



# CHAPTER 11

## Configuring Device Access

---

This chapter contains the following topics:

- [AAA Access](#)
- [HTTPS/ASDM](#)
- [Secure Shell](#)
- [Telnet](#)
- [Virtual Access](#)

### AAA Access

The AAA Access pane includes tabs for configuring authentication, authorization, and accounting for management access. For an overview of AAA services, see [Configuring AAA Servers](#).

- [Authentication Tab](#)
- [Authorization Tab](#)
- [Accounting Tab](#)

#### Modes

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

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

### Authentication Tab

Use this tab to enable authentication for administrator access to the security appliance. Authentication lets you control access by requiring a valid username and password. You can configure the security appliance to authenticate the following items:

- All administrative connections to the security appliance using the following methods:

- Telnet
- SSH
- HTTPS/ASDM
- Serial
- The **enable** command

#### Fields

- Require authentication to allow use of privileged mode commands—Specifies the parameters that control access to the privileged mode commands.
  - Enable—Enables or disables the requirement that a user be authenticated before being allowed to use privileged mode commands.
  - Server Group—Selects the server group to use for authenticating users to use privileged mode commands.
  - Use LOCAL when server group fails—Allows the use of the LOCAL database for authenticating users to use privileged mode commands if the selected server group fails.
- Require authentication for the following types of connections—Specifies the types of connections for which you want to require authentication and specifies the server group to use for that authentication.
  - HTTP/ASDM—Specifies whether to require authentication for HTTP/ASDM connections.
  - Server Group—Selects the server group to use for authenticating the specified connection type.
  - Use LOCAL when server group fails—Allows the use of the LOCAL database for authenticating the specified connection type if the selected server group fails.
  - SSH—Specifies whether to require authentication for SSH connections.
  - Telnet—Specifies whether to require authentication for Telnet connections.
  - Serial—Specifies whether to require authentication for serial connections.

#### Modes

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

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

## Authorization Tab

Authorization lets you control access *per user* after you authenticate with a valid username and password. You can configure the security appliance to authorize management commands.

Authorization lets you control which services and commands are available to an individual user. Authentication alone provides the same access to services for all authenticated users.

When you enable command authorization, you have the option of manually assigning privilege levels to individual commands or groups of commands (using the **Advanced** button) or enabling the Predefined User Account Privileges (using the Restore Predefined User Account Privileges button):

Predefined User	Privilege Level	Description
Admin	15	Full access to all CLI commands
Read Only	5	Read only access to all commands
Monitor Only	3	Monitoring tab only

The Predefined User Account Privileges Setup pane displays a list of commands and privileges ASDM issues to the security appliance if you click Yes. Yes allows ASDM to support the three privilege levels: Admin, Read Only and Monitor Only.

The Command Privileges Setup pane displays a list of commands and privileges ASDM is going to issue to the security appliance. You can select one or more commands in the lists and use the Edit button to change the privilege level for the selected commands.

#### Fields

- **Enable**—Enables or disables authorization for security appliance command access. Selecting this check box activates the remaining parameters on this pane.
- **Server Group**—Selects the server group to use for authorizing users for command access.
- **Use LOCAL when server group fails**—Allows the use of the LOCAL database for authorizing users to use privileged mode commands if the selected server group fails.
- **Advanced**—Opens the Command Privileges Setup pane, on which you can manually assign privilege levels to individual commands or a group of commands.
- **Restore Predefined User Account Privileges**—Opens the Predefined User Account Command Privilege Setup pane, which sets up predefined user profiles and sets the privilege levels for the selected, listed commands.

#### Modes

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

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

## Command Privileges Setup

Use this pane to assign privilege levels to individual commands or groups of commands. Clicking a column heading sorts the entire table in alphanumeric order, using the selected column as the key field.

- **Command Mode**—Selects a specific command mode or All Modes. This selection determines what appears in the Command Modes table immediately below this list.
- **CLI Command**—Specifies the name of a CLI command.

- **Mode**—Indicates a mode that applies to this command. Certain commands have more than one mode.
- **Variant**—Indicates the form (for example, show or clear) of the specified command to which the privilege level applies.
- **Privilege**—Shows the privilege level currently assigned to this command.
- **Edit**—Displays the Select Command(s) Privilege dialog box. This dialog box lets you select from a list the privilege level for one or more commands selected on the parent window. The Command Modes table reflects the change as soon as you click OK.
- **Select All**—Selects the entire contents of the Command Modes table.

### Modes

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

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

## Predefined User Account Command Privilege Setup

This pane asks whether you want the security appliance to set up user profiles named Admin, Read Only, and Monitor Only. You get to this pane by clicking Restore Predefined user Account Privileges on the Authorization tab of the Authentication/Authorization/Accounting pane.

### Fields

- **Command List**—Lists the CLI commands, their modes, variants, and privileges, affected by the predefined user account privilege setup.
  - **CLI Command**—Specifies the name of a CLI command.
  - **Mode**—Indicates a mode that applies to this command. Certain commands have more than one mode.
  - **Variant**—Indicates the form (for example, show or clear) of the specified command to which the privilege level applies.
  - **Privilege**—Shows the privilege level currently assigned to this command.
- **Yes**—Directs the security appliance to set up the listed commands with the respective privilege levels. This setup lets you create users through the User Accounts pane with the roles Admin, privilege level 15; Read Only, with privilege level 5; and Monitor Only with privilege level 3.
- **No**—Lets you manage the privilege levels of commands and users manually.

### Modes

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

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

## Accounting Tab

Accounting lets you keep track of traffic that passes through the security appliance. 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, the AAA client messages and username, the number of bytes that pass through the security appliance for the session, the service used, and the duration of each session.



### Note

You can configure accounting only for a TACACS+ server group. If no such group has yet been configured, go to Configuration > Properties > AAA Setup > AAA Server Groups.

### Fields

- Require accounting to allow accounting of user activity—Specifies parameters related to accounting of user activity.
  - Enable—Enables or disables the requirement to allow accounting of user activity.
  - Server Group—Specifies the selected server group, if any, to use for user accounting. If no TACACS+ server group exists, the default value of this list is --None--.



### Note

The definition of the Server Group list parameter is the same for all group boxes on this pane.

- Require accounting for the following types of connections—Specifies the connection types for which you want to require accounting and the respective server groups for each.
  - HTTP/ASDM—Requires accounting for HTTP/ASDM connections.
  - Serial—Requires accounting for serial connections.
  - SSH—Requires accounting for secure shell (SSH) connections.
  - Telnet—Requires accounting for Telnet connections.
- Require command accounting for *Security Appliance*—You can send accounting messages to the TACACS+ accounting server when you enter any command other than **show** commands at the CLI. If you customize the command privilege level using the Configuration > Device Access > AAA Access > Authorization > Command Privilege Setup dialog box, you can limit which commands the security appliance accounts for by specifying a minimum privilege level. The security appliance does not account for commands that are below the minimum privilege level.
  - Enable—Enables accounting for commands.
  - Privilege level—Sets the minimum privilege level for which to perform command accounting.

### Modes

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

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

## HTTPS/ASDM

The HTTPS/ASDM pane provides a table that specifies the addresses of all the hosts or networks that are allowed access to the ASDM using HTTPS. You can use this table to add or change the hosts or networks that are allowed access.

### Fields

- **Interface**—Lists the interface on the security appliance from which the administrative access to the device manager is allowed.
- **IP Address**—Lists the IP address of the network or host that is allowed access.
- **Mask**—Lists the network mask associated with the network or host that is allowed access.
- **Add**—Displays the Add HTTP Configuration dialog box for adding a new host or network.
- **Edit**—Displays the Edit HTTP Configuration dialog box for editing the selected host or network.
- **Delete**—Deletes the selected host or network.

### 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 HTTP Configuration

The Add/Edit HTTP Configuration dialog box lets you add a host or network that will be allowed administrative access to the security appliance device manager over HTTPS.

### Fields

- **Interface Name**—Specifies the interface on the security appliance from which the administrative access to the security appliance device manager is allowed.
- **IP Address**—Specifies the IP address of the network or host that is allowed access.
- **Mask**—Specifies the network mask associated with the network or host that is allowed access.

### Modes

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

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

## Secure Shell

The Secure Shell pane lets you configure rules that permit only specific hosts or networks to connect to the security appliance for administrative access using the SSH protocol. The rules restrict SSH access to a specific IP address and netmask. SSH connection attempts that comply with the rules must then be authenticated by a AAA server or the Telnet password.

You can monitor SSH sessions using Monitoring > Administration > Secure Shell Sessions.

### Fields

The Secure Shell pane displays the following fields:

- Allowed SSH Versions—Restricts the version of SSH accepted by the security appliance. By default, SSH Version 1 and SSH Version 2 connections are accepted.
- Timeout (minutes)—Displays the number of minutes, 1 to 60, the Secure Shell session can remain idle before the security appliance closes it. The default is 5 minutes.
- SSH Access Rule—Displays the hosts and networks that are allowed to access the security appliance using SSH. Double-clicking a row in this table opens the Edit SSH Configuration dialog box for the selected entry.
  - Interface—Displays the name of a security appliance interface that will permit SSH connections.
  - IP Address—Displays the IP address of each host or network permitted to connect to this security appliance through the specified interface.
  - Mask—Displays the netmask for the IP address of each host or network permitted to connect to this security appliance through the specified interface.
- Add—Opens the Add SSH Configuration dialog box.
- Edit—Opens the Edit SSH Configuration dialog box.
- Delete—Deletes the selected SSH access rule.

### 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 SSH Configuration

The Add SSH Configuration dialog box lets you add a new SSH access rule to the rule table. The Edit SSH Configuration dialog box lets you change an existing rule.

### Fields

- **Interface**—Specifies the name of the security appliance interface that permits SSH connections.
- **IP Address**—Specifies the IP address of the host or network that is permitted to establish an SSH connection with the security appliance.
- **Mask**—The netmask of the host or network that is permitted to establish an SSH connection with 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
•	•	•	•	—

## Telnet

The Telnet pane lets you configure rules that permit only specific hosts or networks running ASDM to connect to the security appliance using the Telnet protocol.

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



### Note

Although a configuration file may contain more, there may be only five Telnet sessions active at the same time in single context mode. In multiple context mode, there may be only five Telnet sessions active per context.

### Fields

The Telnet pane displays the following fields:

Telnet Rule Table:

- **Interface**—Displays the name of a security appliance interface which will permit Telnet connections, an interface on which is located a PC or workstation running ASDM.
- **IP Address**—Displays the IP address of each host or network permitted to connect to this security appliance through the specified interface.



### Note

This is not the IP address of the security appliance interface.

- **Netmask**—Displays the netmask for the IP address of each host or network permitted to connect to this security appliance through the specified interface.



**Note** This is not the IP address of the security appliance interface.

- **Timeout**—Displays the number of minutes, 1 to 60, the Telnet session can remain idle before the security appliance closes it. The default is 5 minutes.
- **Add**—Opens the Add Telnet Configuration dialog box.
- **Edit**—Opens the Edit Telnet Configuration dialog box.
- **Delete**—Deletes the selected item.
- **Apply**—Sends changes made in ASDM to the security appliance and applies them to the running configuration. Click **Save** to write a copy of the running configuration to Flash memory. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby unit.
- **Reset**—Discards changes and reverts to the information displayed before changes were made or the last time you clicked **Refresh** or **Apply**. After **Reset**, use **Refresh** to make sure that information from the current running configuration is displayed.

### 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 Telnet Configuration

### Adding Telnet Rules

To add a rule to the Telnet rule table, perform the following steps:

1. Click the **Add** button to open the **Telnet > Add** dialog box.
2. Click **Interface** to add a security appliance interface to the rule table.
3. In the IP Address box, enter the IP address of the host running ASDM which will be permitted Telnet access through this security appliance interface.



**Note** This is not the IP address of the security appliance interface.

4. In the Mask list, select or enter a netmask for the IP address to be permitted Telnet access.



**Note** This is not a mask for the IP address of the security appliance interface.

5. To return to the previous pane click:

- **OK**—Accepts changes and returns to the previous pane.
- **Cancel**—Discards changes and returns to the previous pane.
- **Help**—Provides more information.

### Editing Telnet Rules

To edit a rule in the Telnet rule table, perform the following steps:

1. Click **Edit** to open the Telnet > Edit dialog box.
2. Click **Interface** to select a security appliance interface from the rule table.
3. In the IP Address field, enter the IP address of the host running ASDM which will be permitted Telnet access through this security appliance interface.




---

**Note** This is not the IP address of the security appliance interface.

---

4. In the Mask list, select or enter a netmask for the IP address to be permitted Telnet access.




---

**Note** This is not a mask for the IP address of the security appliance interface.

---

5. To return to the previous Window, click one of the following buttons:
  - **OK**—Accepts changes and returns to the previous pane.
  - **Cancel**—Discards changes and returns to the previous pane.
  - **Help**—Provides more information.

### Deleting Telnet Rules

To delete a rule from the Telnet table, perform the following steps:

1. Select a rule from the Telnet rule table.
2. Click **Delete**.

### Applying Changes

Changes to the table made by Add, Edit, or Delete are not immediately applied to the running configuration. To apply or discard changes, click one of the following buttons:

1. **Apply**—Sends changes made in ASDM to the security appliance and applies them to the running configuration. Click **Save** to write a copy of the running configuration to Flash memory. Use the **File** menu to write a copy of the running configuration to Flash memory, a TFTP server, or a failover standby unit.
2. **Reset**—Discards changes and reverts to the information displayed before changes were made or the last time you clicked **Refresh** or **Apply**. After Reset, use **Refresh** to make sure that information from the current running configuration is displayed.

### Fields

- **Interface Name**—Select the interface to allow Telnet access to the security appliance.
- **IP Address**—Enter the IP address of the host or network permitted to Telnet to the security appliance.
- **Mask**—Enter the subnet mask of the host or network permitted to Telnet to the security appliance.

- OK—Accepts changes and returns to the previous pane.
- Cancel—Discards changes and returns to the previous pane.
- 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
•	•	•	•	—

## Virtual Access

The Virtual Access pane lets you configure a virtual Telnet server address on the security appliance to use for network access authentication.

Although you can configure network access authentication for any protocol or service, only HTTP, Telnet, or FTP provide an authentication challenge. A user must first authenticate with one of these services before other traffic requiring authentication is allowed through.

In some cases, you might not want to allow HTTP, Telnet, or FTP through the security appliance, but still need to authenticate other types of traffic. In those cases, you can create a virtual Telnet server on the security appliance. User connect to the security appliance using Telnet to the virtual Telnet IP address and the security appliance provides a Telnet prompt. When an unauthenticated user connects to the virtual Telnet IP address, the user is challenged for a username and password, and is then authenticated by the AAA server. Once authenticated, the user sees the message “Authentication Successful.” The user can then access other services that require authentication.

To log out from the security appliance, reconnect to the virtual IP address; you are prompted to log out.

### Fields

- Virtual Telnet Server—Enter the virtual Telnet server IP address.

### Modes

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

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

