



CHAPTER 8

Configuring Device Properties

This section contains the following topics:

- [Management IP](#)
- [Device Administration](#)
- [Auto Update](#)

Management IP

The **Management IP** window lets you set the management IP address for the security appliance or for a context in transparent firewall mode. A transparent firewall does not participate in IP routing. The only IP configuration required for the security appliance is to set the management IP address. The exception is that you can set the IP address for the Management 0/0 management-only interface, which does not pass through traffic. See the [Configuring the Interfaces](#) to set the IP address for Management 0/0.

This address is required because the security appliance uses this address as the source address for traffic originating on the security appliance, such as system messages or communications with AAA servers. You can also use this address for remote management access.

Fields

- **Management IP Address**—Sets the management IP address.
- **Subnet Mask**—Sets the subnet mask.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| — | • | • | • | — |

Device Administration

Under **Device Administration**, you can set basic parameters for the security appliance. This section contains the following topics:

- [Banner](#)
- [Boot Image/Configuration](#)
- [Console](#)
- [Clock](#)
- [Device](#)
- [FTP Mode](#)
- [ICMP Rules](#)
- [Management Access](#)
- [NTP](#)
- [Password](#)
- [Secure Copy](#)
- [SNMP](#)
- [TFTP Server](#)
- [User Accounts](#)

Banner

The **Banner** panel lets you configure message of the day, login, and session banners.

To create a banner, enter text into the appropriate box. Spaces in the text are preserved, however, tabs can be entered in the ASDM interface but cannot be entered through the command line interface. The tokens \$(domain) and \$(hostname) are replaced with the host name and domain name of the security appliance.

Use the \$(hostname) and \$(domain) tokens to echo the hostname and domain name specified in a particular context. Use the \$(system) token to echo a banner configured in the system space in a particular context.

Multiple lines in a banner are handled by entering a line of text for each line you wish to add. Each line is then appended to the end of the existing banner. If the text is empty, then a carriage return (CR) will be added to the banner. There is no limit on the length of a banner other than RAM and Flash memory limits. You can only use ASCII characters, including new line (the Enter key, which counts as two characters).

When accessing the security appliance through Telnet or SSH, the session closes if there is not enough system memory available to process the banner messages or if a TCP write error occurs when attempting to display the banner messages.

To replace a banner, change the contents of the appropriate box and click **Apply**. To clear a banner, clear the contents of the appropriate box and click **Apply**.

Although the banner command is not available in the System Context through the ASDM panel, it can be configured with **Tools > Command Line Interface**.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

Boot Image/Configuration

Boot Image/Configuration lets you choose which image file the security appliance will boot from, as well as which configuration file it will use at startup.

You can specify up to four local binary image files for use as the startup image, and one image located on a TFTP server for the device to boot from. If you specify an image located on a TFTP server, it must be first in the list. In the event the device cannot reach the tftp server to load the image from, it will attempt to load the next image file in the list located in Flash.

If you do not specify any boot variable, the first valid image on internal flash will be chosen to boot the system.

Fields**Boot Configuration**

- **Boot Order**—Displays the order in which binary image files will be used to boot.
- **Boot Image Location**—Displays the physical location and path of the boot file.
- **Boot Config File Path**—Displays the location of the configuration file.
- **Add**—Lets you add a flash or tftp boot image entry to be used in the boot process.
- **Edit**—Lets you edit a flash or tftp boot image entry.
- **Delete**—Deletes the selected flash or tftp boot image entry.
- **Move Up**—Moves the selected flash or tftp boot image entry up in the boot order.
- **Move Down**—Moves the selected flash or tftp boot image entry down in the boot order.
- **Browse Flash**—Lets you specify the location of a boot image or configuration file.

ASDM Image Configuration

- **ASDM Image File Path**—Displays the location of the configuration file the device will use at startup.
- **Browse Flash**—Lets you specify the location of a boot image or configuration file.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | • |

Add Boot Image

To add a boot image entry to the boot order list, click **Add** on the **Boot Image/Configuration** panel.

You can select a Flash or TFTP image to add a boot image to the boot order list.

Either type the path of the image, or click **Browse Flash** to specify the image location. You must type the path of the image location if you are using TFTP.

Fields

- **Flash Image**—Select to add a boot image located in the flash file system.
 - **Path**—Specify the path of the boot image in the flash file system.
- **TFTP Image**—Select to add a boot image located on a TFTP server.
 - **[Path]**—Enter the path on the TFTP server of the boot image file, including the IP address of the server.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | • |

Clock

The **Clock** panel lets you manually set the date and time for the security appliance. The time displays in the status bar at the bottom of the main ASDM window.

In multiple context mode, set the time in the system configuration only.

To dynamically set the time using an NTP server, see the **NTP** panel; time derived from an NTP server overrides any time set manually in the **Clock** panel.

Fields

- **Time Zone**—Sets the time zone as GMT plus or minus the appropriate number of hours. If you select the Eastern Time, Central Time, Mountain Time, or Pacific Time zone, then the time adjusts automatically for daylight saving time, from 2:00 a.m. on the first Sunday in April to 2:00 a.m. on the last Sunday in October.



Note Changing the time zone on the security appliance may drop the connection to intelligent SSMs.

- **Date**—Sets the date. Select the date and year from the lists, and then click the day on the calendar.
- **Time**—Sets the time on a 24-hour clock.
 - **hh, mm, and ss** boxes—Sets the hour, minutes, and seconds.
- **Update Display Time**—Updates the time shown at the bottom right corner of the ASDM window. The current time updates automatically every ten seconds.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | • |

Console

The **Console** panel lets you specify a time period in minutes for the management console to remain active. When it reaches the time limit you specify here, the console automatically shuts down.

Type the time period in the **Console Timeout** text box. To specify unlimited, enter 0. The default value is 0.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | • |

Device

The **Device** panel lets you set the hostname and domain name for the security appliance.

The hostname appears as the command line prompt, and if you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands. The hostname is also used in system messages.

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts. The hostname that you optionally set within a context does not appear in the command line, can be used for a banner.

The security appliance appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com,” and specify a syslog server by the unqualified name of “jupiter,” then the security appliance qualifies the name to “jupiter.example.com.”

Fields

- **Platform Host Name**—Sets the hostname. The default hostname depends on your platform.
- **Domain Name**—Sets the domain name. The default domain name is default.domain.invalid.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | • |

FTP Mode

The **FTP Mode** panel configures FTP mode as active or passive. The security appliance can use FTP to upload or download image files or configuration files to or from an FTP server. In passive FTP, the client initiates both the control connection and the data connection. The server, which is the recipient of the data connection in passive mode, responds with the port number to which it is listening for the specific connection.

Fields

- **Specify FTP mode as passive**—Configures FTP mode as active or passive.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | • |

ICMP Rules

The **ICMP Rules** panel provides a table that lists the ICMP rules, which specify the addresses of all the hosts or networks that are allowed or denied ICMP access to the security appliance. You can use this table to add or change the hosts or networks that are allowed or prevented from sending ICMP messages to the security appliance.

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



Note

Use the **Security Policy** panel to configure access rules for ICMP traffic that is routed *through* the security appliance for destinations on a protected interface.

It is recommended that permission is always granted for the ICMP unreachable message type (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, then the security appliance 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 ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the security appliance discards the ICMP packet and generates a syslog message. An exception is when an ICMP control list is not configured; in that case, a **permit** statement is assumed.

Fields

- **Interface**—Lists the interface on the security appliance from which ICMP access is allowed.
- **Action**—Displays whether ICMP messages are permitted or not allowed from the specified network or host.
- **IP Address**—Lists the IP address of the network or host that is allowed or denied access.
- **Mask**—Lists the network mask associated with the network or host that is allowed access.
- **ICMP Type**—Lists the type of ICMP message to which the rule applies. [Table 8-1](#) lists the supported ICMP type values.
- **Add**—Displays the **Add ICMP Rule** dialog box for adding a new ICMP rule to the end of the table.
- **Insert**—Adds an ICMP rule before or after the currently selected rule.
- **Edit**—Displays the **Edit ICMP Rule** dialog box for editing the selected host or network.
- **Delete**—Deletes the selected host or network.
- **ICMP Unreachable Message Limits**—Adds rate limits and burst size message limits to ICMP messages.

Table 8-1 ICMP Type Literals

| ICMP Type | Literal |
|-----------|---------------|
| 0 | echo-reply |
| 3 | unreachable |
| 4 | source-quench |
| 5 | redirect |

Table 8-1 ICMP Type Literals (continued)

| ICMP Type | Literal |
|-----------|----------------------|
| 6 | alternate-address |
| 8 | echo |
| 9 | router-advertisement |
| 10 | router-solicitation |
| 11 | time-exceeded |
| 12 | parameter-problem |
| 13 | timestamp-request |
| 14 | timestamp-reply |
| 15 | information-request |
| 16 | information-reply |
| 17 | mask-request |
| 18 | mask-reply |
| 31 | conversion-error |
| 32 | mobile-redirect |

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

Add/Edit ICMP Rule

The **Add/Edit ICMP Rule** dialog box lets you add or modify an ICMP rule, which specifies the addresses of all the hosts or networks that are allowed or denied ICMP access to the security appliance.

Fields

- **ICMP Type**—Specifies the type of ICMP message to which the rule applies. [Table 8-2](#) lists the supported ICMP type values.
- **Interface**—Identifies the interface on the security appliance from which ICMP access is allowed.
- **IP Address**—Specifies the IP address of the network or host that is allowed or denied access.
- **Any Address**—Applies the action to all addresses received on the specified interface.
- **Mask**—Specifies the network mask associated with the network or host that is allowed access.
- **Action**—Specifies whether ICMP messages are permitted or not from the specified network or host.
 - **Permit**—Causes ICMP messages from the specified host or network and interface to be allowed.

- **Deny**—Causes ICMP messages from the specified host or network and interface to be dropped.
- **ICMP Unreachable Message Limits**—Adds rate limits and burst size message limits to ICMP messages.

Table 8-2 ICMP Type Literals

| ICMP Type | Literal |
|-----------|----------------------|
| 0 | echo-reply |
| 3 | unreachable |
| 4 | source-quench |
| 5 | redirect |
| 6 | alternate-address |
| 8 | echo |
| 9 | router-advertisement |
| 10 | router-solicitation |
| 11 | time-exceeded |
| 12 | parameter-problem |
| 13 | timestamp-request |
| 14 | timestamp-reply |
| 15 | information-request |
| 16 | information-reply |
| 17 | mask-request |
| 18 | mask-reply |
| 31 | conversion-error |
| 32 | mobile-redirect |

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

Management Access

The **Management Access** panel lets you enable or disable management access on a high-security interface and thus lets you perform management functions on the security appliance. With management access enabled, you can run ASDM on an internal interface with a fixed IP address over an IPSec VPN tunnel. Use this feature if VPN is configured on the security appliance and the external interface is using a dynamically assigned IP address. For example, this feature is helpful for accessing and managing the security appliance securely from home using the VPN client.

Fields

- **Management Access Interface**—Lets you specify the interface to use for managing the security appliance. **None** disables management access and is the default. To enable management access, select the interface with the highest security, which will be an inside interface. You can enable management access on only one interface at a time.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|--------------------|------------------|-----------------|---------------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | — | • | — | — |

NTP

The **NTP** panel lets you define NTP servers to dynamically set the time on the security appliance. The time displays in the status bar at the bottom of the main ASDM window.

Time derived from an NTP server overrides any time set manually in the **Clock** panel.

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp. You can configure multiple NTP servers. The security appliance chooses the server with the lowest stratum—a measure of how reliable the data is.

Fields

- **NTP Server List**—Shows defined NTP servers.
 - **IP Address**—Shows the NTP server IP address.
 - **Interface**—Specifies the outgoing interface for NTP packets, if configured. The system does not include any interfaces, so it uses the admin context interfaces. If the interface is blank, then the security appliance uses the default admin context interface according to the routing table.
 - **Preferred?**—Shows whether this NTP server is a preferred server, Yes or No. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If servers are of similar accuracy, then the preferred server is used. However, if a server is significantly more accurate than the preferred one, the security appliance uses the more accurate one. For example, the security appliance uses a more accurate server over a less accurate server that is preferred.
 - **Key Number**—Shows the authentication key ID number.
 - **Trusted Key?**—Shows if the key is a trusted key, Yes or No. The key must be trusted for authentication to work.
- **Enable NTP Authentication**—Enables authentication for all servers.
- **Add**—Adds an NTP server.
- **Edit**—Edits an NTP server.
- **Delete**—Deletes and NTP server.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | • |

Add/Edit NTP Server Configuration

The **Add/Edit NTP Server Configuration** dialog box lets you add or edit an NTP server.

Fields

- **IP Address**—Sets the NTP server IP address.
- **Preferred**—Sets this server as a preferred server. NTP uses an algorithm to determine which server is the most accurate and synchronizes to that one. If servers are of similar accuracy, then the preferred server is used. However, if a server is significantly more accurate than the preferred one, the security appliance uses the more accurate one. For example, the security appliance uses a more accurate server over a less accurate server that is preferred.
- **Interface**—Sets the outgoing interface for NTP packets, if you want to override the default interface according to the routing table. The system does not include any interfaces, so it uses the admin context interfaces. If you intend to change the admin context (thus changing the available interfaces), you should choose **None** (the default interface) for stability.
- **Authentication Key**—Sets the authentication key attributes if you want to use MD5 authentication for communicating with the NTP server.
 - **Key Number**—Sets the key ID for this authentication key. The NTP server packets must also use this key ID. If you previously configured a key ID for another server, you can select it in the list; otherwise, type a number between 1 and 4294967295.
 - **Trusted**—Sets this key as a trusted key. You must select this box for authentication to work.
 - **Key Value**—Sets the authentication key as a string up to 32 characters in length.
 - **Reenter Key Value**—Validates the key by ensuring that you enter the key correctly two times.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | • |

Password

The **Password** panel lets you set the login password and the enable password.

The login password lets you access EXEC mode if you connect to the security appliance using a Telnet or SSH session. (If you configure user authentication for Telnet or SSH access, then each user has their own password, and this login password is not used; see the [AAA Access](#) panel.)

The enable password lets you access privileged EXEC mode after you log in. Also, this password is used to access ASDM as the default user, which is blank. The default user shows as “enable_15” in the [User Accounts](#) panel. (If you configure user authentication for enable access, then each user has their own password, and this enable password is not used; see the [AAA Access](#) panel. In addition, you can configure authentication for HTTP/ASDM access.)

Fields

- **Enable Password**—Sets the enable password. By default, it is blank.
 - **Change the privileged mode password**—Lets you change the enable password.
 - **Old Password**—Enter the old password.
 - **New Password**—Enter the new password.
 - **Confirm New Password**—Confirm the new password.
- **Telnet Password**—Sets the login password. By default, it is “cisco.” Although this group box is called Telnet Password, this password applies to Telnet and SSH access.
 - **Change the password to access the *platform console***—Lets you change the login password.
 - **Old Password**—Enter the old password.
 - **New Password**—Enter the new password.
 - **Confirm New Password**—Confirm the new password.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

Secure Copy

The **Secure Copy** panel lets you enable the secure copy server on the security appliance. Only clients that are allowed to access the security appliance using SSH can establish a secure copy connection.

Limitations

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.

Fields

- **Enable Secure Copy Server**—Select this check box to enable the secure copy server on the security appliance.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | • |

SMTP

The **SMTP** panel lets you enable or disable the SMTP client for notification by email that a significant event has transpired. Here you can add an IP address of an SMTP server and optionally, the IP address of a backup server. ASDM does not check to make sure the IP address is valid, so it is important to type the address correctly.

You can configure what email addresses will receive alerts in **Configuration > Properties > Logging > Email Setup**.

Fields

- **Remote SMTP Server**—Lets you configure the primary and secondary SMTP servers.
- **Primary Server IP Address**—Enter the IP address of the SMTP server.
- **Secondary Server IP Address (Optional)**—Optionally, you can enter the IP address of a secondary SMTP server.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

SNMP

The **SNMP** panel lets you configure the security appliance for monitoring by Simple Network Management Protocol (SNMP) management stations.

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 the security appliance.

SNMP Terminology

- **Management station**—Network management stations running on PCs or workstations, use the SNMP protocol to administer standardized databases residing on the device being managed. Management stations can also receive messages about events, such as hardware failures, which require attention.
- **Agent**—In the context of SNMP, the management station is a *client* and an SNMP agent running on the security appliance is a *server*.
- **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.
- **MIB**—The agent maintains standardized data structures called Management Information Databases, or MIBs which are compiled into management stations. MIBs collect information, such as packet, connection, and error counters, buffer usage, and failover status. MIBs are defined for specific products, in addition to MIBs 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.
- **Trap**—The agent also monitors alarm conditions. When an alarm condition defined in a trap occurs, such as a link up, link down, or syslog event, the agent sends notification, also known as SNMP trap, to the designated management station immediately.

SNMP

For Cisco MIB files and OIDs, refer to:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>. OIDs may be downloaded at this URL: <ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz>.

MIB Support

The security appliance provides the following SNMP MIB support:



Note

The security appliance does not support browsing of the Cisco syslog MIB.

- You can browse the System and Interface groups of MIB-II. Browsing an MIB is different from sending traps. Browsing means doing an snmpget or snmpwalk of the MIB tree from the management station to determine values.
- The Cisco MIB and Cisco Memory Pool MIB are available.
- The security appliance does not support the following in the Cisco MIB:
 - cfwSecurityNotification NOTIFICATION-TYPE
 - cfwContentInspectNotification NOTIFICATION-TYPE
 - cfwConnNotification NOTIFICATION-TYPE
 - cfwAccessNotification NOTIFICATION-TYPE
 - cfwAuthNotification NOTIFICATION-TYPE
 - cfwGenericNotification NOTIFICATION-TYPE

SNMP CPU Utilization

The security appliance supports monitoring CPU utilization through SNMP. This feature allows network administrators to monitor security appliance CPU usage using SNMP management software, such as HP OpenView, for capacity planning.

This functionality is implemented through support for the `cpmCPUTotalTable` of the Cisco Process MIB (CISCO-PROCESS-MIB.my). The other two tables in the MIB, `cpmProcessTable` and `cpmProcessExtTable`, are not supported in this release.

Each row of the `cpmCPUTotalTable` includes the index of each CPU and the following objects:

| MIB object name | Description |
|---------------------------------------|--|
| <code>cpmCPUTotalPhysicalIndex</code> | The value of this object will be zero because the <code>entPhysicalTable</code> of Entity MIB is not supported on the security appliance SNMP agent. |
| <code>cpmCPUTotalIndex</code> | The value of this object will be zero because the <code>entPhysicalTable</code> of Entity MIB is not supported on the security appliance SNMP agent. |
| <code>cpmCPUTotal5sec</code> | Overall CPU busy percentage in the last five-second period. |
| <code>cpmCPUTotal1min</code> | Overall CPU busy percentage in the last one-minute period. |
| <code>cpmCPUTotal5min</code> | Overall CPU busy percentage in the last five-minute period. |



Note

Because all current security appliance hardware platforms support a single CPU, the security appliance returns only one row from `cpmCPUTotalTable` and the index is always 1.

The values of the last three elements are the same as the output from the `show cpu usage` command.

The security appliance does not support the following new MIB objects in the `cpmCPUTotalTable`:

- `cpmCPUTotal5secRev`
- `cpmCPUTotal1minRev`
- `cpmCPUTotal5minRev`

Fields

- **Community string (default)**—Enter the password used by the SNMP management station when sending requests to the security appliance. The SNMP community string is a shared secret among the SNMP management stations and the network nodes being managed. The security appliance uses the password to determine if the incoming SNMP request is valid. The password is a case-sensitive value up to 32 characters in length. Spaces are not permitted. The default is “public.” SNMPv2c allows separate community strings to be set for each management station. If no community string is configured for any management station, the value set here will be used by default.
- **Contact**—Enter the name of the security appliance system administrator. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Security Appliance Location**—Specify the security appliance location. The text is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Listening Port**—Specify the port on which SNMP traffic is sent. The default is 161.
- **Configure Traps**—Lets you configure the events to notify through SNMP traps.

- **SNMP Management Station** box:
 - **Interface**—Displays the security appliance interface name where the SNMP management station resides.
 - **IP Address**—Displays the IP address of an SNMP management station to which the security appliance sends trap events and receive requests or polls.
 - **Community string**—If no community string is specified for a management station, the value set in **Community String (default)** field will be used.
 - **SNMP Version**—Displays the version of SNMP set on the management station.
 - **Poll/Trap**—Displays the method for communicating with this management station, poll only, trap only, or both trap and poll. Polling means that the security appliance waits for a periodic request from the management station. The trap setting sends syslog events when they occur.
 - **UDP Port**—SNMP host UDP port. The default is port 162.
- **Add**—Opens **Add SNMP Host Access Entry** with these fields:
- **Interface Name**—Select the interface on which the management station resides.
- **IP Address**—Specify the IP address of the management station.
- **Server Poll/Trap Specification**—Select **Poll**, **Trap**, or both.
- **UDP Port**—UDP port for the SNMP host. This field allows you to override the default value of 162 for the SNMP host UDP port.
- **Help**—Provides more information.
- **Edit**—Opens the **Edit SNMP Host Access Entry** dialog box with the same fields as Add.
- **Delete**—Deletes the selected item.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

Add/Edit SNMP Host Access Entry

Adding SNMP Management Stations

To add SNMP management stations, perform the following steps:

1. Click **Add** to open the **SNMP Host Access Entry** dialog box.
2. From **Interface Name**, select the interface on which the SNMP management station resides.
3. Enter the IP address of that management station in **IP Address**.
4. Enter the UDP port for the SNMP host. The default is 162.
5. Enter the Community String password for the SNMP host. If no community string is specified for a management station, the value set in **Community String (default)** field in the SNMP Configuration screen will be used.

6. Click to select **Poll**, **Trap**, or both.
7. To return to the previous panel click:
 - **OK**—Accepts changes and returns to the previous panel
 - **Cancel**—Discards changes and returns to the previous panel
 - **Help**—Provides more information

Editing SNMP Management Stations

To edit SNMP management stations, perform the following steps:

1. Select a list item from the SNMP management station table on the **SNMP** panel.
2. Click **Edit** to open **Edit SNMP Host Access Entry**.
3. From **Interface Name**, select the interface on which the SNMP management station resides.
4. Enter the IP address of that management station in **IP Address**.
5. Enter the Community String password for the SNMP host. If no community string is specified for a management station, the value set in **Community String (default)** field in the SNMP Configuration screen will be used.
6. Enter the UDP port for the SNMP host. The default is 162.
7. Click to select **Poll**, **Trap**, or both.
8. Select SNMP version.
9. To return to the previous panel click:
 - **OK**—Accepts changes and returns to the previous panel
 - **Cancel**—Discards changes and returns to the previous panel
 - **Help**—Provides more information

Deleting SNMP Management Stations

To delete an SNMP management station from the table, perform the following steps:

1. Select an item from the SNMP management station table on the **SNMP** panel.
2. Click **Delete**.

Fields

- **Interface name**—Select the interface where the SNMP host resides.
- **IP Address**—Enter the IP address of the SNMP host.
- **UDP Port**—Enter the UDP port on which to send SNMP updates. The default is 162.
- **Community String**—Enter the community string for the SNMP server.
- **SNMP Version**—Select the SNMP version.
- **Server Port/Trap Specification**
 - **Poll**—Select to send poll information. Polling means that the security appliance waits for a periodic request from the management station.
 - **Trap**—Select to send trap information. The trap setting sends syslog events when they occur.
- **OK**—Accepts changes and returns to the previous panel
- **Cancel**—Discards changes and returns to the previous panel

- **Help**—Provides more information

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

SNMP Trap Configuration

Traps

Traps are different than browsing; they are unsolicited “comments” from the managed device to the management station for certain events, such as link up, link down, and syslog event generated.

An SNMP object ID (OID) for the security appliance displays in SNMP event traps sent from the security appliance. The security appliance provides system OID in SNMP event traps & SNMP mib-2.system.sysObjectID.

The SNMP service running on the security appliance performs two different functions:

- Replies to SNMP requests from management stations (also known as SNMP clients).
- Sends traps (event notifications) to management stations or other devices that are registered to receive them from the security appliance.

The security appliance supports 3 types of traps:

- firewall
- generic
- syslog

Configure Traps

Opens **SNMP Trap Configuration** with the following fields:

- **Standard SNMP Traps**—Select standard traps to send:
 - **Authentication**—Enables authentication standard trap.
 - **Cold Start**—Enables cold start standard trap.
 - **Link Up**—Enables link up standard trap.
 - **Link Down**—Enables link down standard trap.
- **Entity MIB Notifications**
 - **FRU Insert**—Enables a trap notification when a Field Replaceable Unit (FRU) has been inserted.
 - **FRU Remove**—Enables a trap notification when a Field Replaceable Unit (FRU) has been removed.
 - **Configuration Change**—Enables a trap notification when there has been a hardware change.
- **IPSec Traps**—Enables IPSec traps.

- **Start**—Enables a trap when IPsec starts.
- **Stop**—Enables a trap when IPsec stops.
- **Remote Access Traps**—Enables remote access traps.
 - **Session threshold exceeded**—Enables a trap when the number of remote access session attempts exceeds the threshold configured.
- **Enable Syslog traps**—Enables sending of syslog messages to SNMP management station.
- **OK**—Accepts changes and returns to the previous panel.
- **Cancel**—Discards changes and returns to the previous panel.
- **Help**—Provides more information.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

TFTP Server

The **TFTP Server** panel lets you configure the security appliance to save its configuration to a file server using TFTP.



Note

This panel does not write the file to the server. Configure the security appliance for using a TFTP server in this panel, then click **File > Save Running Configuration to TFTP Server**.

TFTP Servers and the security appliance

TFTP is a simple client/server file transfer protocol described in RFC783 and RFC1350 Rev. 2. This panel lets you configure the security appliance as a TFTP *client* so that it can transfer a copy of its running configuration file to a TFTP *server* using **File > Save Running Configuration to TFTP Server** or **Tools > Command Line Interface**. In this way, you can back up and propagate configuration files to multiple security appliances.

This panel uses the **configure net** command to specify the IP address of the TFTP server, and the **tftp-server** command to specify the interface and the path/filename on the server where the running configuration file will be written. Once this information is applied to the running configuration, ASDM **File > Save Running Configuration to TFTP Server** uses the **copy** command to execute the file transfer.

The security appliance supports only one TFTP server. The full path to the TFTP server is specified in **Configuration > Properties > Administration > TFTP Server**. Once configured here, you can use a colon (:) to specify the IP address in the CLI **configure net** and **copy** commands. However, any other authentication or configuration of intermediate devices necessary for communication from the security appliance to the TFTP server is done apart from this function.

The **show tftp-server** command lists the **tftp-server** command statements in the current configuration. The **no tftp server** command disables access to the server.

Fields

The **TFTP** panel provides the following fields:

- **Enable**—Click to select and enable these TFTP server settings in the configuration.
- **Interface Name**—Select the name of the security appliance interface which will use these TFTP server settings.
- **IP Address**—Enter the IP address of the TFTP server.
- **Path**—Type in the TFTP server path, beginning with “/” (forward slash) and ending in the file name, to which the running configuration file will be written.

Example TFTP server path: **/tftpboot/security appliance/config3**



Note The path must begin with a forward slash (/).

For More Information

For more information about TFTP, refer to the security appliance Technical Documentation for your version of software.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

User Accounts

The **User Accounts** panel lets you manage the local user database. The local database is used for the following features:

- ASDM per-user access
By default, you can log into ASDM with a blank username and the enable password (see [Password](#)). However, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.



Note Although you can configure HTTP authentication using the local database (see the [Authentication Tab](#)), that functionality is always enabled by default. You should only configure HTTP authentication if you want to use a RADIUS or TACACS+ server for authentication.

- Console authentication (see the [Authentication Tab](#))
- Telnet and SSH authentication (see the [Authentication Tab](#))
- **enable** command authentication (see the [Authentication Tab](#))
This setting is for CLI-access only and does not affect the ASDM login.
- Command authorization (see the [Authorization Tab](#))

If you enable command authorization using the local database, then the security appliance refers to the user privilege level to determine what commands are available. Otherwise, the privilege level is not generally used. By default, all commands are either privilege level 0 or level 15. ASDM allows you to enable three predefined privilege levels, with commands assigned to level 15 (Admin), level 5 (Read Only), and level 3 (Monitor Only). If you use the predefined levels, then assign users to one of these three privilege levels.



Note If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged mode, you should enable command authorization. Without command authorization, users can access privileged mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use RADIUS or TACACS+ authentication for console access so the user will not be able to use the login command, or you can set all local users to level 1 so you can control who can use the system enable password to access privileged mode.

- Network access authentication
- VPN client authentication

You cannot use the local database for network access authorization.

For multiple context mode, you can configure usernames in the system execution space to provide individual logins at the CLI using the **login** command; however, you cannot configure any **aaa** commands that use the local database in the system execution space.



Note

VPN functions are not supported in multimode.

To configure the enable password from this panel (instead of in **Password**), change the password for the enable_15 user. The enable_15 user is always present in this panel, and represents the default username. This method of configuring the enable password is the only method available in ASDM for the system configuration. If you configured other enable level passwords at the CLI (**enable password 10**, for example), then those users are listed as enable_10, etc.

Fields

- **User Name**—Specifies the user name to which these parameters apply.
- **Privilege (Level)**—Specifies the privilege level assigned to that user. The privilege level is used with local command authorization. See the **Authorization Tab** for more information.
- **VPN Group Policy**—Specifies the name of the VPN group policy for this user. Not available in multimode.
- **VPN Group Lock**—Specifies what, if any, group lock policy is in effect for this user. Not available in multimode.
- **Add**—Displays the Add User Account dialog box.
- **Edit**—Displays the Edit User Account dialog box.
- **Delete**—Removes the selected row from the table. There is no confirmation or undo.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|--------------------|------------------|----------------|---------------|
| | | | Multiple | |
| Routed | Transparent | Single | Context | System |
| • | • | • | • | — |

Add/Edit User Account > Identity Tab

Use this tab to specify parameters that identify the user account you want to add or change. The changes appear in the User Accounts table as soon as you click OK.

Fields

- **Username**—Specifies the username for this account.
- **Password**—Specifies the unique password for this user. The minimum password length is 4 characters. The maximum is 32 characters. Entries are case-sensitive. The field displays only asterisks.



Note To protect security, we recommend a password length of at least 8 characters.

- **Confirm Password**—Asks you to re-enter the user password to verify it. The field displays only asterisks.
- **Privilege Level**—Selects the privilege level for this user to use with local command authorization. The range is 0 (lowest) to 15 (highest). See the [Authorization Tab](#) for more information.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|--------------------|------------------|----------------|---------------|
| | | | Multiple | |
| Routed | Transparent | Single | Context | System |
| • | • | • | • | — |

Add/Edit User Account > VPN Policy Tab

Use this tab to specify VPN policies for this user. Check an Inherit check box to let the corresponding setting take its value from the group policy.

Fields

- **Group Policy**—Lists the available group policies.
- **Tunneling Protocols**—Specifies what tunneling protocols that this user can use, or whether to inherit the value from the group policy. Check the desired **Tunneling Protocols** check boxes to select the VPN tunneling protocols that this user can use. Users can use only the selected protocols. The choices are as follows:

IPSec—IP Security Protocol. IPSec provides the most complete architecture for VPN tunnels, and it is perceived as the most secure protocol. Both LAN-to-LAN (peer-to-peer) connections and client-to-LAN connections can use IPSec.

WebVPN—VPN via SSL/TLS. Uses a web browser to establish a secure remote-access tunnel to a VPN Concentrator; requires neither a software nor hardware client. WebVPN can provide easy access to a broad range of enterprise resources, including corporate websites, web-enabled applications, NT/AD file share (web-enabled), e-mail, and other TCP-based applications from almost any computer that can reach HTTPS Internet sites.

L2TP over IPSec—Allows remote users with VPN clients provided with several common PC and mobile PC operating systems to establish secure connections over the public IP network to the security appliance and private corporate networks.



Note If no protocol is selected, an error message appears.

- **Filter**—Specifies what filter to use, or whether to inherit the value from the group policy. Filters consist of rules that determine whether to allow or reject tunneled data packets coming through the security appliance, based on criteria such as source address, destination address, and protocol. To configure filters and rules, see the Configuration > VPN > VPN General > Group Policy panel.
- **Manage**—Displays the ACL Manager panel, on which you can add, edit, and delete Access Control Lists (ACLs) and Extended Access Control Lists (ACEs).
- **Tunnel Group Lock**—Specifies whether to inherit the tunnel group lock or to use the selected tunnel group lock, if any. Selecting a specific lock restricts users to remote access through this group only. Tunnel Group Lock restricts users by checking if the group configured in the VPN client is the same as the user's assigned group. If it is not, the security appliance prevents the user from connecting. If the Inherit check box is not selected, the default value is --None--.
- **Store Password on Client System**—Specifies whether to inherit this setting from the group. Deselecting the Inherit check box activates the Yes and No radio buttons. Selecting Yes stores the login password on the client system (potentially a less-secure option). Selecting No (the default) requires the user to enter the password with each connection. For maximum security, we recommend that you *not do allow* password storage. This parameter has no bearing on interactive hardware client authentication or individual user authentication for a VPN 3002.
- **Connection Settings**—Specifies the connection settings parameters.
 - **Access Hours**—If the Inherit check box is not selected, you can select the name of an existing access hours policy, if any, applied to this user or create a new access hours policy. The default value is Inherit, or, if the Inherit check box is not selected, the default value is --Unrestricted--.
 - **New**—Opens the Add Time Range dialog box, on which you can specify a new set of access hours.
 - **Simultaneous Logins**—If the Inherit check box is not selected, this parameter specifies the maximum number of simultaneous logins allowed for this user. The default value is 3. The minimum value is 0, which disables login and prevents user access.



Note While there is no maximum limit, allowing several simultaneous connections could compromise security and affect performance.

- **Maximum Connect Time**—If the Inherit check box is not selected, this parameter specifies the maximum user connection time in minutes. At the end of this time, the system terminates the connection. The minimum is 1 minute, and the maximum is 2147483647 minutes (over 4000 years). To allow unlimited connection time, select the Unlimited check box (the default).
- **Idle Timeout**—If the Inherit check box is not selected, this parameter specifies this user's idle timeout period in minutes. If there is no communication activity on the user's connection in this period, the system terminates the connection. The minimum time is 1 minute, and the maximum time is 10080 minutes. This value does not apply to WebVPN users.
- **Dedicated IP Address (Optional)**—
 - **IP Address** box—Specifies the optional Dedicated IP address.
 - **Subnet Mask** list—Specifies the subnet mask for the Dedicated IP address.

Check the **Group Lock** check box to restrict users to remote access through this group only. Group Lock restricts users by checking if the group configured in the VPN client is the same as the user's assigned group. If it is not, the VPN Concentrator prevents the user from connecting.

If this box is unchecked (the default), the system authenticates a user without regard to the user's assigned group.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

Add/Edit User Account > WebVPN Tab

The **Add** or **Edit User Account** panel, **WebVPN** tab, displays six tabs that let you configure WebVPN attributes for users.

Fields

- **Inherit**—Indicates that the corresponding setting takes its value from the default group policy, rather than from the explicit specifications that follow.
- **Functions**—Configures the features available to WebVPN users.
 - **Enable URL entry**—Places the URL entry box on the home page. If this feature is enabled, users can enter web addresses in the URL entry box, and use WebVPN to access those websites.

Using WebVPN does not ensure that communication with every site is secure. WebVPN ensures the security of data transmission between the remote user's PC or workstation and the security appliance on the corporate network. If a user then accesses a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate security appliance to the destination web server is not secured.

In a WebVPN connection, the security appliance acts as a proxy between the end user's web browser and target web servers. When a WebVPN user connects to an SSL-enabled web server, the security appliance establishes a secure connection and validates the server's SSL certificate. The end user's browser never receives the presented certificate, so therefore cannot examine and validate the certificate. The current implementation of WebVPN does not permit

communication with sites that present expired certificates. Neither does the security appliance perform trusted CA certificate validation. Therefore, WebVPN users cannot analyze the certificate an SSL-enabled web-server presents before communicating with it.

To limit Internet access for WebVPN users, deselect the Enable URL Entry field. This prevents WebVPN users from surfing the Web during a WebVPN connection.

- **Enable file server access**—Enables Windows file access (SMB/CIFS files only) through HTTPS. When this box is checked, users can access Windows files on the network. If you enable only this parameter for WebVPN file sharing, users can access only servers that you configure in Servers and URLs group box. To let users access servers directly or to browse servers on the network, see the Enable file server entry and Enable file server browsing parameters.

Users can download, edit, delete, rename, and move files. They can also add files and folders.

Shares must also be configured for user access on the applicable Windows servers. Users might have to be authenticated before accessing files, depending on network requirements.

File access, server/domain access, and browsing require that you configure a WINS server or a master browser, typically on the same network as the security appliance, or reachable from that network. The WINS server or master browser provides the security appliance with an list of the resources on the network. You cannot use a DNS server instead.



Note **Note** File access is not supported in an Active Native Directory environment when used with Dynamic DNS. It is supported if used with a WINS server.

- **Enable file server entry**—Places the file server entry box on the portal page. File server access must be enabled.

With this box selected, users can enter pathnames to Windows files directly. They can download, edit, delete, rename, and move files. They can also add files and folders. Again, shares must also be configured for user access on the applicable Windows servers. Users might have to be authenticated before accessing files, depending on network requirements.

- **Enable file server browsing**—Lets users browse the Windows network for domains/workgroups, servers and shares. File server access must be enabled.

With this box checked, users can select domains and workgroups, and can browse servers and shares within those domains. Shares must also be configured for user access on the applicable Windows servers. Users may need to be authenticated before accessing servers, according to network requirements.

- **Enable port forwarding**—WebVPN Port Forwarding provides access for remote users in the group to client/server applications that communicate over known, fixed TCP/IP ports. Remote users can use client applications that are installed on their local PC and securely access a remote server that supports that application. Cisco has tested the following applications: Windows Terminal Services, Telnet, Secure FTP (FTP over SSH), Perforce, Outlook Express, and Lotus Notes. Other TCP-based applications may also work, but Cisco has not tested them.



Note Port Forwarding does not work with some SSL/TLS versions.

With this box checked users can access client/server applications by mapping TCP ports on the local and remote systems.

**Note**

When users authenticate using digital certificates, the TCP Port Forwarding JAVA applet does not work. JAVA cannot access the web browser's keystore; therefore JAVA cannot use the certificates that the browser uses for user authentication, and the application cannot start. Do not use digital certificates to authenticate WebVPN users if you want them to be able to access applications.

- **Enable Outlook/Exchange proxy**—Enables the use of the Outlook/Exchange e-mail proxy.
- **Apply Web-type ACL**—Applies the WebVPN Access Control List defined for the users of this group.
- **Enable HTTP Proxy**—Enables the forwarding of an HTTP applet proxy to the client. The proxy is useful for technologies that interfere with proper mangling, such as Java, ActiveX, and Flash. It bypasses mangling while ensuring the continued use of the security appliance. The forwarded proxy modifies the browser's old proxy configuration automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser it supports is Microsoft Internet Explorer.
- **Content Filtering**—Blocks or removes the parts of websites that use Java or Active X, scripts, display images, and deliver cookies. By default, these parameters are disabled, which means that no filtering occurs.
 - **Filter Java/ActiveX**—Removes <applet>, <embed> and <object> tags from HTML.
 - **Filter scripts**—Removes <script> tags from HTML.
 - **Filter images**—Removes tags from HTML. Removing images dramatically speeds the delivery of web pages.
 - **Filter cookies from images**—Removes cookies that are delivered with images. This may preserve user privacy, because advertisers use cookies to track visitors.
- **Homepage**—Configures what, if any, home page to use.
 - **Specify URL**—Indicates whether the subsequent fields specify the protocol, either http or https, and the URL of the Web page to use as the home page.
 - **Protocol**—Specifies whether to use http or https as the connection protocol for the home page.
 - **://**—Specifies the URL of the Web page to use as the home page.
 - **Use none**—Specifies that no home page is configured.
- **Port Forwarding**—Configures port forwarding parameters.
 - **Port Forwarding List**—Specifies whether to inherit the port forwarding list from the default group policy, select one from the list, or create a new port forwarding list.
 - **New**—Displays a new panel on which you can add a new port forwarding list. See the description of the Add/Edit Port Forwarding List panel.
 - **Applet Name**—Specifies whether to inherit the applet name or to use the name specified in the box. Specify this name to identify port forwarding to end users. The name you configure displays in the end user interface as a hotlink. When users click this link, a Java applet opens a window that displays a table that lists and provides access to port forwarding applications that you configure for these users. The default applet name is Application Access.
- **Other**—Configures servers and URL lists and the Web-type ACL ID.
 - **Servers and URL Lists**—Specifies whether to inherit the list of Servers and URLs, to select and existing list, or to create a new list.

- **New**—Displays a new panel on which you can add a new port forwarding list.
- **Web-Type ACL ID**—Specifies the identifier of the Web-Type ACL to use.
- **SSL VPN Client tab**—lets you configure the security appliance to download SSL VPN clients (SVCs) to remote computer.

SVC is a VPN tunneling technology that gives remote users the benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers. The SVC uses the SSL encryption that is already present on the remote computer as well as the WebVPN login and authentication of the security appliance.

To establish an SVC session, the remote user enters the IP address of a WebVPN interface of the security appliance in the browser, and the browser connects to that interface and displays the WebVPN login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as *requiring* the SVC, the security appliance downloads the SVC to the remote computer. If the security appliance identifies the user as having the *option* to use the SVC, the security appliance downloads the SVC to the remote computer while presenting a link on the user screen to skip the SVC installation.

After downloading, the SVC installs and configures itself, and then the SVC either remains or uninstalls itself (depending on the configuration) from the remote computer when the connection terminates.

The security appliance might have several unique SVC images residing in cache memory for different remote computer operating systems. When the user attempts to connect, the security appliance can consecutively download portions of these images to the remote computer until the image and operating system match, at which point it downloads the entire SVC. You can order the SVC images to minimize connection setup time, with the first image downloaded representing the most commonly-encountered remote computer operating system.

- **Inherit**—Indicates that the corresponding setting takes its value from the default group policy, rather than from the explicit specifications that follow.
- **Keep Installer on Client System**—Enables permanent SVC installation and disables the automatic uninstalling feature of the SVC. The SVC remains installed on the remote computer for subsequent SVC connections, reducing the SVC connection time for the remote user.
- **Keepalive Messages**—Adjusts the frequency of keepalive messages, in the range of 15 to 600 seconds. The default is keepalive messages are disabled.

You can adjust the frequency of keepalive messages to ensure that an SVC connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle. Adjusting the frequency also ensures that the SVC does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

- **Compression**—Enables compression on the SVC connection. By default, compression is enabled.

SVC compression increases the communications performance between the security appliance and the SVC by reducing the size of the packets being transferred.

- **Rekey Negotiation Settings** group box—When the security appliance and the SVC perform a rekey, they renegotiate the crypto keys and initialization vectors, increasing the security of the connection.

Renegotiation Interval specifies the number of minutes from the start of the session until the rekey takes place, from 1 to 10080 (1 week).

Renegotiation Method specifies whether the SVC establishes a new tunnel during SVC rekey. If you check *none*, SVC rekey is disabled. If you check *ssl*, SSL renegotiation takes place during SVC rekey.

- **Dead Peer Detection**—Dead Peer Detection (DPD) ensures that the security appliance (gateway) or the SVC can quickly detect a condition where the peer is not responding, and the connection has failed.

Gateway Side Detection enables DPD performed by the security appliance (gateway) and specifies the frequency, from 30 to 3600 seconds, with which the security appliance performs DPD. If you check *disable*, DPD performed by the security appliance is disabled.

Client Side Detection enables DPD performed by the SVC (client), and specifies the frequency, from 30 to 3600 seconds, with which the SVC performs DPD. If you check *disable*, DPD performed by the SVC is disabled

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | • | — |

Auto Update

The Auto Update pane lets you configure the security appliance to be managed remotely from servers that supports the Auto Update specification. Auto Update lets you apply configuration changes to the security appliance and receive software updates from remote locations.

Auto Update is useful in solving many of the challenges facing administrators for security appliance management:

- Overcomes dynamic addressing and NAT challenges.
- Gives ability to commit configuration changes in one atomic action.
- Provides a reliable method for updating software.
- Leverages well understood methods for high scalability.
- Open interface gives developers tremendous flexibility.
- Simplifies security solutions for Service Provider environments.
- High reliability, rich security/management features, broad support by many products.

Introduction to Auto Update

The Auto Update specification provides the infrastructure necessary for remote management applications to download security appliance configurations, software images, and to perform basic monitoring from a centralized location or multiple locations.

The Auto Update specification allows the Auto Update server to either push configuration information and send requests for information to the security appliance, or to pull configuration information by causing the security appliance to periodically poll the Auto Update server. The Auto Update server can also send a command to the security appliance to send an immediate polling request at any time. Communication between the Auto Update server and the security appliance requires a communications path and local CLI configuration on each security appliance.

The Auto Update feature on the security appliance can be used with Cisco security products, as well as products from third-party companies that want to manage the security appliance.

Important Notes

- If the security appliance configuration is updated from an Auto Update server, ASDM is not notified. You must choose **Refresh** or **File > Refresh ASDM with the Running Configuration on the Device** to get the latest configuration, and any changes to the configuration made in ASDM will be lost.
- If HTTPS is chosen as the protocol to communicate with the Auto Update server, the security appliance will use SSL. This requires the security appliance to have a DES or 3DES license.

Fields

The Auto Update pane consists of an Auto Update Servers table and two areas: the Timeout area, and the Polling area.

The Auto Update Servers table lets you view the parameters of previously-configured Auto Update servers. The security appliance polls the server listed at the top of the table first. You can change the position of the servers in the table with the Move Up and Move Down buttons. The Auto Update Servers table contains the following columns:

- **Server**—The name or IP address of the Auto Update server.
- **User Name**—The user name used to access the Auto Update server.
- **Interface**—The interface used when sending requests to the Auto Update server.
- **Verify Certificate**—Indicates whether the security appliance checks the certificate returned by the Auto Update server against the Certification Authority (CA) root certificates. This requires that the Auto Update server and the security appliance use the same CA.

Double-clicking any of the rows in the Auto Update Server table opens the Edit Auto Update Server dialog, in which you can modify the Auto Update server parameters. These changes are immediately reflected in the table, but you must click Apply to save them to the configuration.

The Timeout area lets you set the amount of time the security appliance waits for the Auto Update server to timeout. The Timeout area contains the following fields:

- **Enable Timeout Period**—Check to enable the security appliance to timeout if no response is received from the Auto Update server.
- **Timeout Period (Minutes)**—Enter the number of minutes the security appliance will wait to timeout if no response is received from the Auto Update server.

The Polling area lets you configure how often the security appliance will poll for information from the Auto Update server. The Polling area contains the following fields:

- **Polling Period (minutes)**—The number of minutes the security appliance will wait to poll the Auto Update server for new information.
- **Poll on Specified Days**—Allows you to specify a polling schedule.
- **Set Polling Schedule**—Displays the Set Polling Schedule dialog where you can configure the days and time-of-day to poll the Auto Update server.

- **Retry Period (minutes)**—The number of minutes the security appliance will wait to poll the Auto Update server for new information if the attempt to poll the server fails.
- **Retry Count**—The number of times the security appliance will attempt to retry to poll the Auto Update server for new information.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | — |

Set Polling Schedule

The Set Polling Schedule dialog lets you configure specific days, and the time-of-day for the security appliance to poll the Auto Update server.

Fields

The Set Polling Schedule dialog contains the following fields:

Days of the Week—Check the days of the week that you want the security appliance to poll the Auto Update server.

The Daily Update Window group lets you configure the time of day when you want the security appliance to poll the Auto Update server, and contains the following fields:

- **Start Time**—Enter the hour and minute to begin the Auto Update poll.
- **Enable Randomize**—Check to enable the security appliance to randomly choose a time to poll the Auto Update server.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | — |

Add/Edit Auto Update Server

The Edit Auto Update Server dialog contains the following fields:

- **URL**—The protocol the Auto Update server uses to communicate with the security appliance, either http or https, and the path to the Auto Update server.
- **Interface**—The interface to use when sending requests to the Auto Update server.

- **Verify Certificate**—Select to enable the security appliance to verify the certificate returned by the Auto Update server against the Certification Authority (CA) root certificates. This requires that the Auto Update server and the security appliance use the same CA.

The User area contains the following fields:

- **User Name (Optional)**—Enter the user name needed to access the Auto Update server.
- **Password**—Enter the user password for the Auto Update server.
- **Confirm Password**—Reenter the user password for the Auto Update server.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | — |

Advanced Auto Update Settings

Fields

- **Use Device ID to uniquely identify the ASA**—Enables authentication using a Device ID. The Device ID is used to uniquely identify the security appliance to the Auto Update server.
- **Device ID**—Type of Device ID to use.
 - **Hostname**—The name of the host.
 - **Serial Number**—Device serial number.
 - **IP Address on interface**—The IP address of the selected interface, used to uniquely identify the security appliance to the Auto Update server.
 - **MAC Address on interface**—The MAC address of the selected interface, used to uniquely identify the security appliance to the Auto Update server.
 - **User-defined value**—A unique user ID.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | — |

Client Update

The Client Update pane lets you configure the parameters of Auto Update clients associated with the security appliance when it is configured as an Auto Update server.

As an Auto Update server, you can specify the platform and asdm images for security appliances configured as Auto Update clients, including image revision numbers and locations, according to the device ID, device family, or device type of the client.

Introduction to Auto Update Server and Client Update

The Auto Update specification provides the infrastructure necessary for remote management applications to download security appliance configurations, software Images, and to perform basic monitoring from a centralized location.

As an Auto Update server, the specification allows the Auto Update server to either push configuration information and send requests for information to the security appliance, or to pull configuration information by causing the security appliance to periodically poll the Auto Update server. The Auto Update server can also send a command to the security appliance to send an immediate polling request at any time. Communication between the Auto Update server and the security appliance requires a communications path and local CLI configuration on each security appliance.

Fields

The Client Update pane consists of the following fields:

- **Enable Client Update**—Check to allow the security appliance to update the images used by other security appliances that are configured as Auto Update clients.
- **Client Images table**—lets you view previously-configured Client Update entries and includes the following columns:
 - **Device**—Displays a text string corresponding to a device-id of the client.
 - **Device Family**—Displays the family name of a client, either asa, pix, or a text string.
 - **Device Type**—Displays the type name of a client.
 - **Image Type**—Specifies the type of image, either ASDM image or Boot image.
 - **Image URL**—Specifies the URL for the software component.
 - **Client Revision**—Specifies the revision number(s) of the software component.

Double-clicking any of the rows in the Client Images table opens the Edit Client Update Entry dialog, in which you can modify the client parameters. These changes are immediately reflected in the table, but you must click Apply to save them to the configuration.

- **Live Client Update area**—Lets you immediately update Auto Update clients that are currently connected to the security appliance through a tunnel.
 - **Tunnel Group**—Select “all” to update all Auto Update clients connected over all tunnel groups, or specify a tunnel group for clients that you want to update.
 - **Update Now**—Click to begin an immediate update.



Note Live Client Update is only available when the security appliance is configured in routed mode.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | — |

Add/Edit Client Update

Fields

The Add/Edit Client Update dialog displays the following fields:

- Device Identification group:
 - Device ID—Enable if the client is configured to identify itself with a unique string, and specify the same string that the client uses. The maximum length is 63 characters.
 - Device Family—Enable if the client is configured to identify itself by device family, and specify the same device family that the client uses. It can be asa, pix, or a text string with a maximum length of 7 characters.
 - Device Type—Enable if the client is configured to identify itself by device type, and specify the same device type that the client uses. It can be pix-515, pix-515e, pix-525, pix-535, asa5505, asa5510, asa5520, or asa5540. It can also be a text string with a maximum length of 15 characters.
 - Not Specified—Select for clients that do not match the above.
- Image Type—Specifies an image type, either ASDM or boot image. This URL must point to a file appropriate for this client. Maximum length of 255 characters.
- Client Revision—Specifies a text string corresponding to the revision number(s) of the software component. For example: 7.1(0)22.
- Image URL—Specifies the URL for the software component. This URL must point to a file appropriate for this client.

Modes

The following table shows the modes in which this feature is available:

| Firewall Mode | | Security Context | | |
|---------------|-------------|------------------|----------|--------|
| Routed | Transparent | Single | Multiple | |
| | | | Context | System |
| • | • | • | — | — |

