Configuring Device Administration Policies on Firewall Devices

The Device Admin section contains pages for configuring device administration policies for firewall devices.

This chapter contains the following topics:

About AAA on Security Devices

Authentication-Authorization-Accounting (AAA) enables the security appliance to determine who a user is (authentication), what the user can do (authorization), and what the user did (accounting). You can use authentication alone, or with authorization and accounting. Authorization always requires a user to be authenticated first. You also can use accounting alone, or with authentication and authorization.

Authentication-Authorization-Accounting provides an extra level of protection and control for user access beyond access lists alone. For example, you can create an ACL that allows all outside users to access Telnet on a server on the DMZ network. If you want to limit user access to the server when you may not always know the IP addresses of these users, you can enable AAA to allow only authenticated and/or authorized users to make it through the security appliance. (The Telnet server enforces authentication, too; the security appliance prevents unauthorized users from attempting to access the server.)

- **Authentication**—Authentication grants access based on user identity. Authentication establishes user identity by requiring valid user credentials, which are typically a user name and password. You can configure the security appliance to authenticate the following items:
  - Administrative connections to the security appliance using Telnet, SSH, HTTPS/ASDM, or serial console.
  - The **enable** command.
- **Authorization**—Authorization controls user capabilities after users are authenticated. Authorization controls the services and commands available to each authenticated user. If you do not enable authorization, authentication alone would provide the same access to services for all authenticated users.

  If you need the control that authorization provides, you can configure a broad authentication rule, and then have a detailed authorization configuration. For example, you might authenticate inside users who attempt to access any server on the outside network, and then use authorization to limit the outside servers that a particular user can access.

  The security appliance caches the first 16 authorization requests per user, so if the user accesses the same services during the current authentication session, the security appliance does not resend the request to the authorization server.
- **Accounting**—Accounting tracks traffic that passes through the security appliance, providing a record of user activity. If you enable authentication for that traffic, you can account for traffic per user. If you do not authenticate the traffic, you can account for traffic per IP address. Accounting information includes when sessions start and stop, user name, the number of bytes that pass through the security appliance for the session, the service used, and the duration of each session.

Preparing for AAA

AAA services depend upon the use of the Local database or at least one AAA server. You can also use the Local database as a fallback for most services provided by an AAA server. Before you implement AAA, you should configure the Local database and configure AAA server groups and servers.

Configuration of the Local database and AAA servers depends upon the AAA services you want the security appliance to support. Regardless of whether you use AAA servers, you should configure the Local database with user accounts that support administrative access, to prevent accidental lock-outs and, if so desired, to provide a fallback method when AAA servers are unreachable. For more information, see Configuring User Accounts, page 51-7.

The following table provides a summary of AAA service support by each AAA server type and by the Local database. You manage the Local database by configuring user accounts on the **Platform > Device Admin > User Accounts** page (see Configuring User Accounts, page 51-7). You establish AAA server groups and add individual AAA servers to the server groups using the **Platform > Device Admin > AAA** page.

Table 48-1 Summary of AAA Support

AAA Service	Database Type							
	Local	**RADIUS**	**TACACS+**	**SDI**	**NT**	**Kerberos**	**LDAP**	**HTTP Form**
Authentication of...								
VPN users	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes[1]

Table 48-1 Summary of AAA Support (continued)

AAA Service	Database Type							
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP	HTTP Form
Firewall sessions	Yes	Yes	Yes	No	No	No	No	No
Administrators	Yes	Yes	Yes	No	No	No	No	No
Authorization of...								
VPN users	Yes	Yes	No	No	No	No	Yes	No
Firewall sessions	No	Yes[2]	Yes	No	No	No	No	No
Administrators	Yes[3]	No	Yes	No	No	No	No	No
Accounting of...								
VPN connections	No	Yes	Yes	No	No	No	No	No
Firewall sessions	No	Yes	Yes	No	No	No	No	No
Administrators	No	Yes	Yes	No	No	No	No	No

[1] HTTP Form protocol supports single sign-on authentication for WebVPN users only.

[2] For firewall sessions, RADIUS authorization is supported with user-specific ACLs only, which are received or specified in a RADIUS authentication response.

[3] Local command authorization is supported by privilege level only.

Local Database

The security appliance maintains a Local database that you can populate with user accounts, which contain, at a minimum, a user name. Typically, you assign a password and a privilege level to each user name, although passwords are optional. You can manage Local user accounts on the **Platform > Device Admin > User Accounts** page (see Configuring User Accounts, page 51-7).

If you enable command authorization using the Local database, the security appliance refers to the assigned user privilege level to determine what commands are available. By default, all commands are assigned either privilege level 0 or level 15.

Note If you add users to the Local database with 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.

You cannot use the local database for network access authorization.

The user accounts in the Local database can provide fallback support for console and enable-password authentication, for command authorization, and for VPN authentication and authorization. This behavior is designed to help you prevent accidental lock-out from the security appliance.

For users who need fallback support, we recommend that their user names and passwords in the Local database match their user names and passwords on the AAA servers. This provides transparent fallback support. Because the user cannot determine whether a AAA server or the local database is providing the service, using user names and passwords on AAA servers that are different than the user names and passwords in the Local database means that the user cannot be certain which user name and password should be given.

For multiple-context mode, you can configure user names 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 multiple mode.

AAA for Device Administration

You can authenticate all administrative connections to the security appliance, including:

- Telnet
- SSH
- Serial console
- ASDM
- VPN management access

You can also authenticate administrators who attempt to enter enable mode. You can authorize administrative commands. You can have accounting data for administrative sessions and for commands issued during a session sent to an accounting server.

You can configure AAA for device administration using the **Platform > Device Admin > AAA** page (see About AAA on Security Devices, page 48-1).

AAA for Network Access

You can configure rules for authenticating, authorizing, and accounting for traffic passing through the firewall by using the **Firewall > AAA Rules** page (see Chapter 15, “Managing Firewall AAA Rules”). The rules you create are similar to access rules, except that they specify whether to authenticate, authorize, or perform accounting for the traffic defined; and which AAA server group the security appliance is to use to process the AAA service request.

AAA for VPN Access

AAA services for VPN access include the following:

- User account settings for assigning users to VPN groups, configured on the **Platform > Device Admin > User Accounts** page (see Configuring User Accounts, page 51-7).
- VPN group policies that can be referenced by many user accounts or tunnel groups, configured on the **Remote Access VPN > RA VPN Policies > User Group Policy** or **Site to Site VPN > User Group Policy** page.
- Tunnel group policies, configured on the **Remote Access VPN > RA VPN Policies > PIX7.0/ASA Tunnel Group Policy** or **Site to Site VPN > PIX7.0/ASA Tunnel Group Policy** page.

Configuring AAA - Authentication Tab

The AAA page presents three tabbed panels; the **Authentication** panel is presented when you navigate to the AAA page. Use these options to control privileged access to the device console, to restrict access by connection type, and to define access messages.

Use the Authorization Tab, page 48-7 to control the services and commands available to authenticated users.

Use the Accounting Tab, page 48-8 to activate tracking of console traffic, providing a record of user activity.

Navigation Path

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

Related Topics

- About AAA on Security Devices, page 48-1
- Configuring User Accounts, page 51-7

Using the Authentication Tab

Use the Authentication tab to enable authentication for administrator access to the security appliance. The Authentication tab also lets you configure the prompts and messages a user sees when authenticated by an AAA server.

The device will prompt for a user name and password before you can enter commands. If the authentication server is offline, wait until the console login request times out. You can then access the console with the firewall username and the enable password.

Field Reference

Table 48-2 Authentication Tab

Element	Description
Require AAA Authentication to allow use of privileged commands	
Enable	Requires authentication from an AAA server to allow a user to access EXEC mode on the firewall. This option allows up to three attempts to access the firewall console. If this number is exceeded, an “access denied” message is displayed. When checked, the Server Group field is enabled.

Table 48-2 Authentication Tab (continued)

Element	Description
Server Group	Enter or Select the name of an AAA server to contact for user authentication.
Use LOCAL when server group fails	Check this box to use the LOCAL database as back-up if the selected server fails. (This option is not enabled until you provide a Server Group.)
Require AAA Authentication for the following types of connections	
Select the connections that require authentication. For each type, users are allowed up to three attempts to access the firewall console. If this number is exceeded, an "access denied" message is displayed. Select each connection option individually: • **HTTP** – Require AAA authentication when a user initiates an HTTPS connection to the firewall console. • **Serial** – Require AAA authentication when a user initiates a connection to the firewall console via the serial console cable. • **SSH** – Require AAA authentication when a user initiates a Secure Shell (SSH) connection to the console. • **Telnet** – Require AAA authentication when a user initiates a Telnet connection to the firewall console. For each selected connection, provide a Server Group and indicate whether the LOCAL database is used as a back-up: • **Server Group** – Enter or Select the name of an AAA server to contact for user authentication. • **Use LOCAL when server group fails** – Check this box to use the LOCAL database as back-up if the selected server fails. (This option is not enabled until you provide a Server Group.)	
Authentication Prompts	
Login Prompt	Enter the prompt a user will see when logging in to the security appliance.
Accepted Message	Enter the message displayed when successfully authenticated.
Rejected Message	Enter the message displayed when authentication fails for any reason.
Rejected Message for Invalid Credentials	Enter the message displayed when authentication fails following entry of unknown or invalid credentials. Available only on FWSM 3.2+ devices.
Rejected Message for Expired Password	Enter the message displayed when authentication fails following entry of an expired password. Available only on FWSM 3.2+ devices.
Maximum Local Authentication Failed Attempts	Specify the number of times the device will try to authenticate a user in the LOCAL database before that account is locked; valid values are 1 through 16. Available only on ASA/PIX 7.01+ and FWSM 3.11+ devices.

Table 48-2 Authentication Tab (continued)

Element	Description
Login History	Check this to enable the login history reporting feature. When enabled, information about all the administrative login attempts is collected and displayed on the ASA, immediately after a successful login. This includes the following information: • Date and time of the last login • Location of last login (terminal or IP address) • Number of unsuccessful login attempts since the last successful login. • Number of successful login attempts occurring during an organization-defined time period. **Note** This feature is enabled by default.
Duration (Optional)	Enter the number of days for which login events will be saved. When no value is specified here, the login history is unbounded. **Note** The default value is 90 days.

Authorization Tab

The Authorization tab allows you to configure authorization for accessing firewall commands.

Navigation Path

You can access the Authorization tab from the AAA page; see Configuring AAA - Authentication Tab, page 48-5.

Related Topics

- About AAA on Security Devices, page 48-1
- Accounting Tab, page 48-8

Field Reference

Table 48-3 Authorization Tab

Element	Description
Enable Authorization for Command Access	Requires authorization for accessing firewall commands.
Server Group	Specify the server group to use for authorization.
Use LOCAL when server group fails	Uses the LOCAL server group if the selected server group fails.

Table 48-3 Authorization Tab (continued)

Element	Description
Enable Authorization for exec shell access (ASA 8.0(2)+ only)	When selected, enables management authorization. After enabling management authorization, specify whether to use the remote server or the local database for authorization: • **Local Server**—the local user database is the source for the username entered and the Service-Type and Privilege-Level attributes assigned. • **Remote Server**—the same server is used for both authentication and authorization.
Auto Enable Authorization for exec shell access (ASA 9.1(5)+ only)	Allows users with sufficient privileges from the login authentication server to be placed directly in privileged EXEC mode. Otherwise, users are placed in user EXEC mode. These privileges are determined by the Service-Type and Privilege-Level attributes that are required to enter each EXEC mode. To enter privileged EXEC mode, users must have a Service-Type attribute of Administrative and a Privilege Level attribute of greater than 1 assigned to them. This option is not supported in the system context. However, if you configure Telnet or serial authentication in the admin context, then authentication also applies to sessions from the switch to the ASASM.
Enable Authorization for HTTP Connection	When selected, authorization via HTTP is enabled. Authorization of username is disabled by default.
Server Group	Select the server group to use for authorization.
Use LOCAL when server group fails (ASA 9.4(1)+ only)	Uses the LOCAL server group if the selected server group fails.

Accounting Tab

Use the Accounting tab to enable accounting for access to the firewall device and for access to commands on the device.

Navigation Path

You can access the Accounting tab from the AAA page; see Configuring AAA - Authentication Tab, page 48-5.

Related Topics

- About AAA on Security Devices, page 48-1
- Authorization Tab, page 48-7

Field Reference

Table 48-4 Accounting Tab

Element	Description
Require AAA Accounting for privileged commands	
Enable	When selected, enables the generation of accounting records to mark the entry to and exit from privileged mode for administrative access via the console.
Server Group	Specify the server or group of RADIUS or TACACS+ servers to which accounting records are sent.
Require AAA Accounting for the following types of connections	
Connection type	Specify the connection types that will generate accounting records: • **HTTP**—Enable or disable the generation of accounting records to mark the establishment and termination of admin sessions created over HTTP. Valid server group protocols are RADIUS and TACACS+. • **Serial**—Enable or disable the generation of accounting records to mark the establishment and termination of admin sessions that are established via the serial interface to the console. Valid server group protocols are RADIUS and TACACS+. • **SSH**—Enable or disable the generation of accounting records to mark the establishment and termination of admin sessions created over SSH. Valid server group protocols are RADIUS and TACACS+. • **Telnet**—Enable or disable the generation of accounting records to mark the establishment and termination of admin sessions created over Telnet. Valid server group protocols are RADIUS and TACACS+.
Server Group	Specify the server or group of RADIUS or TACACS+ servers to which accounting records are sent.
Require Accounting for command access	
Enable	When selected, enables the generation of accounting records for commands entered by an administrator/user.
Server Group	Provides a drop-down menu from which you can choose the server or group of RADIUS or TACACS+ servers to which accounting records are sent.
Privilege Level	Minimum privilege level that must be associated with a command for an accounting record to be generated. The default privilege level is 0.

Configuring Banners

You can use the Banner page to specify Session (exec), Login, and Message-of-the-Day (motd) banners for a security appliance or shared policy.

Note If you use the token `$(hostname)` or `$(domain)` in a banner, it is replaced with the host name or domain name of the security appliance. When you enter the `$(system)` token in a context configuration, the context uses the banner configured in the system configuration.

Spaces in banner text are preserved; however, tabs cannot be entered. Multiple lines in a banner are created by entering a separate line of text for each line you wish to add. Each line is then appended to the end of the existing banner. If the line is empty, a carriage return (CR) is 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 (press 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.

Related Topics

- Chapter 52, "Configuring Server Access Settings on Firewall Devices"

Step 1 To configure banners, access the Banner page:

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

Step 2 In the **Session (exec) Banner** field, enter the text you want the system to display as a banner before displaying the enable prompt.

Step 3 In the **Login Banner** field, enter the text you want the system to display as a banner before the password login prompt when accessing the security appliance using Telnet.

Step 4 In the **Message-of-the-Day (motd) Banner** field, enter the text you want the system to display as a message-of-the-day banner.

Step 5 To replace a banner, change the contents of the appropriate box.

Step 6 To remove a banner, clear the contents of the appropriate box.

Configuring Boot Image/Configuration Settings

Use the Boot Image/Configuration page to specify which configuration file the security appliance will use at start-up. You can also specify the path to an Adaptive Security Device Manager (ASDM) configuration file.

If you do not specify a boot-image location, the first valid image on internal flash memory will be chosen to launch the system.

Note This page is available only on ASA and PIX 7.0+ devices

Navigation Path

- (Device view) Select **Platform > Device Admin > Boot Image/Configuration** from the Device Policy selector.

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

Field Reference

Table 48-5 Boot Image/Configuration Page

Element	Description
Boot Config Location	Enter the path to and name of the configuration file to be used when the system is loaded. On an ASA, you can use any of the following syntactical constructs: • **disk0:/**[*path/*]*filename* The value "disk0" represents the internal flash card. You can also use "**flash**" instead of "**disk0**," as they are aliased: – **flash:/**[*path/*]*filename* • **disk1:/**[*path/*]*filename* The value "disk1" represents the external flash card. On a PIX device, you can use only the "flash" syntax; that is: • **flash:/**[*path/*]*filename*
ASDM Image Location	The location and name of the ASDM software image to be used when ASDM sessions are initiated. (You can use ASDM to monitor both ASA and PIX devices.) On a PIX device, as with the Boot Config Location, you are restricted to only the "flash" syntax. On an ASA, as with the Boot Config Location, you can use the "disk0," "flash," or "disk1" constructs. In addition, you can specify an image file on a TFTP server, as follows • **tftp://**[*user*[*:password*]@]*server*[*:port*]/[*path/*]*filename*
Boot Images Table	This table lists any alternate configuration files you have defined; you can specify up to four. The first available image in this list is used if you did not specify a primary file in the Boot Config Location field, or if that file is unavailable. This is a standard Security Manager table; use the up-arrow, down-arrow, Add Row, Edit Row, and Delete Row buttons below the table to manage these entries, as described in Using Tables, page 1-48. The Add Row and Edit Row open the Images Dialog Box, page 48-12, used to add and edit the paths to alternate configuration files. **Note** On an ASA, the first (and only the first) entry in this table can refer to an ASDM configuration file on a TFTP server. If the device cannot reach the TFTP server, it will attempt to load the next image file in the list.

Images Dialog Box

Use the Images dialog box to add or edit a configuration file entry in the Boot Images table on the Boot Image/Configuration page.

Navigation Path

You can access the Images dialog box from the Boot Image/Configuration page. For more information, see Configuring Boot Image/Configuration Settings, page 48-10.

Field Reference

The Images dialog box contains one field, used to define the path to a boot image or configuration file, as follows:

Table 48-6 Images Dialog Box

Element	Description
Image File	Enter the path to and name of the configuration file to add to the ordered Boot Images list. On a PIX device, you can use only the "flash" syntax; that is: • **flash:/**[*path/*]*filename* On an ASA, you can use any of the following syntactical constructs: • **disk0:/**[*path/*]*filename* The value "disk0" represents the internal flash card. You can also use "**flash**" instead of "**disk0**," as they are aliased: – **flash:/**[*path/*]*filename* • **disk1:/**[*path/*]*filename* The value "disk1" represents the external flash card. In addition, on an ASA, you can specify an ASDM image file on a TFTP server, as follows • **tftp://**[*user*[*:password*]@]*server*[*:port*]/[*path/*]*filename* Note that you can specify only one TFTP location, and it must be listed first in the Boot Images table on the Boot Image/Configuration page.

Configuring CLI Prompt

You can use the CLI Prompt page to customize the prompt used by ASA 7.2(1)+ devices during CLI sessions. By default, the prompt shows the hostname of the ASA. In multiple context mode, the prompt also displays the context name. You can display the following items in the CLI prompt:

Note The attributes that are available differ by ASA version:

cluster-unit (ASA 9.1.1+ only)	Displays the cluster unit name. Each unit in a cluster can have a unique name.

context	(Multiple mode only) Displays the name of the current context.
domain	Displays the domain name.
hostname	Displays the hostname.
management-mode (ASA 9.2.1+ only)	Displays the management mode.
priority	Displays the failover priority as pri (primary) or sec (secondary).
state	Displays the traffic-passing state or role of the unit. For failover, the following values appear for the state: • act—Failover is enabled, and the unit is actively passing traffic. • stby— Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or another inactive state. • actNoFailover—Failover is not enabled, and the unit is actively passing traffic. • stbyNoFailover—Failover is not enabled, and the unit is not passing traffic. This condition might occur when there is an interface failure above the threshold on the standby unit. For clustering, the following values are displayed for state: • master • slave For example, in the prompt ciscoasa/cl2/slave, the hostname is ciscoasa, the unit name is cl2, and the state is slave.

Step 1 Access the CLI Prompt page by doing one of the following:

- (Device view) Select **Platform > Device Admin > CLI Prompt** from the Device Policy selector.

  Note For devices in multiple context mode, the CLI Prompt page is only available in the system context. In the admin context, the CLI Prompt page is not available.

- (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > CLI Prompt** from the Policy Types selector. Select an existing policy from the Policies selector, or create a new one.

Step 2 Customize the CLI prompt by doing the following:

- To add an attribute to the prompt, select the attribute in the Available Members list and then click **>>**. The attribute is moved from the Available Members list to the Selected Members list.

  You can add multiple attributes to the prompt. The order in which the attributes are added to the Selected Members list will dictate the order in which they are shown in the CLI prompt.

  Note For ASA 9.1.1+, you can configure up to six attributes for the CLI prompt. For earlier ASA versions, you can only configure up to five attributes.

- To remove an attribute from the prompt, select the attribute in the Selected Members list and then click <<. The attribute is moved from the Selected Members list to the Available Members list.

Setting the Device Clock

Use the Clock page to set the date and time on the selected device.

Note This page is not available on Catalyst 6500 service modules (the Firewall Services Module and the Adaptive Security Appliance Service Module).

To dynamically set the time using an NTP server, see NTP Page, page 52-21; time derived from an NTP server overrides any time set manually on the Clock page.

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

Navigation Path

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

Field Reference

Table 48-7 Clock Page

Element	Description
Device Time Zone	Choose a time zone for the device. These options represent Greenwich Mean Time (GMT) plus or minus a number of hours. **Note** Changing the time zone on the device may drop the connection to any installed Security Services modules (SSMs).
Daylight Savings Time (Summer Time)	Choose a daylight savings time option, and if necessary, specify when and how daylight savings time is applied: **None** – Choose this option to disable automatic correction for daylight savings time. **Set by Date** – Choose this option to specify the date and time when daylight savings time begins and ends for a specific year. If you use this option, you will need to reset the dates every year. **Set by Day** – Choose this option to specify the start and end dates for daylight saving time using the month, week, and day on which daylight savings time begins and ends. This option also lets you set a recurring date range that you do not need to alter yearly.
Set by Date The following three parameters appear in a Start section and an End section. Use the two sets to define when daylight savings time starts and ends.	

Table 48-7 Clock Page (continued)

Element	Description
Date	Enter the date on which daylight savings time begins or ends, in MMM DD YYYY format (for example, Jul 15 2011). You also can click the calendar icon to select the date from a pop-up calendar.
Hour	Choose the hour, from 00 to 23, in which daylight savings time begins or ends.
Minute	Choose the minute, from 00 to 59, at which daylight savings time begins or ends.
Set by Day	
Specify Recurring Time	Check this box to enable the Start and End parameters, which are used to set a recurring start and end for daylight savings time that you do not need to alter yearly.
The following five parameters appear in a Start section and an End section. Use the two sets to define when daylight savings time starts and ends.	
Month	Choose the month in which daylight savings time begins or ends.
Week	Choose the week of the month in which daylight savings time begins or ends. You can select a numerical value that corresponds to the week—1 through 4—or you can specify the first or last week in the month by choosing **first** or **last**. For example, if the day might fall in the partial fifth week, choose last.
Weekday	Choose the day of the week on which daylight savings time begins or ends.
Hour	Choose the hour, from 0 to 23, in which daylight savings time begins or ends.
Minute	Choose the minute, from 00 to 59, at which daylight savings time begins or ends.

Enabling/Disabling FIPS

Beginning with 4.15, Cisco Security Manager provides an option to enable or disable the Federal Information Processing Standards (FIPS) mode on the ASA devices. When you enable FIPS mode with FOM, instead of legacy methods implemented in Cisco SSL versions, the FIPS 140-2 standard compliant cryptographic methods implemented in the FOM is used for signature and verification purposes. This feature is supported only on ASA 9.8.2 or higher devices.

Note To configure FIPS mode on a device, you must reboot the device manually.

Before you enable FIPS, ensure the following are configured on ASA:

1. DH group is set to 14 or ECDH group is set to 19, 20, or 21.
2. The Device Identity Certificate key type is set to RSA and the key size is 2048 or above.

Navigation Path

- (Device view) Select **Platform > Device Admin > FIPS** from the Device Policy selector.

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

Field Reference

Table 48-8 FIPS Page

Element	Description
FIPS	Select the check box to enable FIPS on the device. This option is available only for ASA 9.8.2 or above. **Note** You must reboot the device after enabling or disabling FIPS for the configuration to take effect.

Configuring Umbrella Global Policy

Beginning with version 4.18, Cisco Security Manager supports configuring Umbrella global policy. Cisco Umbrella Branch is a cloud based security service, which first inspects the DNS traffic, and then examines suspicious HTTP/(S) traffic. The Umbrella connector intercepts DNS packets and redirects the interesting DNS queries to the Umbrella resolver for resolution. Once the DNS response is received, it forwards the response to the host. This feature is supported only on ASA 9.10.1 or higher devices.

After configuring Umbrella service, ensure that the Umbrella DNS policy-map is also configured.

Navigation Path

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

Field Reference

Table 48-9 Umbrella Page

Element	Description
Umbrella	Select the check box to apply the global Umbrella configuration for the selected device (ASA 9.10.1 or higher).
Token	The token value of the ASA device on registering with the Umbrella server. Cisco Security Manager throws an error message if this value is less than 64 characters.
Public Key	The public key value of the ASA device on registering with the Umbrella server. This value must be 64 hexa-decimal digits and less than 80 characters, else Cisco Security Manager will display an error message.
EDNS Flow Timeout	The configured EDNS timeout value. The Umbrella time-out for edns-flow must be between <0:0:0> and <1193:0:0>, else Cisco Security Manager will display error message.

Configuring Device Credentials

Use the Credentials page to specify the user credentials Security Manager will use when contacting this device. You can also change the Enable password and the Telnet/SSH password on the device.

This user name-password combination lets you log into the device (in EXEC mode) if you connect to the security appliance using an HTTP, HTTPS, Telnet, or SSH session. You also can specify a separate password specifically for Telnet and SSH sessions. (Further, you can define separate credentials for HTTP/HTTPS connections on the Device Credentials Page, page 3-45 in the Device Properties window.)

The Enable password lets you access privileged EXEC mode after you log in.

Tip The Username, Password, and Enable Password on this page are linked to the Credentials settings in the Device Properties window. When you update these parameters and then deploy the changes to the device, Security Manager uses the existing credentials defined in the Device Properties to log into the device and deploy changes. After successful deployment, the Device Properties credentials are updated to match these settings. For more information about Credentials in Device Properties, see Device Credentials Page, page 3-45.

Navigation Path

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

Warning **Since several user accounts may exist on each device, applying a shared Credentials policy to multiple devices will update only the Enable Password on each device; the Username and Password provided in the shared policy are not applied (nor is the Telnet/SSH password). The Enable Password is sufficient for subsequent access to PIX/ASA/FWSM devices, unless external authentication such as AAA or TACACS+ is configured, in which case the Enable Password alone is not sufficient. In this situation, you must manually update the Username, Password and Enable Password on each device that uses external authentication.**

Related Topics

- Configuring User Accounts, page 51-7

Field Reference

Table 48-10 Credentials Page

Element	Description
Username	Enter a user name for logging into the device. The name must be at least four characters; the maximum is 64 characters. Entries are case-sensitive.
Password Confirm	Provide a password for logging into the device (EXEC mode) with the specified Username. This password must be at least three characters; the maximum is 32 characters. Entries are case-sensitive. Re-enter the user password in the Confirm field. **Note** We recommend a password length of at least 8 characters.

Table 48-10 Credentials Page (continued)

Element	Description
Privilege Level	Choose a privilege level for this user; available values are 1 through 15. Level 1 allows EXEC-mode access only, the default level for log-in; level 15 allows Privileged EXEC-mode access; that is, access to the Enable mode. Other levels must be explicitly defined on the device.
Enable password	
Password as encrypted	Select Plain Text or Encrypted.
Password encrypt type	Select MD5 or PBKDF2.
Enable Password Confirm	You can specify an Enable password that lets this user access Privileged EXEC mode after logging in. Entries are case-sensitive. Re-enter the Enable password in the Confirm field. **Note** For Plain Text passwords: – The length of MD5 password should be three to 32 characters. – The length of PBKDF2 password should be 33 to 127 characters. **Note** If you configure user authentication for Enable access, each user has their own password and this password is not used. See Configuring AAA - Authentication Tab, page 48-5 for more information.
Telnet/SSH Password Confirm	You can specify a password that provides access to EXEC mode when connecting to the device via a Telnet or SSH session. This password must be at least three characters; the maximum is 32 characters. Entries are case-sensitive. Re-enter the Telnet/SSH password in the Confirm field. **Note** If you configure user authentication for Telnet or SSH access, each user has their own password and this password is not used. See Configuring AAA - Authentication Tab, page 48-5 for more information.

Managing Mount Points

Use the Mount Points page to make a Common Internet File System (CIFS) or a File Transfer Protocol (FTP) file system accessible to the security appliance.

Note When you create an FTP-type mount point, the FTP server must have a UNIX directory listing style. Microsoft FTP servers have the MS-DOS directory listing style as their default.

The File Mount Point Configuration table lists the configured mount points. The File Mount Point Configuration table is a standard Security Manager table, with Add Row, Edit Row and Delete Row buttons. (These are standard buttons, as described in Using Tables, page 1-48.) The Add Row button opens the Add Mount Point Configuration dialog box, and Edit Row opens the Edit Mount Point Configuration dialog box. Other than the titles, the two dialog boxes are identical. For more information, see Add/Edit Mount Point Configuration Dialog Box, page 48-19.

Note This feature is available only on ASA 8.0(2)+ devices. Mount points are supported in router mode only. For ASA versions between 8.0(2) and 9.x, mount points are not supported in multiple-context mode. Mount points are supported in the Admin context on ASA 9.x+ devices in multiple-context, routed mode.

Navigation Path

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

Add/Edit Mount Point Configuration Dialog Box

Use the Add/Edit Mount Point Configuration dialog box to add or edit a mount point entry in the File Mount Point Configuration table on the Mount Points page. You use mount points to make a Common Internet File System (CIFS) or a File Transfer Protocol (FTP) file system accessible to the security appliance.

Navigation Path

You can access the Add/Edit Mount Point Configuration dialog box from the Mount Points page. For more information, see Managing Mount Points, page 48-18.

Field Reference

Table 48-11 Add/Edit Mount Point Configuration Dialog Box

Element	Description
Enable Mount Point	Whether the file system is mounted or unmounted (available or unavailable).
Connection Type	Select the type of file system to mount: • **cifs**—Specifies that the file system being mounted is CIFS, a file system that provides volume-mounting capabilities for CIFS-shared directories. • **ftp**—Specifies that the file system being mounted is FTP, a Linux kernel module, enhancing the Virtual File System (VFS) with FTP volume-mounting capabilities that allow you to mount FTP-shared directories. **Note** When you create an FTP-type mount point, the FTP server must have a UNIX directory listing style. Microsoft FTP servers have the MS-DOS directory listing style as their default.
Mount Point Name	Specifies the name of the mount point. The mount point name is used when other CLI commands refer to the filesystem already mounted on the security appliance. A maximum of 31 characters are allowed for the mount point name.
Server Name/IP Address	Specifies the predefined name (or the IP address in dotted decimal notation) of the CIFS or FTP file-system server.
Username	Specifies the authorized username for file-system mounting.

Table 48-11 Add/Edit Mount Point Configuration Dialog Box (continued)

Element	Description
Password Confirm	Identifies the authorized password for file-system mounting.
Encrypt Password	Select to indicate that the password supplied is in encrypted format.
Share Name (CIFS only)	Explicitly identifies a specific server share (a folder) by name to access file data within a server.
Domain Name (CIFS only)	For CIFS file systems only, this argument specifies the Windows NT domain name. A maximum of 63 characters is permitted.
Mode (FTP only)	Identifies the FTP transfer mode as either active or passive.
Path (FTP only)	Specifies the directory pathname to the specified FTP file-system server. Question marks and spaces are not allowed in the pathname and will be suppressed.

IP Client

The IP Client page lists the interface name and the IP version. You can use the configured IP Client for integrated routing and bridging support on Firepower 2100 Series devices. The IP Client page has the standard options to Add, Edit and Delete the entries.

Note This feature is available only on ASA 9.8.2+ Firepower 2100 Series single context devices. No multi context support for IP-Client.

Navigation Path

- (Device view) Select **Platform > Device Admin > IP Client** from the Device Policy selector.

Note The menu appears only for a Firepower 2100 Series device.

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

Add/Edit IP Client Dialog Box

Use the Add/Edit IP Client dialog box to add or edit a IP Client entry in the IP Client table on the IP Client page. You use IP Client settings to support integrated routing and bridging on Firepower 2100 Series devices.

Navigation Path

You can access the Add/Edit IP Client dialog box from the IP Client page. For more information, see IP Client, page 48-20.

Field Reference

Table 48-12 Add/Edit IP Client Dialog Box

Element	Description
IP Version	The IP address of the device. It can be an IPv4 or an IPv6 address.
Interface	Select the interface pertaining to the Firepower 2100 Series device.

The preview configuration page displays the IP Client configuration with IPv6 suffixed for IPv6 interfaces. For IPv4 interfaces, only the interface name is displayed.

App Agent

Use the App Agent page to configure the App Agent settings. You can specify the heartbeat interval and retry count.

Note App-Agent is available only on Firepower 2100 Series, Firepower 4000 Series, and Firepower 9000 Series devices. In Cisco Security Manager, App-Agent in Firepower 2100 Series device is supported from 9.8.2+; App-Agent in Firepower 4000 Series, and Firepower 9000 Series device is supported from 9.6.2+.

Navigation Path

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

Field Reference

Table 48-13 App Agent Page

Element	Description
Interval	Enter the app agent heartbeat interval. From ASA 9.6.2 to ASA 9.8.1, App-Agent heartbeat value can be between 300 to 6000 ms. For ASA 9.8.2+ devices, App-Agent heartbeat interval value can be between 100 to 6000 ms. **Note** Cisco Security Manager will display an error message if you do not enter values in multiples of 100.
Retry Count	Enter the retry count between 3 to 10.
Save	Click to save the configuration.