

Managing System Policies

A system policy allows you to manage the following on your ASA FirePOWER module:

- audit log settings
- the mail relay host and notification address
- SNMP polling settings
- STIG compliance

See the following sections for more information:

- Creating a System Policy, page 43-1
- Editing a System Policy, page 43-2
- Applying a System Policy, page 43-2
- Deleting System Policies, page 43-3

Creating a System Policy

License: Any

When you create a system policy, you assign it a name and a description. Next, you configure the various aspects of the policy, each of which is described in its own section.

Instead of creating a new policy, you can export a system policy from another ASA FirePOWER module and then import it onto your ASA FirePOWER module. You can then edit the imported policy to suit your needs before you apply it. For more information, see Importing and Exporting Configurations, page B-1.

To create a system policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > System Policy**.

The System Policy page appears.

Step 2 Click **Create Policy**.

The Create Policy page appears.

Step 3 From the drop-down list, select an existing policy to use as a template for your new system policy.

Step 4 Type a name for your new policy in the **New Policy Name** field.

Step 5 Type a description for your new policy in the **New Policy Description** field.

Step 6 Click **Create**.

Your system policy is saved and the Edit System Policy page appears. For information about configuring each aspect of the system policy, see one of the following sections:

- Configuring Audit Log Settings, page 43-5
- Configuring a Mail Relay Host and Notification Address, page 43-6
- Configuring SNMP Polling, page 43-8
- Enabling STIG Compliance, page 43-9

Editing a System Policy

License: Any

You can edit an existing system policy. If you edit a system policy that is currently applied to an ASA FirePOWER module, reapply the policy after you have saved your changes. For more information, see Applying a System Policy, page 43-2.

To edit an existing system policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > System Policy**.

The System Policy page appears, including a list of the existing system policies.

Step 2 Click the edit icon ( ) next to the system policy that you want to edit.

The Edit Policy page appears. You can change the policy name and policy description. For information about configuring each aspect of the system policy, see one of the following sections:

- Configuring Audit Log Settings, page 43-5
- Configuring a Mail Relay Host and Notification Address, page 43-6
- Configuring SNMP Polling, page 43-8
- Enabling STIG Compliance, page 43-9

Note If you are editing a system policy applied to an ASA FirePOWER module, make sure you reapply the updated policy when you are finished. See Applying a System Policy, page 43-2.

Step 3 Click **Save Policy and Exit** to save your changes. The changes are saved, and the System Policy page appears.

Applying a System Policy

License: Any

You can apply a system policy to an ASA FirePOWER module. If a system policy is already applied, any changes you make do not take effect until you reapply it.

To apply a system policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > System Policy**.

The System Policy page appears.

Step 2 Click the apply icon ( ) next to the system policy that you want to apply.

Step 3 Click **Apply**.

The System Policy page appears. A message indicates the status of applying the system policy.

Deleting System Policies

License: Any

You can delete a system policy, even if it is in use. If the policy is still in use, it is used until a new policy is applied. Default system policies cannot be deleted.

To delete a system policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > System Policy**.

The System Policy page appears.

Step 2 Click the delete icon ( ) next to the system policy that you want to delete. To delete the policy, click **OK.**

The System Policy page appears. A pop-up message appears, confirming the policy deletion.

Configuring a System Policy

License: Any

You can configure various system policy settings. For information about configuring each aspect of the system policy, see one of the following sections:

- Configuring the Access List for Your Appliance, page 43-3
- Configuring Audit Log Settings, page 43-5
- Configuring a Mail Relay Host and Notification Address, page 43-6
- Configuring SNMP Polling, page 43-8
- Enabling STIG Compliance, page 43-9

Configuring the Access List for Your Appliance

License: Any

The Access List page allows you to control which computers can access your appliance on specific ports. By default, port 443 (Hypertext Transfer Protocol Secure, or HTTPS), which is used to access the web interface, and port 22 (Secure Shell, or SSH), which is used to access the command line, are enabled for any IP address. You can also add SNMP access over port 161. Note that you must add SNMP access for any computer you plan to use to poll for SNMP information.

Caution By default, access to the appliance is **not** restricted. To operate the appliance in a more secure environment, consider adding access to the appliance for specific IP addresses and then deleting the default `any` option.

The access list is part of the system policy. You can specify the access list either by creating a new system policy or by editing an existing system policy. In either case, the access list does not take effect until you apply the system policy.

Note that this access list does not also control external database access. For more information on the external database access list, see Enabling Cloud Communications, page 44-2.

To configure the access list:

Access: Admin

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > System Policy**.

The System Policy page appears.

Step 2 You have the following options:

- To modify the access list in an existing system policy, click the edit icon ( ) next to the system policy.
- To configure the access list as part of a new system policy, click **Create Policy**.

  Provide a name and description for the system policy as described in Creating a System Policy, page 43-1, and click **Save**.

In either case, the Access List page appears.

Step 3 Optionally, to delete one of the current settings, click the delete icon ( ).

The setting is removed.

Caution If you delete access for the IP address that you are currently using to connect to the appliance interface, and there is no entry for "`IP=any port=443`", you will lose access to the system when you apply the policy.

Step 4 Optionally, to add access for one or more IP addresses, click **Add Rules**.

The Add IP Address page appears.

Step 5 In the **IP Address** field, you have the following options, depending on the IP addresses you want to add:

- an exact IP address (for example, 192.168.1.101)
- an IP address block using CIDR notation (for example, 192.168.1.1/24)

  For information on using CIDR in the Firepower system, see IP Address Conventions, page 1-4.
- `any`, to designate any IP address

Step 6 Select **SSH**, **HTTPS**, **SNMP**, or a combination of these options to specify which ports you want to enable for these IP addresses.

Step 7 Click **Add**.

The Access List page appears again, reflecting the changes you made.

Step 8 Click **Save Policy and Exit**.

The system policy is updated. Your changes do not take effect until you apply the system policy. See Applying a System Policy, page 43-2 for more information.

Configuring Audit Log Settings

License: Any

You can configure the system policy so that the ASA FirePOWER module streams an audit log to an external host.

Note You must ensure that the external host is functional and accessible from the ASA FirePOWER module sending the audit log.

The sending host name is part of the information sent. You can further identify the audit log stream with a facility, a severity, and an optional tag. The ASA FirePOWER module does not send the audit log until you apply the system policy.

After you apply a policy with this feature enabled, and your destination host is configured to accept the audit log, the syslog messages are sent. The following is an example of the output structure:

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

where the local date, time, and hostname precede the bracketed optional tag, and the sending device name precedes the audit log message.

For example:

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3000: admin@10.1.1.2, Operations > Monitoring, Page
View
```

To configure the audit log settings:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > System Policy**.

The System Policy page appears.

Step 2 You have the following options:

- To modify the audit log settings in an existing system policy, click the edit icon ( ) next to the system policy.
- To configure the audit log settings as part of a new system policy, click **Create Policy**.

  Provide a name and description for the system policy as described in Creating a System Policy, page 43-1, and click **Save**.

Step 3 Click **Audit Log Settings**.

The Audit Log Settings page appears.

Step 4 Select **Enabled** from the **Send Audit Log to Syslog** drop-down menu. (The default setting is **Disabled**.)

Step 5 Designate the destination host for the audit information by using the IP address or the fully qualified name of the host in the **Host** field. The default port (514) is used.

Caution If the computer you configure to receive an audit log is not set up to accept remote messages, the host will not accept the audit log.

Step 6 Select a syslog facility from the **Facility** field.

Step 7 Select a severity from the **Severity** field.

Step 8 Optionally, insert a reference tag in the **Tag (optional)** field.

Step 9 To send regular audit log updates to an external HTTP server, select **Enabled** from the **Send Audit Log to HTTP Server** drop-down list. The default setting is **Disabled**.

Step 10 In the **URL to Post Audit** field, designate the URL where you want to send audit information. You must enter an URL that corresponds to a listener program that expects the HTTP POST variables as listed:

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- `result`
- `time`
- `tag` (if defined, as above)

Caution To allow encrypted posts, you must use an HTTPS URL. Note that sending audit information to an external URL may affect system performance.

Step 11 Click **Save Policy and Exit**.

The system policy is updated. Your changes do not take effect until you apply the system policy. See Applying a System Policy, page 43-2 for more information.

Configuring a Mail Relay Host and Notification Address

License: Any

You must configure a mail host if you plan to:

- email event-based reports
- email status reports for scheduled tasks
- email change reconciliation reports
- email data pruning notifications
- use email for intrusion event alerting

You can select an encryption method for the communication between appliance and mail relay host, and can supply authentication credentials for the mail server if needed. After configuring settings, you can test the connection between the appliance and the mail server using the supplied settings.

To configure a mail relay host:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > System Policy**.

The System Policy page appears.

Step 2 You have the following options:

- To modify the email settings in an existing system policy, click the edit icon ( ) next to the system policy.
- To configure the email settings as part of a new system policy, click **Create Policy**.

  Provide a name and description for the system policy as described in Creating a System Policy, page 43-1, and click **Save**.

Step 3 Click **Email Notification**.

The Configure Email Notification page appears.

Step 4 In the **Mail Relay Host** field, type the hostname or IP address of the mail server you want to use.

Note The mail host you enter must allow access from the appliance.

Step 5 Enter the port number to use on the email server in the **Port Number** field. Typical ports include 25, when using no encryption, 465, when using SSLv3, and 587, when using TLS.

Step 6 To select an encryption method, you have the following options:

- To encrypt communications between the appliance and the mail server using Transport Layer Security, select **TLS** from the **Encryption Method** drop-down list.
- To encrypt communications between the appliance and the mail server using Secure Socket Layers, select **SSLv3** from the **Encryption Method** drop-down list.
- To allow unencrypted communication between the appliance and the mail server, select **None** from the **Encryption Method** drop-down list.

Note that certificate validation is not required for encrypted communication between the appliance and mail server.

Step 7 Enter a valid email address in the **From Address** field for use as the source email address for messages sent by the appliance.

Step 8 Optionally, to supply a user name and password when connecting to the mail server, select **Use Authentication**. Enter a user name in the **Username** field. Enter a password in the **Password** field.

Step 9 To send a test email using the configured mail server, click **Test Mail Server Settings**.

A message appears next to the button indicating the success or failure of the test.

Step 10 Click **Save Policy and Exit**.

The system policy is updated. Your changes do not take effect until you apply the system policy. See Applying a System Policy, page 43-2 for more information.

Configuring SNMP Polling

License: Any

You can enable Simple Network Management Protocol (SNMP) polling of an appliance using the system policy. The SNMP feature supports use of versions 1, 2, and 3 of the SNMP protocol.

Note that enabling the system policy SNMP feature does not cause the appliance to send SNMP traps; it only makes the information in the MIBs available for polling by your network management system.

Note You must add SNMP access for any computer you plan to use to poll the appliance. For more information, see Configuring the Access List for Your Appliance, page 43-3. Note that the SNMP MIB contains information that could be used to attack your appliance. Cisco recommends that you restrict your access list for SNMP access to the specific hosts that will be used to poll for the MIB. Cisco also recommends you use SNMPv3 and use strong passwords for network management access.

To configure SNMP polling:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > System Policy**.

The System Policy page appears.

Step 2 You have the following options:

- To modify the SNMP polling settings in an existing system policy, click the edit icon ( ) next to the system policy.
- To configure the SNMP polling settings as part of a new system policy, click **Create Policy**.

  Provide a name and description for the system policy as described in Creating a System Policy, page 43-1, and click **Create**.

Step 3 If you have not already added SNMP access for each computer you plan to use to poll the appliance, do so now. For more information, see Configuring the Access List for Your Appliance, page 43-3.

Step 4 Click **SNMP**.

The SNMP page appears.

Step 5 From the **SNMP Version** drop-down list, select the SNMP version you want to use.

The drop-down list displays the version you selected.

Step 6 You have the following options:

- If you selected **Version 1** or **Version 2**, type the SNMP community name in the **Community String** field. Go to step 15.
- If you selected **Version 3**, click **Add User** to display the user definition page.

Step 7 Enter a username in the **Username** field.

Step 8 Select the protocol you want to use for authentication from the **Authentication Protocol** drop-down list.

Step 9 Type the password required for authentication with the SNMP server in the **Authentication Password** field.

Step 10 Retype the authentication password in the **Verify Password** field just below the **Authentication Password** field.

Step 11 Select the privacy protocol you want to use from the **Privacy Protocol** list, or select **None** to not use a privacy protocol.

Step 12 Type the SNMP privacy key required by the SNMP server in the **Privacy Password** field.

Step 13 Retype the privacy password in the **Verify Password** field just below the **Privacy Password** field.

Step 14 Click **Add**.

The user is added. You can repeat steps 6 through 13 to add additional users. Click the delete icon ( ) to delete a user.

Step 15 Click **Save Policy and Exit**.

The system policy is updated. Your changes do not take effect until you apply the system policy. See Applying a System Policy, page 43-2 for more information.

Enabling STIG Compliance

License: Any

Organizations within the United States federal government sometimes need to comply with a series of security checklists set out in Security Technical Implementation Guides (STIGs). The STIG Compliance option enables settings intended to support compliance with specific requirements set out by the United States Department of Defense.

Enabling STIG compliance does not guarantee strict compliance to all applicable STIGs.

When you enable STIG compliance, password complexity and retention rules for local shell access accounts change. In addition, you cannot use `ssh` remote storage when in STIG compliance mode.

Note that applying a system policy with STIG compliance enabled forces appliances to reboot. If you apply a system policy with STIG enabled to an appliance that already has STIG enabled, the appliance does not reboot. If you apply a system policy with STIG disabled to an appliance that has STIG enabled, STIG remains enabled and the appliance does not reboot.

Caution You cannot disable this setting without assistance from Support. In addition, this setting may substantially impact the performance of your system. Cisco does not recommend enabling STIG compliance except to comply with Department of Defense security requirements.

To enable STIG compliance:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > System Policy**.

The System Policy page appears.

Step 2 You have the following options:

- To modify the time settings in an existing system policy, click the edit icon ( ) next to the system policy.
- To configure the time settings as part of a new system policy, click **Create Policy**.

  Provide a name and description for the system policy as described in Creating a System Policy, page 43-1, and click **Save**.

Step 3 Click **STIG Compliance**.

The STIG Compliance page appears.

Step 4 If you want to *permanently* enable STIG compliance on the appliance, select **Enable STIG Compliance**.

Caution You cannot disable STIG compliance on an appliance after you apply a policy with STIG compliance enabled. If you need to disable compliance, contact Support.

Step 5 Click **Save Policy and Exit**.

The system policy is updated. Your changes do not take effect until you apply the system policy. See Applying a System Policy, page 43-2 for more information.

When you apply a system policy that enables STIG compliance to an appliance, note that the appliance reboots. Note that if you apply a system policy with STIG enabled to an appliance that already has STIG enabled, the appliance does not reboot.