add an ICMP rule, which specifies a host/network that is allowed or denied the specified ICMP access on the specified device interface.

Note The Edit ICMP dialog box is virtually identical to the Add ICMP dialog box, and is used to modify existing ICMP rules. The following descriptions apply to both dialog boxes.

Navigation Path

You can access the Add or Edit ICMP dialog boxes from the Configuring ICMP, page 49-4.

Note While adding an ICMP policy, make sure that the network and service is of the same type i.e. IPv6 networks support IPv6 services.

Field Reference

Table 49-4 Add and ICMP Dialog Boxes

Element	Description
Action	Whether this rule permits or denies the selected ICMP Service message from the specified Network on the specified Interface. Choose: • **Permit** – ICMP messages from the specified networks/hosts are allowed to the specified interface. • **Deny** – ICMP messages from the specified networks/hosts to the specified interface are dropped.
ICMP Service	Enter or Select the specific ICMP service message to which the rule applies.
Interface	Enter or Select the device interface to which these ICMP messages are directed.
Network	Enter a host name, IPv4 or IPv6 address, or Select a Networks/Hosts object, to define the specified ICMP message source.

Configuring Management Access

Use the Management Access page to enable or disable access on a high-security interface so you can perform management functions on the device. You can enable this feature on an internal interface to allow management functions to be performed on the interface over an IPsec VPN tunnel. You can enable the Management Access feature on only one interface at a time.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Management Access** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > Management Access** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Enabling and Disabling Management Access

In the **Management Access Interface** field, enter the name of the device interface that is to permit management access connections. You can click Select to select the interface from a list of interface objects.

You can enable the Management Access feature on only one interface at a time.

Clear the Management Access Interface field to disable management access.

Configuring Management Session Quota Limits

Beginning with 4.19, Cisco Security Manager allows you to configure enforcement of limits for the maximum number of admin sessions across all connection types and usernames, and for maximum number of concurrent sessions per username as well as per protocol limits on ASA 9.12(1) devices or later. The configured session concurrence limits is enforced prior to authenticating the incoming administrative session.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > Management Session Quota** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > Management Session Quota** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Note The sequence of enforcement on the session limits would be—user limit followed by aggregate limit, and then by protocol limit.

Field Reference

Table 49-5 Add and ICMP Dialog Boxes

Element	Description
Aggregate	The maximum number of admin sessions across all connection types. The default is 15. You can configure the limit between 1 and 15.
HTTP	Enter management session quota limit for HTTP between 1 and 5. The default value is 5.
SSH	Enter management session quota limit for SSH between 1 and 5. The default value is 5.
Telnet	Enter management session quota limit for Telnet between 1 and 5. The default value is 5.
User	Enter management session quota limit for the user between 1 and 5. There is no default value specified for user limit.

Configuring Secure Shell Access

Use the Secure Shell page to configure rules that permit administrative access to a security device using the SSH protocol. The rules restrict SSH access to a specific IP address and netmask. Any SSH connection attempts that comply with these rules must then be authenticated by an AAA server or Telnet password.

Navigation Path

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

- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > Secure Shell** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 49-6 Secure Shell Page

Element	Description
SSH Version	Specify the SSH version(s) accepted by the device: choose **1**, **2**, or **1 and 2**. By default, SSH Version 1 and SSH Version 2 connections are accepted.
Timeout	Enter the number of minutes, 1 to 60, the Secure Shell session can remain idle before the device closes it. The default value is 5 minutes.
Allowed Hosts table	Use the Add Row, Edit Row, and Delete Row buttons below this table to manage the hosts allowed to connect to the security device via SSH. Add Row opens the Add Host dialog box, while Edit Row opens the Edit Host dialog box. See Add and Edit SSH Host Dialog Boxes, page 49-8 for information about these dialog boxes.
Enable Secure Copy	Check this box to enable the secure copy (SCP) server on the security appliance. This allows the appliance to function as an SCP server for transferring files from/to the device. Only clients that are allowed to access the security appliance using SSH can establish a secure copy connection. This implementation of the secure copy server has the following limitations: • The server can accept and terminate connections for secure copy, but cannot initiate them. • The server does not have directory support. The lack of directory support limits remote client access to the security appliance internal files. • The server does not support banners. • The server does not support wildcards. • The security appliance license must have the VPN-3DES-AES feature to support SSH version 2 connections.

Add and Edit SSH Host Dialog Boxes

Use the Add Host dialog box to add an SSH access rule.

Note The Edit Host dialog box is virtually identical to the Add Host dialog box, and is used to modify existing SSH access rules. The following descriptions apply to both dialog boxes.

Navigation Path

You can access the Add and Edit Host dialog boxes from the Configuring Secure Shell Access, page 49-7.

Field Reference

Table 49-7 Add and Edit Host Dialog Boxes

Element	Description
Interface	Enter or Select the name of the device interface on which SSH connections are permitted. **Note** Beginning with Cisco Security Manager version 4.17, you can configure BVI interface for SSH connections on ASA 9.9.2 devices and above. However, in multi-context, "Transparent" mode security context only supports BVI interface.
IP Addresses	Enter the name or IP address for each host or network that is permitted to establish an SSH connection with the security device on the specified interface; use commas to separate multiple entries. You also can click Select to select Networks/Hosts objects from a list. **Note** Beginning with version 4.13, Cisco Security Manager supports policies—Groups, Hosts, Address Range, and Network for IPv6 devices.

Configuring SSL - Basic and Advanced tabs

Beginning from version 4.8, Security Manager provides enhanced security features using Secure Sockets Layer (SSL).

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > SSL** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > SSL** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Field Reference

Table 49-8 SSL Page Basic Tab

Element	Description
Certificate Authentication	
FCA Timeout	Enter a value in the range of 1 to 120. **Note** FCA Timeout is applicable for devices running the ASA software version 9.1(2) or later.
Interface	Use the Add Row, Edit Row, and Delete Row buttons below the Interface table to manage the interfaces and their port numbers allowed to connect to the security device via SSL. Add Row opens the Add Interface and Port dialog box, while Edit Row opens the Edit Interface and Port dialog box. You can select the interface from the available entries in the Interface Selector dialog box. Enter a value in the range of 1 to 65535 for the port number.

Table 49-8 SSL Page Basic Tab (continued)

Element	Description
Client Version SSL/TLS Protocol Version	The Client Version is the SSL/TLS protocol version to use when the device acts as a client. Select any one of the following: • Any—Select this keyword to transmit SSLV3 ClientHellos and negotiate SSLV3 or greater. This is the default keyword. • SSLV3—Enter this keyword to transmit SSLv3 ClientHellos and negotiate SSLV3 or greater. • TLSV1—Enter this keyword to transmit TLSv1 ClientHellos and negotiate TLSV1 or greater. • TLSV1.1—Enter this keyword to transmit TLSV1.1 ClientHellos and negotiate TLSV1.1 or greater. • TLSV1.2—Enter this keyword to transmit TLSV1.2 ClientHellos and negotiate TLSV1.2 or greater. **Note** TLSV1.1 and TLSV1.2 protocol versions are applicable for devices running the ASA software version 9.3(2) or later.
Server Version SSL/TLS Protocol Version	The Server Version is the minimum SSL/TLS protocol version to use when the device acts as a server. Select any one of the following: • Any—Select this keyword to accept SSLV2 ClientHellos and negotiate the highest common version. This is the default keyword. • SSLV3—Enter this keyword to accept SSLV2 ClientHellos and negotiate SSLV3 or greater. • SSLV3-Only—Enter this keyword to accept SSLV2 ClientHellos and negotiate SSLV3 or greater. • TLSV1—Enter this keyword to accept SSLV2 ClientHellos and negotiate TLSV1 or greater. • TLSV1-Only—Enter this keyword to accept SSLV2 ClientHellos and negotiate TLSV1 or greater. • TLSV1.1—Enter this keyword to accept SSLV2 ClientHellos and negotiate TLSV1.1 or greater. • TLSV1.2—Enter this keyword to accept SSLV2 ClientHellos and negotiate TLSV1.2 or greater. **NOTES:** • The **Any** keyword is the default for both Server Version and Client Version and means that the device will negotiate the highest common supported version of TLS. • TLSV1.1 and TLSV1.2 protocol versions are applicable for devices running the ASA software version 9.3(2) or later. • SSLV3-Only and TLSV1-Only protocol versions are applicable for devices running the ASA software version older than 9.3(2).

Table 49-9 SSL Page Advanced Tab

Element	Description
Advanced SSL Settings for devices running the ASA software version older than 9.3(2)	
Encryption	Choose the encryption algorithms from the available list. To add an encryption algorithm, select the item in the Available Members list and then click >>. The item is moved from the Available Members list to the Selected Members list. You can add multiple encryption algorithms. The available encryption algorithms are as follows: • 3DES-SHA1 • AES128-SHA1 • AES256-SHA1 • DES-SHA1 • RC4-MD5 • RC4-SHA1 • NULL-SHA1 • DHE-AES128-SHA1 • DHE-AES256-SHA1 **Note** Beginning from 4.19, Cisco Security Manager does not support configuring TLS proxy with NULL SHA1 in SSL ciphers in ASA 9.12(1) and later devices. To remove an encryption algorithm, select the item in the Selected Members list and then click <<. The item is moved from the Selected Members list to the Available Members list. Click Save to save your settings.
Advanced SSL Settings for devices running the ASA software version 9.3(2) or later	
SSL Cipher	Use the Add Row, Edit Row, and Delete Row buttons below the SSL Cipher table to manage the SSL cipher version and level. On the Add Cipher dialog select a combination of the version and level.
Version	Select one of the following versions: • DEFAULT • DTLSV1 • DTLSV1.2 • SSLV3 • TLSV1 • TLSV1.1 • TLSV1.2 **Note** The DEFAULT keyword is used to configure outbound connections when the device is acting as a client and establishing a connection to a server. All the other keywords are used when the device is acting as a server and accepting connections from a client. **Note** The SSLV3 version has been deprecated from ASA version 9.4(1). Therefore, beginning with version 4.9, Security Manager performs a validation to check if SSLV3 option has been configured for any ASA devices running the version 9.4(1) or later.

Table 49-9 SSL Page Advanced Tab (continued)

Element	Description
Level	Select one of the following versions: • ALL - It includes all ciphers including NULL-SHA. • LOW - It includes all ciphers except NULL-SHA. • MEDIUM - It includes all ciphers except NULL-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5. • FIPS - It includes all FIPS-compliant ciphers (that is, not NULL-SHA:DES-CBC-SHA:RC4-MD5:RC4-SHA:DES-CBC3-SHA) • HIGH - It includes only AES-256 with SHA-2 ciphers, so it only applies to TLSV1.2.
Custom String	Use the CUSTOM keyword for Security Manager to exercise full control over the cipher suite using OpenSSL cipher definition strings. **Note** Beginning with version 4.9, Security Manager provides support for the following new TLSV1.2 ciphers for devices running the ASA software version 9.4(1) or later. • ECDHE_RSA_AES128_SHA256 • ECDHE_RSA_AES256_SHA384 • ECDHE_ECDSA_AES128_SHA256 • ECDHE_ECDSA_AES256_SHA384 **Note** Beginning with version 4.16, Security Manager provides support for the following new TLSV1.2 ciphers in addition to the above mentioned ciphers for devices running the ASA software version 9.4(1) or later. • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • AES128-GCM-SHA256
ECDH Configuration	Select from one of the options (19,20,21,none) in the ECDH Group. This feature is available from Security Manager version 4.9 onwards for ASA devices version 9.4(1) or later.

Note Due to import regulations in some countries the Oracle implementation provides a default cryptographic jurisdiction policy file that limits the strength of cryptographic algorithms. If stronger algorithms need to be configured or are already configured on the device (for example, AES with 256-bit keys, DH group with 5,14,24), follow these steps:

1. Download the Java 7 unlimited strength cryptography policy .jar files from http://www.oracle.com. Cisco recommends to search for the following on the Oracle website:

   Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files Java 7

(Click the download button to download the files by accepting the license agreement.)

2. Replace local_policy.jar and US_export_policy.jar on your Security Manager server in the folder CSCOpx\MDC\vms\jre\lib\security.
3. Restart your Security Manager server.

Reference Identities

Beginning with version 4.12, Security Manager enables you to configure Reference Identity policy objects for Secure Syslog Server connections on devices running the ASA software version 9.6(2) or later. This object enables support for Common Criteria requirements.
Reference identities are configured as one or more identifiers to be compared to the presented identifiers in the server certificate. Identifiers are specific instances of the four identifier types specified in RFC 6125.

Add/Edit Reference Identity Dialog Box

Use the Add/Edit Reference Identity Dialog Box to create a new Reference Identity policy object or to edit existing policy objects.

Navigation Path

Select **Manage > Policy Objects**, then select **Reference Identity** from the Object Type Selector. Right-click inside the work area, then select **New Object** or click the **+** button to add a new object, or right-click a row, then select **Edit Object.**

Field Reference

Table 49-10 Add/Edit Reference Identity Dialog Box

Element	Description
Name	Name of the Reference Identity policy object. Note that each Reference Identifier can have multi line values.
Description	Description of the Reference Identity policy object.
Common Name ID	A Relative Distinguished Name (RDN) in a certificate subject field that contains only one attribute-type-and-value pair of type Common Name (CN), where the value matches the overall form of a domain name. The CN value can be free text. A CN-ID reference identifier does not identify an application service.
Domain Name ID	A subjectAltName entry of type dNSName. This is a DNS domain name. A DNS-ID reference identifier does not identify an application service.
Service Name ID	A subjectAltName entry of type otherName whose name form is SRVName as defined in RFC 4985. A SRV-ID identifier may contain both a domain name and an application service type. For example, a SRV-ID of “_imaps.example.net” would be split into a DNS domain name portion of “example.net” and an application service type portion of “imaps.”

Table 49-10 Add/Edit Reference Identity Dialog Box (continued)

Element	Description
Uniform Resource Identifier ID	A subjectAltName entry of type uniformResourceIdentifier whose value includes both (i) a "scheme" and (ii) a "host" component (or its equivalent) that matches the "reg-name" rule specified in RFC 3986. A URI-ID identifier must contain the DNS domain name, not the IP address, and not just the hostname. For example, a URI-ID of "sip:voice.example.edu" would be split into a DNS domain name portion of "voice.example.edu" and an application service type of "sip."
Category	(Optional) Select a category between CAT-A and CAT-J.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden, page 6-18 and Understanding Policy Object Overrides for Individual Devices, page 6-18. If you allow device overrides, you can click the Edit button to create, edit, and view the overrides. The Overrides field indicates the number of devices that have overrides for this object.

Note A reference identity is created when configuring one with a previously unused name. Once a reference identity has been created, the four identifier types and their associated values can be added or deleted from the reference identity. The reference identifiers MAY contain information identifying the application service and MUST contain information identifying the DNS domain name.

Configuring SNMP

Simple Network Management Protocol (SNMP) defines a standard way for network management stations running on PCs or workstations to monitor the health and status of many types of devices, including switches, routers, and security appliances. You can use the SNMP page to configure a firewall device for monitoring by SNMP management stations.

The Simple Network Management Protocol (SNMP) enables monitoring of network devices from a central location. Cisco security appliances support network monitoring using SNMP versions 1, 2c, and 3, as well as traps and SNMP read access; SNMP write access is not supported.

You can configure a security appliance to send "traps" (event notifications) to a network management station (NMS), or you can use the NMS to browse the management information bases (MIBs) on the security appliance. Use CiscoWorks for Windows or any other SNMP MIB-II-compliant browser to receive SNMP traps and browse a MIB.

The security appliance has an SNMP agent that notifies designated management stations if specified events occur, for example, when a link in the network goes up or down. The notification includes an SNMP system object ID (OID), identifying the device to the management stations. The security appliance SNMP agent also replies when a management station asks for information.

SNMP MIBs and OIDs

An SNMP trap reports significant events occurring on a network device, most often errors or failures. SNMP traps are defined in Management Information Bases (MIBs), which can be either standard or enterprise-specific.

Standard traps and MIBs are created by the Internet Engineering Task Force (IETF) and documented in various RFCs. Standard traps are compiled into the security appliance software. If needed, you can also download RFCs, standard MIBS, and standard traps from the IETF website: http://www.ietf.org/.

For Cisco MIB files and OIDs, refer to: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml. OIDs may be downloaded from this FTP site: ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz.

This section contains the following topics:

- SNMP Terminology, page 49-15
- SNMP Version 3, page 49-15
- SNMP Page, page 49-17

SNMP Terminology

Here are definitions for some common SNMP terms:

- **Agent** – The SNMP server running on the security appliance. The agent responds to requests for information and action from the management station. The agent also controls access to its management information base (MIB), the collection of data objects that can be viewed or changed by the SNMP manager.
- **Management stations** – The PCs or workstations set up to monitor SNMP events and manage devices such as the security appliance. Management stations can also receive messages about events which require attention, such as hardware failures.
- **MIBs** – The agent maintains standardized data structures called Management Information Bases (MIBs), used to collect information, such as packet, connection and error counters, and buffer usage and failover status. A number of MIBs are defined for specific products, and for the common protocols and hardware standards used by most network devices. SNMP management stations can browse MIBs, or request only specific fields. In some applications, MIB data can be modified for administrative purposes.
- **OID** – The SNMP standard assigns a system object ID (OID) so that a management station can uniquely identify network devices with SNMP agents, and indicate to users the source of information monitored and displayed.
- **Traps** – Specified events that generate a message from the SNMP agent to the management station. Events include alarm conditions such as linkup, linkdown, coldstart, warmstart, authentication, or syslog events.

SNMP Version 3

SNMP Version 3 provides security enhancements that are not available in SNMP Version 1 or SNMP Version 2c. SNMP Versions 1 and 2c transmit data between the SNMP server and SNMP agent in clear text. SNMP Version 3 adds authentication and privacy options to secure protocol operations. In addition, this version controls access to the SNMP agent and MIB objects through the User-based Security Model

(USM) and View-based Access Control Model (VACM). The ASA and ASASM also support the creation of SNMP groups and users, as well as hosts, which is required to enable transport authentication and encryption for secure SNMP communications.

Note SNMP Version 3 is supported on ASA devices running 8.2(1) or later and on ASASM devices running 8.5(1) or later.

Security Models

For configuration purposes, the authentication and privacy options are grouped together into security models. Security models apply to users and groups, which are divided into the following three types:

- NoAuth—No Authentication and No Privacy, which means that no security is applied to messages.
- Auth—Authentication but No Privacy, which means that messages are authenticated.
- Priv—Authentication and Privacy, which means that messages are authenticated and encrypted.

SNMP Groups

An SNMP group is an access control policy to which users can be added. Each SNMP group is configured with a security model, and is associated with an SNMP view. A user within an SNMP group must match the security model of the SNMP group. These parameters specify what type of authentication and privacy a user within an SNMP group uses. Each SNMP group name and security model pair must be unique.

SNMP Users

SNMP users have a specified username, a group to which the user belongs, authentication password, encryption password, and authentication and encryption algorithms to use. The authentication algorithm options are MD5 and SHA. The encryption algorithm options are DES, 3DES, and AES (which is available in 128, 192, and 256 versions). When you create a user, you must associate it with an SNMP group. The user then inherits the security model of the group.

SNMP Hosts

An SNMP host is an IP address to which SNMP notifications and traps are sent. To configure SNMP Version 3 hosts, along with the target IP address, you must configure a username, because traps are only sent to a configured user. SNMP target IP addresses and target parameter names must be unique on the ASA and ASA Services Module. Each SNMP host can have only one username associated with it. To receive SNMP traps, configure the SNMP NMS, and make sure that you configure the user credentials on the NMS to match the credentials for the ASA and ASASM.

Implementation Differences Between the ASA, ASA Services Module, and the Cisco IOS Software

The SNMP Version 3 implementation in the ASA and ASASM differs from the SNMP Version 3 implementation in the Cisco IOS software in the following ways:

- The local-engine and remote-engine IDs are not configurable. The local engine ID is generated when the ASA or ASASM starts or when a context is created.
- No support exists for view-based access control, which results in unrestricted MIB browsing.
- Support is restricted to the following MIBs: USM, VACM, FRAMEWORK, and TARGET.
- You must create users and groups with the correct security model.
- You must remove users, groups, and hosts in the correct sequence.

- Use of the **snmp-server host** command creates an ASA or ASASM rule to allow incoming SNMP traffic.

SNMP Page

Use the SNMP page to configure the security appliance for monitoring by Simple Network Management Protocol (SNMP) management stations.

Note For SNMP Version 3, configuration must occur in the following order: group, user, host.

Navigation Path

- (Device view) Select **Platform > Device Admin > Device Access > SNMP** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Device Access > SNMP** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Configuring SNMP, page 49-14
- SNMP Trap Configuration Dialog Box, page 49-19
- Add/Edit SNMP Host Access Entry Dialog Box, page 49-22
- Add/Edit SNMP Host Group Entry Dialog Box, page 49-23
- Add/Edit SNMP Group Entry Dialog Box, page 49-24
- Add/Edit SNMP User Entry Dialog Box, page 49-25
- Add/Edit SNMP User List Entry Dialog Box, page 49-27

Field Reference

Table 49-11 SNMP Page

Element	Description
Enable SNMP Servers	When this option is selected, the security device provides SNMP information on the specified interface(s). You can deselect this option to disable SNMP monitoring while retaining the configuration information.
Read Community String Confirm	Enter the password used by a SNMP management station when sending requests to this device. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. The security device uses the password to determine if the incoming SNMP request is valid. The password is a case-sensitive alphanumeric string of up to 32 characters; spaces are not permitted. Repeat the password in the **Confirm** field to ensure it was entered correctly.

Table 49-11 SNMP Page (continued)

Element	Description
System Administrator Name	Enter the name of the device administrator or other contact person. This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
Location	Describe the location of this security device (for example, ***Building 42, Sector 54***). This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
Port (PIX 7.x, ASA and FWSM 3.x only)	Specify the port on which incoming requests will be accepted. The default is 161.
Configure SNMP Traps	Click this button to configure SNMP traps in the SNMP Trap Configuration Dialog Box, page 49-19.
SNMP Engine ID	Shows the ID of the SNMP engine configured on the device. Click **Get SNMP Engine ID** to retrieve the engine ID from the device.
SNMP Hosts table	This table lists the SNMP management stations that can access the security appliance. This is a standard Security Manager table, with Add Row, Edit Row and Delete Row buttons, as described in Using Tables, page 1-48. The Add Row and Edit Row buttons open the Add/Edit SNMP Host Access Entry Dialog Box, page 49-22, used to add and edit management station host entries. **Note** For ASA devices running 9.1(5) or later, you can configure up to 129 SNMP hosts. For other devices and earlier ASA versions, you can only configure up to 32 SNMP hosts.
SNMP Host Group table	Beginning with version 4.12, Security Manager enables you to add and edit the Host Group entries for SNMP Users. See Add/Edit SNMP Host Group Entry Dialog Box, page 49-23 for more information.
SNMPv3 Configuration	
SNMP Group tab	Lists the SNMP groups that have been configured. This is a standard Security Manager table, with Add Row, Edit Row and Delete Row buttons, as described in Using Tables, page 1-48. The Add Row and Edit Row buttons open the Add/Edit SNMP Group Entry Dialog Box, page 49-24, used to add and edit SNMP groups.
SNMP User tab	Lists the SNMP users that have been configured. This is a standard Security Manager table, with Add Row, Edit Row and Delete Row buttons, as described in Using Tables, page 1-48. The Add Row and Edit Row buttons open the Add/Edit SNMP User Entry Dialog Box, page 49-25, used to add and edit SNMP users.
SNMP User List tab	Beginning with version 4.12, Security Manager enables you to add a user list containing multiple SNMP users. See Add/Edit SNMP User List Entry Dialog Box, page 49-27 for more information.

SNMP Trap Configuration Dialog Box

Use the SNMP Trap Configuration dialog box to configure SNMP traps (event notifications) for the selected security device.

Traps are different than browsing; they are unsolicited "comments" from the managed device to the management station for certain events, such as ***linkup***, ***linkdown***, and ***syslog event generated***.

An SNMP object ID (OID) for the device appears in SNMP event traps sent from the device. The SNMP service running on a security device performs two functions:

- Replies to SNMP requests from management stations.
- Sends traps to management stations or other devices that are registered to receive them from the security appliance.

Cisco security devices support three types of traps:

- firewall
- generic
- syslog

In the SNMP Trap Configuration dialog box, available traps are presented on four tabbed panels: Standard, Entity MIB, Resource, and Other.

Navigation Path

You can access the SNMP Trap Configuration dialog box from the SNMP Page, page 49-17.

Related Topics

- Configuring SNMP, page 49-14
- Add/Edit SNMP Host Access Entry Dialog Box, page 49-22

Field Reference

Table 49-12 SNMP Trap Configuration Dialog Box

Element	Description
Enable All SNMP Traps	Check this box to quickly select all traps on all four tabbed panels.
Enable Syslog Traps	Check this box to enable transmission of trap-related syslog messages. The severity level for syslog messages trapped is set on the Logging Filters Page, page 54-12.
Select the desired event-notification traps on the following four tabbed panels. Note that only the traps applicable to the selected device are displayed in the dialog box.	

Table 49-12 SNMP Trap Configuration Dialog Box (continued)

Element	Description
Standard	• **Authentication** – Unauthorized SNMP access. This authentication failure occurs for packets with an incorrect community string. • **Link Up** – One of the device's communication links has become available (it has "come up"), as indicated in the notification. • **Link Down** – One of the device's communication links has failed, as indicated in the notification. • **Cold Start** – The device is reinitializing itself such that its configuration or the protocol entity implementation may be altered. • **Warm Start** – The device is reinitializing itself such that its configuration and the protocol entity implementation is unaltered.
Entity MIB	• **Field Replaceable Unit Insert** – A Field Replaceable Unit (FRU) has been inserted, as indicated. (FRUs include assemblies such as power supplies, fans, processor modules, interface modules, etc.) • **Field Replaceable Unit Delete** – A Field Replaceable Unit (FRU) has been removed, as indicated in the notification. • **Configuration Change** – There has been a hardware change, as indicated in the notification. • **Fan Failure** – A device cooling fan has failed, as indicated in the notification. • **CPU Temperature** – Temperature of the central processing unit has reached the configured limit. • **Power-Supply Failure** – A device power supply has failed, as indicated in the notification. • **Redundancy Switchover** – Switchover occurred for redundant component, as indicated in the notification. • **Alarm Asserted** – The condition described by the alarm exists. • **Alarm Cleared** – The condition described by the alarm does not exist.
Resource	• **Connection Limit Reached** – This trap indicates that a connection attempt was rejected because the configured connections limit has been reached. • **Resource Limit Reached** – This notification is generated when the configured resource limit is reached, as described in the notification. • **Resource Rate Limit Reached** – This notification is generated when the configured resource rate limit is reached, as described in the notification

Table 49-12 SNMP Trap Configuration Dialog Box (continued)

Element	Description
Other	• **IKEv2 Start** – Internet Key Exchange version 2 (IKEv2) exchange initiated. • **IKEv2 Stop** – Internet Key Exchange version 2 (IKEv2) exchange terminated. • **Memory Threshold** – Available free memory has fallen below configured threshold, as indicated in the notification. • **ASA CPU Rising Threshold** – This notification is triggered when utilization of CPU resources exceeds the specified Percentage for a specified Period of time: **Percentage** – Enter the desired upper limit of CPU resource usage as a percentage of total available. Valid values range from 10 to 94; default is 70%. **Period** – Specify the length of time, in minutes, that the specified Percentage can be exceeded before notification is triggered. Valid values range from 1 to 60. • **Interface Threshold** – This notification is triggered when utilization of a physical interface exceeds the specified Percentage of total bandwidth: **Percentage** – Enter the desired upper limit on interface usage as a percentage of total available bandwidth. Valid values range from 30 to 99; default is 70%. • **IPSec Start** – IPsec has started, as indicated in the notification. • **IPSec Stop** – IPsec has stopped, as indicated in the notification. • **Remote Access Session Threshold Exceeded** – The number of remote access sessions has reach the defined limit, as indicated in the notification. • **NAT Packet Discard** – This notification is generated when IP packets are discarded by the NAT function. Available Network Address Translation addresses or ports have fallen below configured threshold. • **CPU Rising Threshold** – This notification is triggered when utilization of CPU resources exceeds the specified Percentage for a specified Period of time: **Percentage** – Enter the desired upper limit of CPU resource usage as a percentage of total available. Valid values range from 10 to 100; default is 70%. **Period** – Specify the length of time, in seconds, that the specified Percentage can be exceeded before notification is triggered. Valid values range from 60 to 3600.

Add/Edit SNMP Host Access Entry Dialog Box

Use the Add/Edit SNMP Host Access Entry dialog box to add and edit entries in the SNMP Hosts table on the SNMP page. These entries represent SNMP management stations allowed to access the security device.

For ASA devices running any software version between 9.1(5) and 9.3(2), you can configure 129 SNMP hosts. For ASA devices running the software version lower than 9.1(5) you can configure only 32 SNMP hosts.

Beginning with version 4.9, Security Manager enables you to configure up to 4096 SNMP hosts for ASA devices running the software version 9.4(1) or later. However, only 129 of this number can be for traps. You cannot configure more than 129 trap configured SNMP hosts.

Navigation Path

You can access the Add/Edit SNMP Host Access Entry dialog box from the SNMP Page, page 49-17.

Related Topics

- Configuring SNMP, page 49-14
- SNMP Trap Configuration Dialog Box, page 49-19
- Add/Edit SNMP Group Entry Dialog Box, page 49-24
- Add/Edit SNMP User Entry Dialog Box, page 49-25

Field Reference

Table 49-13 Add/Edit SNMP Host Access Entry Dialog Box

Element	Description
Interface Name	Enter or Select the interface on which this SNMP management station contacts the device.
IP Address	Enter the IP address, or Select a Networks/Hosts object, representing the SNMP management station. **Note** Beginning with Cisco Security Manager version 4.17, IPv6 Address for SNMP policy is supported on ASA 9.9.2 devices and above.
UDP Port	(Optional) Enter a UDP port for requests from the SNMP host. You can use this field to override the global value specified on the SNMP page.
Community String Confirm	Enter the password used by the SNMP management station when sending requests to the security device. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. Thus, the password is used to determine if the incoming SNMP request is valid. The password is a case-sensitive alphanumeric string of up to 32 characters; spaces are not permitted. Repeat the password in the **Confirm** field.
SNMP Version	Choose the version of SNMP used by this management station: **1**, **2c**, or **3**.
SNMP User Name	If SNMP version 3 is selected, select the SNMP user. For information on SNMP users, see Add/Edit SNMP User Entry Dialog Box, page 49-25.

Table 49-13 Add/Edit SNMP Host Access Entry Dialog Box (continued)

Element	Description
Server Poll/Trap Specification	Specify the type(s) of communication with this management station: poll only, trap only, or both trap and poll. Check either or both: • Poll – The security device waits for periodic requests from the management station. • Trap – The device sends trap events when they occur.

Add/Edit SNMP Host Group Entry Dialog Box

Beginning with Security Manager version 4.12, you can use the Add/Edit SNMP Host Group Entry dialog box to add and edit entries in the SNMP Host Group table on the SNMP page. These entries represent SNMP management stations allowed to access the security device.

For ASA devices running any software version between 9.1(5) and 9.4, you can configure 129 SNMP hosts. For ASA devices running the software version lower than 9.1(5) you can configure only 32 SNMP hosts.

Beginning with version 4.9, Security Manager enables you to configure up to 4096 SNMP hosts for ASA devices running the software version 9.4(1) or later. However, only 129 of this number can be for traps. You cannot configure more than 129 trap configured SNMP hosts.

Note If you edit a used Address Range or Network object in the Networks/Host Policy Object Manager after adding or editing SNMP Host or Host Group entries in the Add/ Edit SNMP Host Group entry page, Cisco Security Manager will not validate for the total number of SNMP traps. Thus, if the trap entries exceed 129, it will result in a deployment failure.

Navigation Path

You can access the Add/Edit SNMP Host Access Entry dialog box from the SNMP Page, page 49-17.

Related Topics

- Configuring SNMP, page 49-14
- SNMP Trap Configuration Dialog Box, page 49-19
- Add/Edit SNMP Group Entry Dialog Box, page 49-24
- Add/Edit SNMP User Entry Dialog Box, page 49-25

Field Reference

Table 49-14 Add/Edit SNMP Host Access Entry Dialog Box

Element	Description
Interface Name	Enter or Select the interface on which this SNMP management station contacts the device.
IP Address	Enter the IP address, or Select a Networks/Hosts object, representing the SNMP management station.
UDP Port	(Optional) Enter a UDP port for requests from the SNMP host. You can use this field to override the global value specified on the SNMP page.

Table 49-14 Add/Edit SNMP Host Access Entry Dialog Box (continued)

Element	Description
Community String Confirm	Enter the password used by the SNMP management station when sending requests to the security device. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. Thus, the password is used to determine if the incoming SNMP request is valid. The password is a case-sensitive alphanumeric string of up to 32 characters; spaces are not permitted. Repeat the password in the **Confirm** field.
SNMP Version	Choose the version of SNMP used by this management station: **1**, **2c**, or **3**.
Server Poll/Trap Specification	Specify the type(s) of communication with this management station: poll only, trap only, or both trap and poll. Check either or both: • Poll – The security device waits for periodic requests from the management station. • Trap – The device sends trap events when they occur. **Note** You cannot enable both traps and polling for the same SNMP Host Group. If you need to enable this, Cisco recommends that you use the **snmp-server host** command for the relevant hosts.

Add/Edit SNMP Group Entry Dialog Box

Use the Add/Edit SNMP Group Entry dialog box to add and edit entries in the SNMP Groups table on the SNMP page. An SNMP group is an access control policy to which users can be added. Each SNMP group is configured with a security model, and is associated with an SNMP view. A user within an SNMP group must match the security model of the SNMP group. These parameters specify what type of authentication and privacy a user within an SNMP group uses. Each SNMP group name and security model pair must be unique.

For configuration purposes, the authentication and privacy options are grouped together into security models. Security models apply to users and groups, which are divided into the following three types:

- NoAuth—No Authentication and No Privacy, which means that no security is applied to messages.
- Auth—Authentication but No Privacy, which means that messages are authenticated.
- Priv—Authentication and Privacy, which means that messages are authenticated and encrypted.

Notes

- Before a group can be deleted, you must ensure that all users associated with that group are deleted. If any hosts are associated with a user that needs to be deleted, you must delete those hosts before you can delete the user.
- If users have been configured to belong to a particular group with a certain security model, you must do the following to change the security level of that group:
  a. Remove all host entries associated with any users belonging to the group.
  b. Remove the users from the group.
  c. Deploy the changes to the device.
  d. Change the group security level.

e. Add users that belong to the group.

f. Add hosts belonging to the users that were added for the group.

g. Deploy the changes to the device.

Navigation Path

You can access the Add/Edit SNMP Group Entry dialog box from the SNMP Page, page 49-17.

Related Topics

- Configuring SNMP, page 49-14
- SNMP Trap Configuration Dialog Box, page 49-19
- Add/Edit SNMP Host Access Entry Dialog Box, page 49-22
- Add/Edit SNMP User Entry Dialog Box, page 49-25

Field Reference

Table 49-15 Add/Edit SNMP Group Entry Dialog Box

Element	Description
Group Name	Enter the name of the SNMP group. Group names must be 32 characters or less.
Security Level	Specify the security level for the group: • NoAuth—No Authentication and No Privacy, which means that no security is applied to messages. • Auth—Authentication but No Privacy, which means that messages are authenticated. • Priv—Authentication and Privacy, which means that messages are authenticated and encrypted.

Add/Edit SNMP User Entry Dialog Box

Use the Add/Edit SNMP User Entry dialog box to add a user to an SNMP group or to edit entries in the SNMP User table on the SNMP page. SNMP users inherit the security model of the group to which they are assigned.

Notes

- After a user has been created, you cannot change the group to which the user belongs.
- Before a user can be deleted, you must ensure that no hosts are configured that are associated with that username.

Navigation Path

You can access the Add/Edit SNMP User Entry dialog box from the SNMP Page, page 49-17.

Related Topics

- Configuring SNMP, page 49-14
- SNMP Trap Configuration Dialog Box, page 49-19
- Add/Edit SNMP Host Access Entry Dialog Box, page 49-22

- Add/Edit SNMP Group Entry Dialog Box, page 49-24

Field Reference

Table 49-16 Add/Edit SNMP User Entry Dialog Box

Element	Description
Group Name	Select the SNMP group to which this user belongs. For information on SNMP groups, see Add/Edit SNMP Group Entry Dialog Box, page 49-24.
Security Level	Shows the security level for the selected group: • NoAuth—No Authentication and No Privacy, which means that no security is applied to messages. • Auth—Authentication but No Privacy, which means that messages are authenticated. • Priv—Authentication and Privacy, which means that messages are authenticated and encrypted.
User Name	Enter the name of the SNMP user. Usernames must be 32 characters or less and must be unique for the SNMP server group selected.
Engine ID (SNMP version v3 only)	The SNMP EngineID identifier used for authentication in v3. You can enter comma separated multiple Engine IDs. The Engine ID identifier must be valid, and each Engine Id must be within the range of 1 to 257 characters. **Note** • If you configure EngineID for an SNMP user with MD5 algorithm, the EngineID must be a valid one. If the EngineID is not valid, the preview config would fail with an error "failed to generate raw config". For example, the preview config fails if the EngineID entered is 111. • For an SNMP group with a security level of NoAuth, do not provide an EngineID identifier because on deployment, the ASA will ignore this engine ID and take the default local engine ID. • The following dynamic behaviors of the device cannot be handled in Security Manager: – If you upgrade a failover ASA device from version 8.x or 9.x to version 9.6(2), the device will automatically create multiple SNMP User commands for multiple SNMP Engine IDs. You must copy the Engine ID by retrieving it from the device into this Engine ID text box. For information about retrieving Engine ID from the device see SNMP Page, page 49-17. – If you add or remove an ASA device to or from a failover configuration, you must manually enter the Engine ID because the ASA device automatically removes or creates new SNMP User commands for the existing Engine IDs.

Table 49-16 Add/Edit SNMP User Entry Dialog Box (continued)

Element	Description
Encrypt Password Type	Specify the type of password you want to use: Clear Text or Encrypted. If the password type is Clear Text, Security Manager will encrypt the password when deploying to the device. If the password type is Encrypted, Security Manager will directly deploy the encrypted password. Security Manager will never directly deploy the clear text password to device.
Auth Algorithm Type	Specify the type of authentication you want to use: MD5 or SHA.
Authentication Password Confirm	Enter the password to use for authentication. If you selected Encrypted as the Encrypt Password Type, the password must be formatted as *xx:xx:xx...*, where *xx* are hexadecimal values. **Note** The length of the password will depend on the authentication algorithm selected. For all passwords, the length must be 256 characters or less. If you selected Clear Text as the Encrypt Password Type, repeat the password in the **Confirm** field.
Encryption Type	Specify the type of encryption you want to use: AES128, AES192, AES256, 3DES, DES. **Note** To use AES or 3DES encryption, you must have the appropriate license installed on the device.
Encryption Password Confirm	Enter the password to use for encryption. If you selected Encrypted as the Encrypt Password Type, the password must be formatted as *xx:xx:xx...*, where *xx* are hexadecimal values. For encrypted passwords, the length of the password depends on the encryption type selected. The password sizes are as follows (where each *xx* is one octal): • AES 128 requires 16 octals • AES 192 requires 24 octals • AES 256 requires 32 octals • 3DES requires 32 octals • DES can be any size **Note** For all passwords, the length must be 256 characters or less. If you selected Clear Text as the Encrypt Password Type, repeat the password in the **Confirm** field.

Add/Edit SNMP User List Entry Dialog Box

Beginning with version 4.12, Security Manager enables you to use the Add/Edit SNMP User List Entry dialog box to add a user list containing multiple SNMP users.

Notes

- You cannot delete a user list if the list is used by a particular host group.

- You cannot delete an SNMP user if that user is referred to in a particular user list..

Navigation Path

You can access the Add/Edit SNMP User List Entry dialog box from the SNMP Page, page 49-17.

Field Reference

Table 49-17 Add/Edit SNMP User List Entry Dialog Box

Element	Description
User List Name	Enter the name of the User List. User List names must be 1-33 characters in length.
User Names	Select the user names from the drop-down list.

Related Topics

- Configuring SNMP, page 49-14
- SNMP Trap Configuration Dialog Box, page 49-19
- Add/Edit SNMP Host Access Entry Dialog Box, page 49-22
- Add/Edit SNMP Group Entry Dialog Box, page 49-24

Telnet Page

Use the Telnet page to configure rules that permit only specific hosts or networks to connect to the firewall device using the Telnet protocol.

The rules restrict administrative Telnet access through a firewall device interface to a specific IP address and netmask. Connection attempts that comply with the rules must then be authenticated by a preconfigured AAA server or the Telnet password. You can monitor Telnet sessions using Monitoring > Telnet Sessions.

Note Only five Telnet sessions can be active at the same time in single-context mode. In multiple-context mode on ASAs, there can be only five Telnet sessions active per context, 100 Telnet sessions active per blade. With resource class, the administrator can further tune this parameter.

Related Topics

Navigation Path

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

Related Topics

- Telnet Configuration Dialog Box, page 49-29

Field Reference

Table 49-18 Telnet Page

Element	Description
Timeout	Number of minutes a Telnet session can remain idle before the firewall device closes it. Values can range from 1 to 1440 minutes.
Telnet Access Table	
Interface	Interface that receives Telnet packets from the client.
IP Addresses	The IP address and network mask of each host or network that can access the Telnet console through the specified interface.

Telnet Configuration Dialog Box

Use the Telnet Configuration dialog box to configure Telnet options for an interface.

Navigation Path

You can access the Telnet Configuration dialog box from the Telnet Page, page 49-29.

Field Reference

Table 49-19 Telnet Configuration Dialog Box

Element	Description
Interface Name	Enter or Select an interface that can receive Telnet packets from a client. **Note** Beginning with Cisco Security Manager version 4.17, you can configure BVI interface for Telnet on ASA 9.9.2 devices and above. However, in multi-context, "Transparent" mode security context only supports BVI interface.
IP Addresses/Netmask	Enter or Select the IP address and netmask, separated by a "/", of each host or network permitted to access the firewall device's Telnet console through the specified interface. Use commas to separate multiple entries. **Note** To limit access to a single IP address, use 255.255.255.255 or 32 as the netmask. Do not use the subnetwork mask of the internal network. **Note** Beginning with version 4.13, Cisco Security Manager supports policies—Groups, Hosts, Address Range, and Network for IPv6 devices.