

Platform Settings

Platform settings for Firewall Threat Defense devices configure a range of unrelated features whose values you might want to share among several devices. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.

- Platform settings policies, on page 1
- List requirements and prerequisites for platform settings policies, on page 2
- Manage platform settings policies, on page 2
- Configure ARP inspection, on page 4
- Configure a banner, on page 5
- Configure DNS server settings, on page 6
- Configure external authentication, on page 9
- Configure fragment settings, on page 15
- Configure HTTP access, on page 16
- Configure ICMP access, on page 17
- Configure Secure Shell (SSH) access, on page 18
- Configure an SMTP server, on page 20
- Configure SNMP for a security device, on page 21
- Configure SSL settings, on page 34
- Syslog, on page 38
- Configure timeouts, on page 56
- Synchronize time on FTD devices, on page 58
- Configure a time zone for a device, on page 59
- Configure UCAPL/CC compliance, on page 60
- Configure a performance profile, on page 61
- History for platform settings, on page 62

Platform settings policies

A platform settings policy is a shared set of features or parameters that

- define aspects of managed devices that are likely to be similar to other managed devices in a deployment, such as time settings and external authentication,
- enable configuration of multiple managed devices at once, providing consistency and streamlining management efforts, and

- apply changes to all managed devices where the policy is used, requiring creation and application of shared policies even for device-specific settings.

Platform settings policy reference information

Use platform settings policies to enforce security requirements, such as displaying a login banner message, and to manage device configurations efficiently.

- You can set a “No Unauthorized Use” message for appliance logins using platform settings policies.
- You can apply multiple platform settings policies to a single Firewall Management Center to accommodate different mail relay hosts or access lists.

Platform settings policy example

Your organization’s security policies may require that appliances display a “No Unauthorized Use” message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.

Multiple platform settings policy example

If your organization has different mail relay hosts that you use for different circumstances or if you want to test different access lists, you can create several platform settings policies and switch between them, rather than editing a single policy.

List requirements and prerequisites for platform settings policies

You must meet specific requirements and prerequisites before you configure Platform Settings Policies, including supported domains and user roles.

Supported domains

Any

User roles

Admin

Access Admin

Network Admin

Manage platform settings policies

Manage platform settings policies to control device configurations and assignments within your environment. This task allows you to create, edit, or delete policies for supported device types.

Use the **Platform Settings** page (**Devices** > **Platform Settings**) to manage platform settings policies. This page indicates the type of device for each policy. The **Status** column shows the device targets for the policy.

Procedure

Step 1 Choose **Devices** > **Platform Settings**.

Step 2 For an existing policy, you can **Copy** (), **Edit** (), or **Delete** ( ) the policy.

Caution
You should not delete a policy that is the last-deployed policy on any of its target devices, even if it is out of date. Before you delete the policy completely, it is a good practice to deploy a different policy to those targets.

Step 3 To create a new policy, click **New Policy**.

a) Choose a device type from the drop-down list:

- **Firepower Settings** to create a shared policy for managed Classic devices.
- **Threat Defense Settings** to create a shared policy for managed Firewall Threat Defense devices.

b) Enter a **Name** for the new policy and optionally, a **Description**.

c) Optionally, choose the **Available Devices** where you want to apply the policy and click **Add** (or drag and drop) to add the selected devices. You can enter a search string in the **Search** field to narrow the list of devices.

d) Click **Save**.

- When you have selected a device and if the device is already applied with a policy, the **Confirm PFS Overwrite** dialog appears. To override the applied policy, click **OK**. The selected device is applied with the new policy.
- The system creates the policy and opens it for editing.

Step 4 To change the target devices for a policy, click **Edit** () next to the platform settings policy that you want to edit.

a) Click **Policy Assignment**.

b) To assign a device, high-availability pair, or device group to the policy, select it in the **Available Devices** list and click **Add**. You can also drag and drop.

c) To remove a device assignment, click **Delete** ( ) next to a device, high-availability pair, or device group in the **Selected Devices** list.

d) Click **OK**.

After completing these steps, platform settings policies are created, edited, or deleted as needed, and device assignments are updated accordingly.

What to do next

- Deploy configuration changes; see Deploy configuration changes.

Configure ARP inspection

Configure ARP inspection to ensure that only valid ARP packets are accepted on your network, reducing the risk of ARP spoofing and related attacks.

- Apply ARP inspection policies to specific interfaces and security zones.
- Add static ARP entries for enhanced control and security.

By default, all ARP packets are allowed between bridge group members. You can control the flow of ARP packets by enabling ARP inspection.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

ARP inspection ensures that an attacker cannot send an ARP response with the attacker MAC address, so long as the correct MAC address and the associated IP address are in the static ARP table.

When you enable ARP inspection, the Firewall Threat Defense device compares the MAC address, IP address, and source interface in all ARP packets to static entries in the ARP table, and takes the following actions:

- If the IP address, MAC address, and source interface match an ARP entry, the packet is passed through.
- If there is a mismatch between the MAC address, the IP address, or the interface, then the Firewall Threat Defense device drops the packet.
- If the ARP packet does not match any entries in the static ARP table, then you can set the Firewall Threat Defense device to either forward the packet out all interfaces (flood), or to drop the packet.



Note The dedicated Diagnostic interface never floods packets even if this parameter is set to flood.

Use this task when you need to protect your network from ARP spoofing by validating ARP packets and controlling ARP traffic on selected interfaces and zones.

Use ARP inspection in environments where network security is a priority and static ARP entries are needed.

Before you begin

Make sure you have device access and permission to edit platform settings and ARP inspection policies.

- Have the list of interfaces and security zones where ARP inspection will be applied.
- Prepare the static ARP entries that you intend to add.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **ARP Inspection**.

Step 3 Add entries to the ARP inspection table.

a) Click **Add** to create a new entry, or click **Edit** if the entry already exists.

b) Select the desired options.

- **Inspect Enabled**—To perform ARP inspection on the selected interfaces and zones.
- **Flood Enabled**—Floods ARP requests that do not match static ARP entries to all interfaces except the originating or dedicated management interface. By default, this behavior is enabled.

  If you choose not to flood ARP requests, only requests that match static ARP entries are allowed.
- **Security Zones**—Add the zones that contain the interfaces on which to perform the selected actions. The zones must be switched zones. For interfaces not in a zone, type the interface name into the field in the Selected Security Zone list and click **Add**. The device applies these rules only if it includes the selected interfaces or zones.

c) Click **OK**.

Step 4 Add static ARP entries according to Add a static ARP entry.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

ARP inspection is enabled on the selected interfaces and security zones. Only valid ARP packets are accepted, and static ARP entries are enforced. The policy is active after deployment.

Configure a banner

Configure a banner to display messages to users when they connect to the device command line interface (CLI). This helps inform users and discourage unauthorized access.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Banner**.

Step 3 Configure the banner.

These are some tips and requirements for banners.

- Use only ASCII characters. You can add line returns (press Enter), but do not use tabs.
- You can dynamically add the hostname or domain name of the device by including the variables **$(hostname)** or **$(domain)**.
- Although banners do not have an absolute length restriction, Telnet or SSH sessions close if the system does not have enough memory to process banner messages.

- Create a banner that discourages unauthorized access by avoiding the words "welcome" or "please," which may seem inviting. The sample banner provided discourages intruders.

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk criminal charges.
```

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

The system displays the banner to users when they connect to the device CLI. The changes occur after you deploy the policy.

Configure DNS server settings

Configure DNS server settings to enable hostname resolution for data traffic on managed devices. This task allows you to set up DNS server groups, trusted DNS services, and interface-specific DNS lookups. These configurations support features such as access control rules, NAT, and application detection.

- Set up DNS server groups for resolving FQDNs used in data traffic.
- Configure trusted DNS servers for DNS snooping and application-based PBR.
- Enable DNS lookups on specific interfaces to control routing behavior.

The Domain Name System (DNS) servers are used to resolve hostnames to IP addresses. Data DNS settings apply to services that use FQDNs, such as access control rules and remote access VPN. Special management traffic uses separate DNS settings configured via CLI commands. This procedure applies only to data DNS servers. For management DNS settings, see the CLI **configure network dns servers** and **configure network dns searchdomains** commands.

Managed devices use routing lookups to determine the correct interface for DNS server communications. The system selects the routing table based on the interfaces enabled for DNS. Multiple DNS server groups can be configured to resolve different DNS domains, allowing internal and external DNS resolution as needed.

Trusted DNS servers

You can configure trusted DNS services for DNS snooping. DNS snooping is used to map the application domains to IPs in order to detect the application on the first packet. You can also include the already configured servers in DNS group, DHCP pool, DHCP relay and DHCP client as trusted DNS servers.

For application-based PBR, configure trusted DNS servers. Ensure DNS traffic passes through Firewall Threat Defense in clear text format (because encrypted DNS is not supported) for domain resolution and application detection.

Before you begin

- Ensure you have created one or more DNS server groups. For more information, see Create a DNS server group object.
- Ensure you have created interface objects to connect to the DNS servers.

- Ensure that the managed device has appropriate static or dynamic routes to access the DNS servers.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit a Threat Defense policy.

Step 2 Click **DNS**, and then click the **DNS Settings** tab.

Step 3 Check **Enable DNS name resolution by device**.

Step 4 Configure the DNS server groups.

a) Do any of these actions in the DNS server group list:

- To add a group, click **Add**. You cannot add another group once there are 30 filter domains configured within the existing list of server groups.
- To edit a group, click **Edit** ( ) next to the group.
- To remove a group, click **Delete** ( ) next to the group. When you remove a group, you do not delete the DNS server group object. You remove it only from this list.

b) When adding or editing a group, configure the following settings, then click **OK**:

- **Select DNS Group**—Select an existing DNS server group object, or click + to create a new one.
- **Make as default**—Select this option to make this group the default group. Any DNS resolution request that does not match the filters for other groups will be resolved using the servers in this group.
- **Filter Domains**—For non-default groups only, enter a list of domain names separated by commas, such as example.com,example.net. Do not include spaces.

  The group is used only for DNS resolutions for these domains. You can enter up to 30 separate domains across all groups in this DNS platform settings policy. Each domain name can contain up to 127 characters.

  Note that these filter domains are not related to the default domain name for the group. The filter list can be different from the default domain.

Step 5 (Optional) Enter the **Expiry Entry Timer** and **Poll Timer** values in minutes.

These options apply to FQDNs specified in network objects only and do not apply to FQDNs used in other features.

- **Expire Entry Timer** specifies the minimum time-to-live (TTL) value for the DNS entry, in minutes. If the expiration timer is longer than the entry's TTL, the TTL is increased to the expire entry time value. If the TTL is longer than the expiration timer, the expire entry time value is ignored. Upon expiration, the entry is removed from the DNS lookup table. When you remove an entry, the device recompiles the table. Frequent removals can increase the processing load on the device. Some DNS entries can have very short TTL (as short as three seconds); use this setting to virtually extend the TTL. The default is 1 minute. The range is 1 to 65535 minutes.

  For systems running 7.0 or earlier, the expiration time is actually added to the TTL; it does not specify a minimum value.

- **Poll Timer** specifies the time limit after which the device queries the DNS server to resolve the FQDN defined in a network object. An FQDN is resolved periodically when either the poll timer has expired or the TTL of the resolved IP entry has expired, whichever occurs first.

Step 6 Enable DNS lookups on all interfaces or on specific interfaces. These choices also affect which routing tables are used.

Enabling DNS lookups on an interface is not the same as specifying the source interface for lookups. The Firewall Threat Defense always uses a route lookup to determine the source interface.

- No interfaces selected—This setting enables DNS lookups on all interfaces, including Management and management-only interfaces. The Firewall Threat Defense checks the data routing table, and if no route is found, falls back to the management-only routing table.
- Specific interfaces selected but not the **Enable DNS Lookup via diagnostic interface also** option—Enables DNS lookups on the specified interfaces. The Firewall Threat Defense checks the data routing table only.
- Specific interfaces selected plus the **Enable DNS Lookup via diagnostic interface also** option—Enables DNS lookups on the specified interfaces and the Diagnostic interface. The Firewall Threat Defense checks the data routing table, and if no route is found, falls back to the management-only routing table.
- Only the **Enable DNS Lookup via diagnostic interface also** option—Enables DNS lookups on Diagnostic. The Firewall Threat Defense checks only the management-only routing table. Be sure to configure an IP address for the Diagnostic interface on the **Devices** > **Device Management** > **edit device** > **Interfaces** page.

Step 7 Configure Trusted DNS servers.

a) Click the **Trusted DNS Servers** tab.
b) By default, the existing DNS servers that are configured in DHCP pool, DHCP relay, DHCP client, or DNS server group are included as trusted DNS servers. If you want to exclude any of them, uncheck the appropriate check boxes.
c) To add trusted DNS servers, under **Specify DNS Servers**, click **Edit**.
d) In the **Select DNS Servers** dialog box, either choose a host object as the trusted DNS server or directly specify the IP address of the trusted DNS server:

1. To choose existing host objects, under **Available Host Objects**, select the required host object and click **Add** to include it to **Selected DNS Servers**. For information on adding the host objects, see Create a network object.
2. To directly provide the IP address (IPv4 or IPv6) of the trusted DNS server, enter the address in the given text field, and click **Add** to include it to **Selected DNS Servers**.
3. Click **Save**. The added DNS servers are displayed in the **Trusted DNS Servers** page.

Note
You can configure a maximum of 12 DNS servers per policy.

To search for a DNS server that was added, using either the host name or the IP address, use the search field under **Specify DNS Servers**.

Step 8 Click **Save**.

What to do next

To use FQDN objects for access control rules, create an FQDN network object which can then be assigned to an access control rule. For instructions, see Create a network object.

Configure external authentication

Configure external authentication to allow management users to be authenticated using an LDAP or RADIUS server, as specified in an external authentication object. Centralized user management also enhances security for device access.



Note You must have administrator privileges to perform this task.

When you enable external authentication for management users, the Firewall Threat Defense verifies the user credentials with an LDAP or RADIUS server as specified in an external authentication object.

Sharing External Authentication Objects

External authentication objects can be used by the Firewall Management Center and Firewall Threat Defense devices. You can share the same object between the Firewall Management Center and devices. Alternatively, create separate objects. Note that the Firewall Threat Defense supports defining users on the RADIUS server, while the Firewall Management Center requires you to predefine the user list in the external authentication object. You can choose to use the predefined list method for the Firewall Threat Defense, but if you want to define users on the RADIUS server, you must create separate objects for the Firewall Threat Defense and the Firewall Management Center.



Note The timeout range is different for the Firewall Threat Defense and the Firewall Management Center, so if you share an object, be sure not to exceed the Firewall Threat Defense's smaller timeout range (1 to 30 seconds for LDAP, and 1 to 300 seconds for RADIUS). If you set the timeout to a higher value, the Firewall Threat Defense external authentication configuration will not work.

Assigning External Authentication Objects to Devices

For the Firewall Management Center, enable the external authentication objects directly on **System** (⚙) > **Users** > **External Authentication**; this setting only affects Firewall Management Center usage, and it does not need to be enabled for managed device usage. For Firewall Threat Defense devices, you must enable the external authentication object in the platform settings that you deploy to the devices, and you can only activate one external authentication object per policy. An LDAP object with CAC authentication enabled cannot also be used for CLI access. Be sure that both the Firewall Threat Defense and the Firewall Management Center can reach the LDAP server, even if you are not sharing the object. The Firewall Management Center is essential to retrieving the user list and downloading it to the device.

Firewall Device Supported Fields

Only a subset of fields in the external authentication object are used for Firewall Threat Defense SSH access. If you fill in additional fields, they are ignored. If you also use this object for the Firewall Management Center, those fields will be used. This procedure only covers the supported fields for the Firewall Threat Defense.

For other fields, see *Configure External Authentication for the Firewall Management Center* in the *Cisco Secure Firewall Management Center Administration Guide*.

Usernames

Usernames must be Linux-valid usernames and be lowercase only, using alphanumeric characters plus period (.) or hyphen (-). Special characters such as at sign (@) and slash (/) are not supported. You cannot add these default internal users for external authentication—**root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, ntp, lldpd, bind, dhcp, qemu, rpcuser, rpc, sshd, radiusd, messagebus, admin, mysql, www, sfrna, snorty, sfsnort, sfremediation, nobody, samdme, extuser, p2puser, rloginUser**. You can only add external users (as part of the External Authentication object) in the Firewall Management Center; you cannot add them at the CLI. Note that internal users can only be added at the CLI, not in the Firewall Management Center.

If you previously configured the same username for an internal user using the **configure user add** command, the Firewall Threat Defense first checks the password against the internal user, and if that fails, it checks the AAA server. Note that you cannot later add an internal user with the same name as an external user; only pre-existing internal users are supported. For users defined on the RADIUS server, be sure to set the privilege level to be the same as any internal users; otherwise you cannot log in using the external user password.

Privilege Level

LDAP users always receive Config privileges. You can define RADIUS users as either config or basic users.

Before you begin

- SSH access is enabled by default on the management interface. To enable SSH access on data interfaces, see Configure Secure Shell (SSH) access, on page 18. SSH is not supported to the Diagnostic interface.
- Inform RADIUS users of the following behavior to set their expectations appropriately:
  - The first time an external user logs in, Firewall Threat Defense creates the required structures but cannot simultaneously create the user session. The user simply needs to authenticate again to start the session. The user will see a message similar to this: "New external username identified. Please log in again to start a session."
  - If the user's Service-Type attribute is not defined or incorrectly configured in the RADIUS server and you use the RADIUS-defined users for authentication, the user will see a message similar to this: "Your username is not defined with a service type that is valid for this system. You are not authorized to access the system?".

    In some cases, the SSH clients close the CLI window on an unsuccessful SSH connection, even before displaying the failure message. Hence, ensure that the user's Service-Type attribute is correctly defined in the RADIUS server.
  - Similarly, if the user’s Service-Type authorization was changed since the last login, the user will need to re-authenticate. The user will see a message similar to this: "Your authorization privilege has changed. Please log in again to start a session."

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **External Authentication**, and then click the **Manage External Authentication Server** link.

You can also open the External Authentication screen by clicking **System** > **Users** > **External Authentication**.

Step 3 Click **Add External Authentication Object**.

Step 4 Configure an LDAP Authentication Object.

Step 5 Configure a RADIUS Authentication Object.

Step 6 Return to **System** (⚙) > **Users** > **External Authentication**.

Step 7 Click **Refresh** (↻) to view any newly-added objects.

For LDAP when you specify SSL or TLS encryption, you must upload a certificate for the connection; otherwise, the server will not be listed on this window.

Step 8 Click **Slider enabled** (⬭) next to the External Authentication object you want to use. You can only enable one object.

Step 9 Click **Save**; deploy configuration changes (see Deploy configuration changes).

After completing this task, external authentication is enabled for management users. The system verifies user credentials with the configured LDAP or RADIUS server and grants access based on the authentication object and user privileges.

Configure an LDAP External Authentication Object

Configure external authentication to allow management users to be authenticated using an LDAP server.

Note You must have administrator privileges to perform this task.

Procedure

Step 1 In the **External Authentication Object** page, select **LDAP** from the **Authentication Method** drop-down list and enter appropriate values in these fields:

a) Enter a **Name**.

b) (Optional) Enter **Description**.

Step 2 Choose a **Server Type** from the drop-down list.

Step 3 For the **Primary Server** enter these values:

a) Enter a **Host Name/IP Address**.

Note
If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used in this field. In addition, IPv6 addresses are not supported for encrypted connections.

b) Change the **Port** from the default.

Step 4 Enter the **Backup Server** parameters.

Step 5 Enter **LDAP-Specific Parameters**.

- **Base DN**—Enter the base distinguished name for the LDAP directory you want to access. For example, to authenticate names in the Security organization at the Example company, enter `ou=security,dc=example,dc=com`. Alternatively click **Fetch DNs**, and choose the appropriate base distinguished name from the drop-down list.
- (Optional) **Base Filter**—For example, if the user objects in a directory tree have a `physicalDeliveryOfficeName` attribute and users in the New York office have an attribute value of `NewYork` for that attribute, to retrieve only users in the New York office, enter `(physicalDeliveryOfficeName=NewYork)`.
- **User Name**—Enter a distinguished name for a user who has sufficient credentials to browse the LDAP server. For example, if you are connecting to an OpenLDAP server where user objects have a `uid` attribute, and the object for the administrator in the Security division at our example company has a `uid` value of `NetworkAdmin`, you might enter `uid=NetworkAdmin,ou=security,dc=example,dc=com`.
- **Password** and **Confirm Password**—Enter and confirm the password for the user.
- (Optional) **Show Advanced Options**—Configure the following advanced options.
  - **Encryption**—Click **None**, **TLS**, or **SSL**.

    Note
    If you change the encryption method after specifying a port, you reset the port to the default value for that method. For **None** or **TLS**, the port resets to the default value of 389. If you choose SSL encryption, the port resets to 636.

  - **SSL Certificate Upload Path**—For SSL or TLS encryption, you must choose a certificate by clicking **Choose File**.
  - (Not Used) **User Name Template**—Not used by the Firewall Threat Defense.
  - **Timeout**—Enter the number of seconds before rolling over to the backup connection between 1 and 30. The default is 30.

    Note
    The timeout range is different for the Firewall Threat Defense and the Firewall Management Center, so if you share an object, be sure not to exceed the Firewall Threat Defense's smaller timeout range (1-30 seconds). If you set the timeout to a higher value, the Firewall Threat Defense external authentication configuration will not work.

Step 6 (Optional) Set the **CLI Access Attribute** if you want to use a shell access attribute other than the user distinguished type. For example, on a Microsoft Active Directory Server, use the `sAMAccountName` shell access attribute to retrieve shell access users by typing `sAMAccountName` in the **CLI Access Attribute** field.

Step 7 Set the **CLI Access Filter**.

Choose one of these methods:

- To use the same filter you specified when configuring authentication settings, choose **Same as Base Filter**.
- To retrieve administrative user entries based on attribute value, enter the attribute name, a comparison operator, and the attribute value you want to use as a filter, enclosed in parentheses. For example, if all network administrators have a `manager` attribute which has an attribute value of `shell`, you can set a base filter of `(manager=shell)`.

The names on the LDAP server must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Step 8 Click **Save**.

Step 9 For LDAP, if you later add or delete users on the LDAP server, you must refresh the user list and redeploy the Platform Settings.

a) Choose **System** (⚙) > **Users** > **External Authentication**.

b) Click **Refresh** (↻) next to the LDAP server.

If the user list changed, you will see a message advising you to deploy configuration changes for your device. The Firepower Theat Defense Platform Settings will also show that it is "Out-of-Date on *x* targeted devices."

c) Deploy configuration changes; see Deploy configuration changes.

Configure a RADIUS Authentication Object

Configure external authentication to allow management users to be authenticated using a RADIUS server

Note You must have administrator privileges to perform this task.

Procedure

Step 1 In the **External Authentication Object** page, select **RADIUS** from the **Authentication Method** drop-down list and enter appropriate values in these fields:

a) Check the **Enabled Message Authenticator** check box to require the Message-Authenticator attribute in all RADIUS responses, ensuring that every response from the RADIUS server is securely verified by the Firewall Threat Defense.

This feature is enabled by default for new RADIUS servers. We recommend you enable it for existing servers after the upgrade. Disabling message authenticators may expose your firewalls to potential attacks. Ensure that your RADIUS server has the Message-Authenticator configuration.

b) Define users on the RADIUS server using the Service-Type attribute.

This is the list of supported values for the Service-Type attribute:

- Administrator (6)—Provides Config access authorization to the CLI. These users can use all commands in the CLI.

- NAS Prompt (7) or any level other than 6—Provides Basic access authorization to the CLI. These users can use read-only commands, such as **show** commands, for monitoring and troubleshooting purposes.

The names must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Alternatively, you can predefine users in the external authentication object (see Step Configure external authentication, on page 9). To use the same RADIUS server for the Firewall Threat Defense and Firewall Management Center while using the Service-Type attribute method for the Firewall Threat Defense, create two external authentication objects that identify the same RADIUS server: one object includes the predefined **CLI Access Filter** users (for use with the Firewall Management Center), and the other object leaves the **CLI Access Filter** empty (for use with Firewall Threat Defenses).

c) Enter a **Name** and optional **Description**.

Step 2 For the **Primary Server**, enter a **Host Name/IP Address**.

Note
If you are using a certificate to connect via TLS or SSL, the host name in the certificate must match the host name used in this field. In addition, IPv6 addresses are not supported for encrypted connections.

Step 3 (Optional) Change the **Port** from the default.

Step 4 Enter a **RADIUS Secret Key**.

Step 5 (Optional) Enter the **Backup Server** parameters.

Step 6 Enter **RADIUS-Specific Parameters**.

- **Timeout (Seconds)**—Enter the number of seconds before rolling over to the backup connection. The default is 30.
- **Retries**—Enter the number of times the primary server connection should be tried before rolling over to the backup connection. The default is 3.

Step 7 (Optional) Enter a comma-separated list of usernames in the **Administrator CLI Access User List** field. For example, enter `jchrichton, aerynsun, rygel`.

You may want to use the **CLI Access Filter** method for Firewall Threat Defense so you can use the same external authentication object with Firewall Threat Defense and other platform types. Note that if you want to use RADIUS-defined users, you must leave the **CLI Access Filter** empty.

Make sure that these usernames match usernames on the RADIUS server. The names must be Linux-valid usernames:

- Maximum 32 alphanumeric characters, plus hyphen (-) and underscore (_)
- All lowercase
- Cannot start with hyphen (-); cannot be all numbers; cannot include a period (.), at sign (@), or slash (/)

Note

If you want to only define users on the RADIUS server, you must leave this section empty.

Step 8 Click **Save**.

Configure fragment settings

Configure fragment settings to manage the handling of fragmented IP packets on your Firewall Threat Defense device. These settings help prevent Denial of Service (DoS) attacks and ensure applications that require packet fragmentation operate properly.

- Set limits for the number of fragments per packet and for fragments awaiting reassembly.
- Set the timeout for fragment reassembly.
- Allow fragments only if your network applications require them.

By default, the Firewall Threat Defense device allows up to 24 fragments per IP packet. It also allows up to 200 fragments awaiting reassembly. Applications such as NFS over UDP may require fragmented packets, but attackers often use fragmented packets in Denial of Service (DoS) attacks.

These settings establish the defaults for devices assigned this policy. You can override these settings for specific interfaces on a device by selecting **Override Default Fragment Setting** in the interface configuration. When you edit an interface, you can find the option on **Advanced** > **Security Configuration**. Select **Devices** > **Device Management**, edit a Firewall Threat Defense device, and select **Interfaces** to edit interface properties.

- Allow fragments only if required by your network applications.
- Override the default settings for specific interfaces when your configuration requires it.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Fragment Settings**.

Step 3 Configure the available options. To use the default settings, click **Reset to Defaults**.

- **Size (Block)**—The maximum number of packet fragments from all connections collectively that can be waiting for reassembly. The default value is 200 fragments. (One fragment equals one packet segment.)
- **Chain (Fragment)**—The maximum number of packets into which a full IP packet can be fragmented. The default is 24 packets. Set this option to one to disallow fragments.
- **Timeout (Sec)**—The maximum number of seconds to wait for an entire fragmented packet to arrive. The default is five seconds. If all fragments are not received within this time, all fragments are discarded.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

Deploy the policy to activate the new fragment settings on assigned devices. Monitor device performance and change fragment settings as needed.

Configure HTTP access

You can enable the HTTPS server to provide a health check mechanism for a cloud load balancer, for example, for the Firewall Threat Defense Virtual on AWS using an Application Load Balancer.

Use HTTPS with the Firewall Threat Defense only as described for health checks and management. You cannot configure the Firewall Threat Defense through a web interface in this management mode.

Configure HTTP access only on data interfaces, including interfaces you set as management-only. Use only data interfaces for HTTP access, not the dedicated Management interface. The physical management interface is shared between the Diagnostic logical interface and the Management logical interface. This configuration affects only the Diagnostic logical interface (when used) and other data interfaces. The Management logical interface is separate from the other interfaces on the device. Use the Management interface only to set up and register your device to the Firewall Management Center. It has a separate IP address and static routing.

Configure HTTPS access as described in this section. An access rule for the host IP address is not required.

Use HTTPS only on a reachable interface. If your HTTPS host is on the outside interface, initiate the management connection directly to it.

Before you begin

- Configure HTTPS and AnyConnect VPN module of Cisco Secure Client on separate TCP ports if both features are required on the same interface. For example, assign a different port to HTTPS, such as port 4443.
- Create network objects to define the hosts or networks that are allowed for HTTPS connections. You can add these objects as part of this procedure. If you plan to use object groups for IP addresses, ensure the groups exist in the rules. Select **Objects** > **Object Management** to configure objects.



Note Use the **any-ipv4** or **any-ipv6** network object group instead of the system-provided **any** object.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **HTTP**.

Step 3 Check the **Enable HTTP Server** check box to enable the HTTP server.

Step 4 (Optional) Change the HTTP port. The default is 443.

Step 5 Identify the interfaces and IP addresses that allow HTTP connections.

Allow HTTP connections only from specific interfaces and client IP addresses by configuring this table. You may use network addresses instead of individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.
b) Configure the rule properties:

- **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make HTTP connections. Choose an object from the drop-down menu, or click + to add a new network object.
- **Security Zones**—Add the zones that contain the interfaces to which you will allow HTTP connections. For interfaces not in a zone, type the interface name into the field under the selected **Selected Security Zones** list. Then click **Add**. The device applies these rules only if it includes the selected interfaces or zones.

c) Click **OK**.

Step 6 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After you complete this task, the device enables HTTP access on the specified interfaces and IP addresses. Use secure connections for health checks or management.

Configure ICMP access

By default, you can send ICMP packets to any interface using either IPv4 or IPv6, with these exceptions:

- The Firewall Threat Defense does not respond to ICMP echo requests directed to a broadcast address.
- The Firewall Threat Defense only responds to ICMP traffic sent to the interface that traffic comes in on; you cannot send ICMP traffic through an interface to a far interface.

To protect the device from attacks, you can use ICMP rules to limit ICMP access to interfaces to particular hosts, networks, or ICMP types. ICMP rules function like access rules, where the rules are ordered, and the first rule that matches a packet defines the action.

If you configure any ICMP rule for an interface, an implicit deny ICMP rule is added to the end of the ICMP rule list, changing the default behavior. Thus, if you want to simply deny a few message types, you must include a permit any rule at the end of the ICMP rule list to allow the remaining message types.

We recommend that you always grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP path MTU discovery, which can halt IPsec and PPTP traffic. Additionally ICMP packets in IPv6 are used in the IPv6 neighbor discovery process.

Before you begin

Make sure the required objects exist before you configure rules. Select **Objects** > **Object Management** to configure objects. Create network objects or groups to specify the hosts or networks, and port objects to specify the ICMP message types you want to control.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **ICMP**.

Step 3 Configure ICMP rules.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

- **Action**—Whether to permit (allow) or deny (drop) matching traffic.
- **ICMP Service**—The port object that identifies the ICMP message type.
- **Network**—The network object or groupthat identifies the hosts or networks whose access you are controlling.
- **Security Zones**—Add the zones that contain the interfaces that you are protecting. If an interface is not in a zone, type the interface name into the field beneath the **Selected Security Zones** list, and click **Add**. A device applies these rules only if it includes the selected interfaces or zones.

c) Click **OK**.

Step 4 (Optional.) Set rate limits on ICMPv4 Unreachable messages.

- **Rate Limit**—Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.
- **Burst Size**—Sets the burst rate, between 1 and 10. The system sends this number of replies, but subsequent replies are not sent until the rate limit is reached.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

ICMP access rules take effect after you deploy the policy to the assigned devices. Your configuration permits or denies ICMP traffic for the hosts or networks you specified.

Configure Secure Shell (SSH) access

If you enabled Firewall Management Center access on a data interface, such as outside, you should enable SSH on that interface using this procedure. This section describes how to enable SSH connections to one or more *data* interfaces on the Firewall Threat Defense. SSH is not supported to the Diagnostic logical interface.

Note SSH is enabled by default on the Management interface; however, this screen does not affect Management SSH access.

To use SSH, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

Data vs. Management SSH

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firewall Management Center. SSH for data interfaces shares the internal and external user lists with SSH for the Management interface. Other settings are configured separately. For data interfaces, enable SSH and access lists using this screen. SSH traffic for data interfaces uses the regular routing configuration. Routing for the Management interface configured during setup or at the CLI is not used.

For the Management interface, to configure an SSH access list, see the **configure SSH-access-list** command in the *Cisco Secure Firewall Threat Defense Command Reference*. To configure a static route, see the **configure network static-routes** command. By default, you configure the default route through the Management interface at initial setup.

Interface Access

You can SSH only to a reachable interface; for example, if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface.

Ciphers and Key Exchange

SSH supports the following ciphers and key exchange:

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- Integrity—hmac-sha2-256
- Key exchange—dh-group14-sha256

SSH Stack

The Firewall Threat Defense uses the CiscoSSH stack, which is based on OpenSSH. CiscoSSH supports FIPS compliance and regular updates, including updates from Cisco and the open source community.

Maximum Attempts

After you make three consecutive failed attempts to log into the CLI using SSH, the device terminates the SSH connection.

Before you begin

- You can configure SSH internal users at the CLI using the **configure user add** command; see Add an internal user at the CLI. By default, there is an **admin** user for which you configured the password during initial setup. You can also configure external users on LDAP or RADIUS by configuring **External Authentication** in platform settings. See Configure external authentication, on page 9.
- You need network objects that define the hosts or networks permitted to make SSH connections to the device. You can add objects during the procedure. If you want to use object groups to identify a group of IP addresses, make sure the required groups already exist in the rules. Select **Objects** > **Object Management** to configure objects.



Note You cannot use the system-provided **any** network object. Instead, use **any-ipv4** or **any-ipv6**.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Secure Shell**.

Step 3 Identify the interfaces and IP addresses that allow SSH connections.

Use this table to limit which interfaces will accept SSH connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

- **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.
- **Security Zones**—Add the zones that contain the interfaces to which you will allow SSH connections. For interfaces not in a zone, you can type the interface name into the field below the **Selected Security Zones** list and click **Add**. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c) Click **OK**.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure an SMTP server

Configure an SMTP server to enable email alerts in Syslog. Ensure the source email address configured for Syslog is a valid account on the SMTP servers.

Before you begin

Ensure that the network objects for the primary and secondary SMTP server addresses exist. Define the objects using **Objects** > **Object Management**. You can also create these objects when you edit the policy.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **SMTP Server**.

Step 3 Select the network objects that identify the **Primary Server IP Address** and optionally, the **Secondary Server IP Address**.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing this task, email alerts can be sent through Syslog using the specified SMTP servers.

Configure SNMP for a security device

Configure SNMP monitoring to allow network management stations to monitor the health and status of Cisco security devices. This task enables centralized visibility and management of devices using SNMP.

- Enable SNMP so that SNMP management stations can monitor devices.
- SNMP versions 1, 2c, and 3, including traps and read access, are supported. SNMP write access is not supported.

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

SNMPv3 supports read-only users and encryption with DES(deprecated), 3DES, AES256, AES192, and AES128.

The DES option has been deprecated. If your deployment includes SNMP v3 users using DES encryption and that were created using a version earlier than 6.5, you can continue to use those users for Firewall Threat Defense devices running versions 6.6 or earlier. However, you cannot edit those users and retain DES encryption or create new users with DES encryption. If your Firewall Management Center manages any Firewall Threat Defense devices running Versions 7.0+, deploying a platform settings policy that uses DES encryption to those Firewall Threat Defense devices will fail.

Note

- You can configure SNMP only on Routed and Diagnostic interfaces.
- To create an alert to an external SNMP server, access **Policies** > **Actions** > **Alerts**.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **SNMP**.

Step 3 Enable SNMP, and configure basic options.

- **Enable SNMP Servers**—Whether to provide SNMP information to the configured SNMP hosts. You can deselect this option to disable SNMP monitoring while retaining the configuration information.
- **Read Community String**, **Confirm**—Enter the password used by a SNMP management station when sending requests to the Firewall Threat Defense device. The SNMP community string (also known as password) is a shared secret among the SNMP management stations and the network nodes. The security

device uses this password to determine if the incoming SNMP request is valid. The password is a case-sensitive alphanumeric string of up to 32 characters; spaces and special characters are not permitted.

- **System Administrator Name**—Enter the name of the device administrator or other contact person. This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Location**—Enter the location of this security device (for example, Building 42, Sector 54). This string is case-sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.
- **Port**—Enter the UDP port on which incoming requests will be accepted. The default is 161.

Step 4 (SNMPv3 only.) Add SNMPv3 users, on page 27.

Step 5 Add SNMP hosts, on page 30.

Step 6 Configure SNMP traps, on page 32.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

SNMP protocol

SNMP protocol is an application-layer protocol that

- facilitates the exchange of management information between network devices, and
- is part of the TCP/IP protocol suite.

SNMP protocol support and access

Firewall Threat Defense provides support for network monitoring using SNMP Versions 1, 2c, and 3, and supports the use of all three versions simultaneously. The SNMP agent runs on the Firewall Threat Defense interface. You can monitor network devices using management systems (NMSs) such as OpenView network management system. Firewall Threat Defense supports SNMP read-only access with a GET request. SNMP does not support write access or the SNMP SET request, so you cannot make changes with SNMP.

You can configure the Firewall Threat Defense to send traps, which are messages sent to the management station when certain events occur. These messages are called event notifications. You can also use the NMS to browse Management Information Bases (MIBs) on the security devices. MIBs are collections of definitions, and the Firewall Threat Defense maintains a database of values for each definition. To browse a MIB, issue a series of GET-NEXT or GET-BULK requests from the NMS to the MIB tree to get values.

The SNMP agent sends a notification to your management station when a specified event occurs, such as a network link going up or down. The notification includes an SNMP OID, which identifies the source device. The agent also replies when your management station requests information.

List SNMP terminology

This reference lists and defines the terms that are commonly used when working with SNMP.

Table 1: SNMP terminology

Term	Description
Agent	The SNMP server running on the Secure Firewall Threat Defense. The SNMP agent has these features: • responds to requests for information and actions from the network management station. • ontrols access to its Management Information Base, the collection of objects that the SNMP manager can view or change. • does not allow SET operations.
Browsing	Monitoring the health of a device from the network management station by polling required information from the SNMP agent on the device. This activity may include issuing a series of GET-NEXT or GET-BULK requests of the MIB tree from the network management station to determine values.
Management Information Bases (MIBs)	Standardized data structures for collecting information about packets, connections, buffers, failovers, and other items. MIBs are defined by the product, protocols, and hardware standards used by most network devices. SNMP network management stations can browse MIBs and request specific data or events be sent as they occur.
Network management stations (NMSs)	The PCs or workstations SET up to monitor SNMP events and manage devices.
Object identifier (OID)	The system that identifies a device to its NMS and indicates to users the source of information monitored and displayed.
Trap	Predefined events that generate a message from the SNMP agent to the NMS. Events include alarm conditions such as link-up, link-down, cold-start, warm-start, authentication events, or syslog messages. **coldStart**—The coldStart trap occurs when the SNMP agent starts after the SNMP configuration. This trap also occurs when the agent starts after a system reboot. **Note** For cluster and HA nodes, after a reload, if the interface reboot time exceeds 5 minutes (preset threshold), the trap is dropped. When the cluster and HA nodes have rebooted successfully, all other traps are sent as expected. The **SNMP-server enable traps SNMP coldstart** command is used to enable and disable transmission of these traps.

Describe MIBs and traps

MIBs are either standard or enterprise-specific. Standard MIBs are created by the IETF and described in various RFCs. Traps report significant events, such as errors or failures, on a network device. SNMP traps can be defined in standard or enterprise-specific MIBs. The IETF also creates standard traps, documented in various RFCs. SNMP traps are compiled into ASA software.

If needed, you can also download RFCs, standard MIBs, and standard traps from these locations:

http://www.IETF.org/

Browse the SNMP Object Navigator to look up Cisco MIBs, traps, and OIDs from this location:

https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do?local=en

In addition, download Cisco OIDs by FTP from this location:

ftp://FTP.cisco.com/pub/mibs/oid/oid.tar.gz

List of supported tables and objects in MIBs

This reference lists the supported tables and objects for the specified MIBs, including details for each MIB such as counters, OIDs, and descriptions.

Remote Access VPN polling

Table 2: CISCO-REMOTE-ACCESS-MONITOR-MIB

Counter	OID	Description
Active Sessions	crasNumSessions (1.3.6.1.4.1.9.9.392.1.3.1)	The number of currently active sessions.
Users	crasNumUsers (1.3.6.1.4.1.9.9.392.1.3.3)	The number of users who have active sessions.
Peak Sessions	crasNumPeakSessions (1.3.6.1.4.1.9.9.392.1.3.41)	The number of peak RA sessions since system up.

Site-to-site VPN tunnel polling

Table 3: CISCO-REMOTE-ACCESS-MONITOR-MIB

Counter	OID	Description
LAN to LAN Sessions	crasL2LNumSessions (1.3.6.1.4.1.9.9.392.1.3.29)	The number of currently active LAN to LAN sessions.
Peak LAN to LAN Sessions	crasL2LPeakConcurrentSessions (1.3.6.1.4.1.9.9.392.1.3.31)	The number of peak concurrent LAN to LAN sessions since the system is up.

Connection polling

Table 4: CISCO-FIREWALL-MIB

Counter	OID	Description
Active Connections	cfwConnectionActive (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.6)	The number of connections currently in use by the entire firewall.

Counter	OID	Description
Peak Connections	cfwConnectionPeak (1.3.6.1.4.1.9.9.147.1.2.2.2.1.3.40.7)	The highest number of connections in use at any one time since system startup.
Connections Per Second	cfwConnectionPerSecond (1.3.6.1.4.1.9.9.147.1.2.2.3)	The current connections per second rate on the firewall.
Peak Connections Per Second	cfwConnectionPerSecondPeak (1.3.6.1.4.1.9.9.147.1.2.2.4)	The highest number of connections per second on the firewall since system startup.

NAT translation polling

Table 5: CISCO-NAT-EXT-MIB

Counter	OID	Description
Active Translations	cneAddrTranslationNumActive (1.3.6.1.4.1.9.9.532.1.1.1.1)	The total number of address translation entries that are currently available in the NAT device. This indicates the aggregate of the translation entries created from both the static and dynamic address translation mechanisms.
Peak Active Translations	cneAddrTranslationNumPeak (1.3.6.1.4.1.9.9.532.1.1.1.2)	The maximum number of address translation entries that are active at any one time since system startup. This value indicates the high watermark of address translation entries active at any one time since system startup. This object includes the translation entries created from both the static and dynamic address translation mechanisms.

Routing table entries polling

Table 6: IP-FORWARD-MIB

Counter	OID	Description
Active Translations	inetCidrRouteNumber (1.3.6.1.2.1.4.24.6)	The total number of current inetCidrRouteTable entries that are valid.

Interface duplex status polling

Table 7: CISCO-IF-EXTENSION-MIB

Counter	OID	Description
Duplex Status	cieIfDuplexCfgStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.20)	This object specifies the configured duplex status for the given interface.
Detected Duplex Status	cieIfDuplexDetectStatus (1.3.6.1.4.1.9.9.276.1.1.2.1.21)	This object specifies the detected duplex status for the given interface.

Snort 3 intrusion EVENT rate polling

Table 8: CISCO-UNIFIED-FIREWALL-MIB

Counter	OID	Description
Snort 3 Intrusion event Rate	cufwAaicIntrusionEvtRate (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	The rate at which intrusion events were recorded by Snort on this firewall, averaged over the last 300 seconds.

BGP peer-flap trap notification

Table 9: BGP4-MIB

Counter	OID	Description
BGP Peer-flap	bgpBackwardTransition (1.3.6.1.4.1.9.9.491.1.5.3.2.1)	The BGPBackwardTransition event is generated when the BGP FSM moves from a higher numbered state to a lower numbered state.

CPU utilization polling

Table 10: CISCO-PROCESS-MIB

Counter	OID	Description
CPU Total Utilization	cpmCPUTotal1minRev (1.3.6.1.4.1.9.9.109.1.1.1.1.7.1)	Total system CPU utilization for the last one minute.
Individual CPU Core Utilization	Associated parameters and values of cpmCPUTotal1minRev 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 to 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	Individual CPU core utilization values for the last one minute, where 'n' represents the number of cores. Examples: • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) - Aggregate system CPU utilization % (This value is the same as the system CPU usage from .3.6.1.4.1.9.9.109.1.1.1.1.7.1 in single context mode). • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) - Snort average CPU utilization % (total aggregate value of all snort instances) • 3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) - System PROCESS average % (average of "Sysproc" cores)

Note The SNMP OIDs 1.3.6.1.2.1.25.3.3 and 1.3.6.1.2.1.25.3.4 pertaining to CPU monitoring (hrProcessorTable and hrNetworkTable) were removed on ASA FirePOWER. You can view and MONITOR the CPU health details of the device only through its device manager.

Add SNMPv3 users

Add SNMPv3 users to provide secure, authenticated, and encrypted SNMP management access to your device. This task ensures that only authorized users can access SNMPv3 features using specified authentication and encryption algorithms.

You create users for SNMPv3 only. These steps are not applicable for SNMPv1 or SNMPv2c.

Note SNMPv3 only supports read-only users.

SNMP users have a specified username, an authentication password, an encryption password, and authentication and encryption algorithms to use.

Note If you add a new cluster unit or replace a High Availability unit when using SNMPv3 with clustering or High Availability, SNMPv3 users are not replicated to the new unit. Remove the users, add them again, and redeploy your configuration to replicate users to the new unit.

The authentication algorithm options are MD5 (deprecated, pre-6.5 only), SHA, SHA224, SHA256, and SHA384.

Note The MD5 option has been deprecated. If your deployment includes SNMP v3 users using the MD5 authentication algorithm that were created using a version previous to 6.5, you can continue to use those users for FTD devices running versions 6.7 and previous. However, you cannot edit those users and retain the MD5 authentication algorithm, or create new users with the MD5 authentication algorithm. If your management center manages any threat defenses running Versions 7.0+, deploying a platform settings policy that uses the MD5 authentication algorithm to those threat defenses will fail.

The encryption algorithm options are DES (deprecated, pre-6.5 only), 3DES, AES256, AES192, and AES128.

Note The DES option has been deprecated. If your deployment includes SNMP v3 users using DES encryption that were created using a version previous to 6.5, you can continue to use those users for threat defenses running versions 6.7 and previous. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption. If your management center manages any threat defenses running Versions 7.0+, deploying a platform settings policy that uses DES encryption to those threat defenses will fail.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Choose **SNMP** > **Users** tab.

Step 3 Click **Add** and completed the following:

a) Select the security level for the user from the **Security Level** drop-down list.

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

b) Enter the name of the SNMP user in the **Username** field. Usernames must be 32 characters or fewer.

c) Select the type of password, you want to use in the **Encryption Password Type** drop-down list. Choose from:

- **Clear text**—The Firewall Threat Defense device will still encrypt the password when deploying to the device.
- **Encrypted**—The Firewall Threat Defense device will directly deploy the encrypted password.

d) In the **Auth Algorithm Type** drop-down list, select the type of authentication you want to use: SHA, SHA224, SHA256, or SHA384.

Note
The MD5 option has been deprecated. If your deployment includes SNMP v3 users using the MD5 authentication algorithm that were created using a version previous to 6.5, you can continue to use those users for FTD devices running versions 6.7 and previous. However, you cannot edit those users and retain the MD5 authentication algorithm, or create new users with the MD5 authentication algorithm. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy that uses the MD5 authentication algorithm to those Firewall Threat Defenses will fail.

e) In the **Authentication Password** field, enter the password to use for authentication. If you selected Encrypted as the Encrypt Password Type, the password must be formatted as xx:xx:xx..., where xx are hexadecimal values.

Note
The length of the password will depend on the authentication algorithm selected. For all passwords, the length must be 256 characters or less.

If you selected Clear Text as the Encrypt Password Type, repeat the password in the **Confirm** field.

f) In the **Encryption Type** drop-down list, select the type of encryption you want to use: AES128, AES192, AES256, 3DES.

Note
To use AES or 3DES encryption, you must have the appropriate license installed on the device.

Note
The DES option has been deprecated. If your deployment includes SNMP v3 users using DES encryption that were created using a version previous to 6.5, you can continue to use those users for Firewall Threat Defenses running versions 6.7 and previous. However, you cannot edit those users and retain DES encryption, or create new users with DES encryption. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy that uses DES encryption to those Firewall Threat Defenses will fail.

g) Enter the password to use for encryption in the **Encryption Password** field. If you selected Encrypted as the Encrypt Password Type, the password must be formatted as xx:xx:xx..., where xx are hexadecimal values. For encrypted passwords, the length of the password depends on the encryption type selected. The password sizes are as follows. Each xx is one octal.:

- AES 128 requires 16 octals
- AES 192 requires 24 octals
- AES 256 requires 32 octals

- 3DES requires 32 octals
- DES can be any size

Note
For all passwords, the length must be 256 characters or fewer.

If you selected Clear Text as the Encrypt Password Type, repeat the password in the **Confirm** field.

Step 4 Click **OK**.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing these steps, SNMPv3 users are added with the specified authentication and encryption settings. The device is now configured for secure SNMPv3 management access.

Add SNMP hosts

Define SNMP hosts and their communication parameters to enable SNMP management stations to access and monitor the device. This task allows you to specify which hosts are permitted and how they communicate with the device.

Use Host to add or edit entries in the SNMP Hosts table on the SNMP page. These entries represent SNMP management stations allowed to access the Firewall Threat Defense device.

You can add up to 8192 hosts. Only 128 of this number can be for traps.

Before you begin

Ensure that the network objects that define the SNMP management stations exist. Select **Device** > **Object Management** to configure network objects.

Note The supported network objects include IPv6 hosts, IPv4 hosts, IPv4 range and IPv4 subnet addresses.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Choose **SNMP** > **Hosts** tab.

Step 3 Click **Add** and completed the following:

a) In the **IP Address** field, either enter a valid IPv6 or IPv4 host or select the network object that defines the SNMP management station's host address.

The IP address can be an IPv6 host, IPv4 host, IPv4 range or IPv4 subnet.

b) Select the appropriate SNMP version from the **SNMP version** drop-down list.

c) (SNMPv3 only.) Select the username of the SNMP user that you configured from the **User Name** drop-down list.

Note
You can associate up to 23 SNMP users per SNMP host.

d) (SNMPv1, 2c only.) In the **Read Community String** field, enter the community string that you have already configured, for read access to the device. Re-enter the string to confirm it.

Note
This string is required, only if the string used with this SNMP station is different from the one already defined in the **Enable SNMP Server** section.

e) Select the type of communication between the device and the SNMP management station. You can select both types. Choose from:

- **Poll**—The management station periodically requests information from the device.
- **Trap**—The device sends trap events to the management station as they occur.

Note
When the SNMP host IP address is either an IPv4 range or an IPv4 subnet, you can configure either **Poll** or **Trap**, not both.

f) In the **Port** field, enter a UDP port number for the SNMP host. The default value is 162. The valid range is 1 to 65535.

g) Select the interface type for communication between the device and the SNMP management station under the **Reachable By** options. You can select either the Management interface of the device or an available security zone/named interface. Choose from:

- **Device Management Interface**—Communication between the device and the SNMP management station occurs over the Management interface.
  - When you choose this interface for SNMPv3 polling, all configured SNMPv3 users are allowed to poll and are not restricted to the user chosen in 3.c, on page 31. Here, SNMPv1 and SNMPv2c are not allowed from an SNMPv3 host.
  - When you choose this interface for SNMPv1 and SNMPv2c polling, the polling is not restricted at all to the version selected in 3.b, on page 30.
- **Security Zones or Named Interface**—Communication between the device and the SNMP management station occurs over a security zone or interface.
  - Search for zones in the **Available Zones** field.
  - Add the zones that contain the interfaces through which the device communicates with the management station to the **Selected Zone/Interface** field. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zone/Interface** list and click **Add**. The host will be configured on a device only if the device includes the selected interfaces or zones.

Note
VTI tunnel interfaces are not supported for SNMP.

Step 4 Click **OK**.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Configure SNMP traps

Use SNMP traps to configure event notifications for Firewall Threat Defense. Traps are unsolicited notifications sent from the device to the management station for certain events, such as linkup, linkdown, and syslog event generation. Each SNMP trap includes an object ID (OID) for your device.

Some traps are not applicable to certain hardware models. These traps will be ignored if you apply the policy to one of these models. For example, not all models have field-replaceable units, so the **Field Replaceable Unit Insert/Delete** trap will not be configured on those models.

SNMP traps are defined in standard MIBs or in enterprise-specific MIBs. Standard traps are created by the IETF and documented in various RFCs. The Firewall Threat Defense software includes SNMP traps.

If needed, you can download RFCs, standard MIBs, and standard traps from http://www.IETF.org/.

Browse the complete list of CISCO MIBs, traps, and OIDs using the SNMP Object Navigator on the Cisco website: SNMP Object Navigator.

In addition, download CISCO OIDs by FTP: ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **SNMP** > **SNMP Traps** to configure SNMP traps (event notifications) for the Firewall Threat Defense device.

Step 3 Select the appropriate Enable Traps options. You can select either or both options.

a) Check **Enable All SNMP Traps** to select all traps in the subsequent four sections.

b) Check **Enable All Syslog Traps** to enable transmission of trap-related syslog messages.

Note
SNMP traps are of higher priority than other notification messages because they are expected to be near real-time. When you enable all SNMP or syslog traps, it is possible for the SNMP process to consume excess resources in the agent and in the network, causing the system to hang. If you notice system delays, unfinished requests, or timeouts, you can selectively enable SNMP and syslog traps. You can also limit the rate at which syslog messages are generated by severity level or message ID. For example, all syslog message IDs that begin with the digits 212 are associated with the SNMP class; see Configure syslog rate limits, on page 51.

Step 4 The event-notification traps in the **Standard** section are enabled by default for an existing policy:

- **Authentication** – Unauthorized SNMP access. This authentication failure occurs for packets with an incorrect community string.
- **Link Up** – One of the device's communication links has become available (it has "come up"), as indicated in the notification.
- **Link Down** – One of the device's communication links has failed, as indicated in the notification.

- **Cold Start** – The device is reinitializing itself such that its configuration or the protocol entity implementation may be altered.
- **Warm Start** – The device is reinitializing itself such that its configuration and the protocol entity implementation is unaltered.

Step 5 Select the desired event-notification traps in the **Entity MIB** section:

- **Field Replaceable Unit Insert** – A Field Replaceable Unit (FRU) has been inserted, as indicated. (FRUs include assemblies such as power supplies, fans, processor modules, interface modules, etc.)
- **Field Replaceable Unit Delete** – A Field Replaceable Unit (FRU) has been removed, as indicated in the notification
- **Configuration Change** – There has been a hardware change, as indicated in the notification

Step 6 Select the desired event-notification traps in the **Resource** section:

- **Connection Limit Reached** – This trap indicates that a connection attempt was rejected because the configured connections limit has been reached.

Step 7 Select the desired event-notification traps in the **Other** section:

- **NAT Packet Discard** – This notification is generated when IP packets are discarded by the NAT function. Available Network Address Translation addresses or ports have fallen below configured threshold.
- **CPU Rising Threshold** – This notification is generated when rising CPU utilization exceeds a predefined threshold for a configured period of time. Check this option to enable CPU rising threshold notifications:
  - **Percentage** – The default value is 70% for the high threshold notification; the range is 10 to 94%. The critical threshold is 95%.
  - **Period** – The default monitoring period is 1 minute; the range is 1 to 60 minutes.
- **Memory Rising Threshold** – This notification is generated when rising memory utilization exceeds a predefined threshold, thus reducing available memory. Check this option to enable memory rising threshold notifications:
  - **Percentage** – The default value is 70% for the high threshold notification; the range is 50 to 95%.
- **Failover** – This notification is generated when there is a change in the failover state as reported by the CISCO-UNIFIED-FIREWALL-MIB.
- **Cluster** – This notification is generated when there is a change in the cluster health as reported by the CISCO-UNIFIED-FIREWALL-MIB.
- **Peer Flap** – This notification is generated when there is BGP route flapping, a situation in which BGP systems send an excessive number of update messages to advertise network reachability information.

Step 8 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing this task, SNMP traps are configured on the Firewall Threat Defense device, and event notifications will be sent to the management station for the selected events. This enables proactive monitoring and timely response to device events.

Configure SSL settings

This task enables you to configure SSL settings for remote access VPN sessions, allowing you to specify protocol versions, security levels, and available algorithms to ensure secure communication.

You must have administrator privileges and be in a leaf domain to perform this task.

Make sure that you are running a fully licensed version of the Secure Firewall Management Center. The SSL Settings are disabled if you are running Secure Firewall Management Center in evaluation mode. SSL Settings are also disabled if the licensed Secure Firewall Management Center version does not meet the export-compliance criteria. If you are using Remote Access VPN with SSL, your Smart Account must have the strong-crypto features enabled. For more information, see *License Types and Restrictions* in the *Cisco Secure Firewall Management Center Administration Guide*.

Before you begin

Ensure you have administrator privileges and are in a leaf domain. Verify that you are running a fully licensed version of the management center with strong-crypto features enabled if using Remote Access VPN with SSL.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit a Firewall Threat Defense policy.

Step 2 Select **SSL**.

Step 3 Add entries to the **Add SSL Configuration** table.

a) Click **Add** to create a new entry, or click **Edit** if the entry already exists.

b) Select the required security configurations from the drop-down list.

- **Protocol Version**—Specifies the TLS protocols to be used while establishing remote access VPN sessions.
- **Security Level**—Indicates the kind of security positioning you would like to set up for the SSL.

Step 4 Select the **Available Algorithms** based on the protocol version that you select and click **Add** to include them for the selected protocol. For more information, see Configure SSL settings, on page 35.

The algorithms are listed based on the protocol version that you select. Each security protocol identifies a unique algorithm for setting up the security level.

Step 5 Click **OK** to save the changes.

What to do next

Select **Deploy** > **Deployment** and click **Deploy** to deploy the policy to the assigned devices.

Configure SSL settings

The Firewall Threat Defense device uses the Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS) to support secure message transmission for Remote Access VPN connection from remote clients. The SSL Settings window lets you configure SSL versions and encryption algorithms that will be negotiated and used for message transmission during remote VPN access over SSL.

Note Though you configure Firewall Management Center and Firewall Threat Defense to operate in a security certifications (UCAPL, CC, or FIPS) compliance mode, the Firewall Management Center allows configuration of unsupported ciphers. For example, in a FIPS enabled mode, management center allows configuring DH Group 5 which is not FIPS-compliant. However, VPN tunnel does not negotiate due to the non-compliant cipher usage.

Configure the SSL Settings at this location:

Devices > **Platform Settings**, and then click **SSL**.

Fields

Minimum SSL Version as Server—Specify the minimum SSL/TLS protocol version that the Firewall Threat Defense device uses when acting as a server. For example, when it functions as a Remote Access VPN Gateway.

TLS Version—Select one of these TLS versions from the drop-down list:

TLS V1	Accepts SSLv2 client hellos and negotiates TLSv1 (or greater).
TLSV1.1	Accepts SSLv2 client hellos and negotiates TLSv1.1 (or greater).
TLSV1.2	Accepts SSLv2 client hellos and negotiates TLSv1.2 (or greater).
TLSV1.3	Accepts SSLv2 client hellos and negotiates TLSv1.3 (or greater).

Note TLS 1.3 in remote access VPN requires Cisco Secure Client, Version 5.0 and above.

DTLS Version—Select the DTLS versions from the drop-down list, based on the selected TLS version. By default, DTLSv1 is configured on Firewall Threat Defense devices, you can choose the DTLS version as per your requirement.

Note Ensure that the TLS protocol version is higher than or equal to the DTLS protocol version selected. TLS protocol versions support these DTLS versions:

TLS V1	DTLSv1
TLSV1.1	DTLSv1

TLSV1.2	DTLSv1, DTLSv1.2
TLSV1.3	DTLSv1, DTLSv1.2

Diffie-Hellman Group—Choose a group from the drop-down list. Available options are Group1 - 768-bit modulus, Group2 - 1024-bit modulus, Group5 - 1536-bit modulus, Group14 - 2048-bit modulus, 224-bit prime order, and Group24 - 2048-bit modulus, 256-bit prime order. The default is Group1.

Elliptical Curve Diffie-Hellman Group—Choose a group from the drop-down list. Available options are Group19 - 256-bit EC, Group20 - 384-bit EC, and Group21 - 521-bit EC. The default value is Group19.

TLSv1.2 adds support for these ciphers:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

Note
ECDSA and DHE ciphers are the highest priority.

TLSv1.3 adds support for these ciphers:

- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_256_GCM_SHA384

The SSL configuration table can be used to specify the protocol version, security level, and Cipher algorithms that you want to support on the Secure Firewall Threat Defense devices.

Protocol Version—Lists the protocol version that the Secure Firewall Threat Defense device supports and uses for SSL connections. Available protocol versions are:

- Default
- TLSV1
- TLSV1.1
- TLSV1.2
- TLSV1.3
- DTLSv1
- DTLSv1.2

Security Level—Lists the cipher security levels that Firewall Threat Defense device supports and uses for SSL connections.

If you have Firewall Threat Defense devices with evaluation license, the security level is Low by default. With Firewall Threat Defense smart license, the default security level is High. You can choose one of these options to configure the required security level:

- **All** includes all ciphers, including NULL-SHA.
- **Low** includes all ciphers, except NULL-SHA.
- **Medium** includes all ciphers, except NULL-SHA, DES-CBC-SHA, RC4-SHA, and RC4-MD5 (this is the default).
- **FIPS** includes all FIPS-compliant ciphers, except NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, and DES-CBC3-SHA, TLS_CHACHA20_POLY1305_SHA256.
- **High** includes only AES-256 with SHA-2 ciphers and applies to TLS version 1.2 and the *default* version.
- **Custom** includes one or more ciphers that you specify in the Cipher algorithms/custom string box. This option provides you with full control of the cipher suite using OpenSSL cipher definition strings.

Cipher Algorithms/Custom String—Lists the cipher algorithms that the Firewall Threat Defense device supports and uses for SSL connections. For more information about ciphers using OpenSSL, see https://www.openssl.org/docs/apps/ciphers.html

Ciphers supported by TLSv1.2 only

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384

- DHE-RSA-AES256-SHA256
- AES256-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- AES128-SHA256



Note ECDSA and DHE ciphers are the highest priority.

Ciphers not supported by TLSv1.1 or TLSv1.2

- RC4-SHA
- RC4-MD5
- DES-CBC-SHA
- NULL-SHA

Syslog

Logging information

Logging information can help you identify and isolate network or device configuration problems.

- System logging (syslog) can be enabled for Firewall Threat Defense devices.
- Some security events can be sent to a syslog server.

Syslog messages

A syslog message is a log event that

- collects messages from devices to a server running a syslog daemon
- enables aggregation of logs and alerts for centralized management, and
- provides protected long-term storage for logs, supporting troubleshooting and incident handling.

System log configuration details

Devices can send their log messages to a UNIX-style syslog service. A syslog service accepts messages and either stores them in files or prints them, based on a simple configuration file.

Table 11: System logs for Secure Firewall Threat Defense

Logs related to	Details	Configure in
Device and system health, network configuration	This syslog configuration generates messages for features running on the data plane, that is, features that are defined in the CLI configuration that you can view with the **show running-config** command. This includes features such as routing, VPN, data interfaces, DHCP server, NAT, and so forth. Data plane syslog messages are numbered, and they are the same as those generated by devices running ASA software. However, Secure Firewall Threat Defense does not necessarily generate every message type that is available for ASA Software. For information on these messages, see *Cisco Secure Firewall Threat Defense syslog messages* at https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html. This configuration is explained in these topics.	**Platform settings**
Security events	This syslog configuration generates alerts for file and malware, connection, Security Intelligence, and intrusion events. For details, see *About sending syslog messages for security events* and subtopics in the *Cisco Secure Firewall Management Center Administration Guide*.	**Platform settings** and the **Logging** in an access control policy
(All devices) Policies, rules, and events	This syslog configuration generates alerts for access control rules, intrusion rules, and other advanced services as described in *Configurations supporting alert responses* in the *Cisco Secure Firewall Management Center Administration Guide*. These messages are not numbered. For information on configuring this type of syslog, see *Creating a syslog alert response* in the *Cisco Secure Firewall Management Center Administration Guide*.	**alert responses** and the **Logging** in an access control policy

You can set up multiple syslog servers and control the messages and events sent to each server. You can also configure varied destinations, such as console, email, or internal buffer.

Syslog message severity levels

The syslog message severity levels define the importance of system messages.

Table 12: Syslog message severity levels

Level Number	Severity Level	Description
0	**emergencies**	You cannot use the system.
1	**alert**	You need to take immediate action.
2	**critical**	The system has critical conditions to be addressed.
3	**error**	Error conditions.
4	**warning**	The system has warnings you should review.
5	**notification**	The system reports significant events you should monitor.
6	**informational**	Informational messages only.
7	**debugging**	The system generates only debugging messages Log at this level only temporarily, when debugging issues. This log level can generate many messages, which might affect system performance.

Note Firewall Threat Defense does not generate syslog messages with a severity level of zero (emergencies).

Syslog message filters

Syslog message filter criteria

You can direct syslog messages to an output destination according to these criteria:

- Syslog message ID number

  (This does not apply to syslog messages for security events such as connection and intrusion events.)

- Syslog message severity level
- Syslog message class (equivalent to a functional area)

  (This rule does not apply to syslog messages for security events, including connection and intrusion events.)

You can create a message list with specific criteria, which you can then specify as the output destination is set. Alternatively, you can configure the Firewall Threat Defense device to send a particular message class to each type of output destination independently of the message list.

(Message lists do not apply to syslog messages for security events such as connection and intrusion events.)

Syslog message classes and associated message ID numbers

Note This topic does not apply to messages for security events (connection, intrusion, etc.)

You can use syslog message classes in two ways:

- Specify an output location for an entire category of syslog messages.
- Create a message list that specifies the message class.

Use the syslog message class to categorize syslog messages by type, such as features or functions of the device. For example, use the RIP class for RIP routing.

Syslog messages in the same class have the same three initial digits in their message ID numbers. For example, the syslog messages for the VPN client feature use ID numbers 611101 to 611323.

Most ISAKMP syslog messages include prepended objects that identify the tunnel. When available, these objects appear before the descriptive text of a syslog message. If the object is unknown when the syslog message is generated, the heading and value combination is omitted.

The objects are prefixed in this manner:

Group = *groupname*, Username = *user*, IP = *IP_address*

The term 'group' here refers to the tunnel-group configuration. The username is from the local database or AAA server. The IP address is the public IP address of the remote access client or Layer 2 peer.

See the message classes and the range of message ID numbers in each class in this table.

Table 13: Syslog message classes and associated message ID numbers

Class	Definition	Syslog Message ID Numbers
auth	User Authentication	109, 113
—	Access Lists	106
—	Application Firewall	415
—	Botnet Traffic Filtering	338
bridge	Transparent Firewall	110, 220
ca	PKI Certification Authority	717
citrix	Citrix Client	723
—	Clustering	747
—	Card Management	323
config	Command Interface	111, 112, 208, 308
csd	Secure Desktop	724

Class	Definition	Syslog Message ID Numbers
cts	Cisco TrustSec	776
dap	Dynamic Access Policies	734
EAP, eapoudp	EAP or EAPoUDP for Network Admission Control	333, 334
EIGRP	EIGRP Routing	336
email	E-mail Proxy	719
—	Environment Monitoring	735
ha	Failover	101, 102, 103, 104, 105, 210, 311, 709
—	Identity-based Firewall	746
ids	Intrusion Detection System	400, 733
—	IKEv2 Toolkit	750, 751, 752
IP	IP Stack	209, 215, 313, 317, 408
ipaa	IP Address Assignment	735
ips	Intrusion Protection System	400, 401, 420
—	IPv6	325
—	Licensing	444
MDM-proxy	MDM Proxy	802
NAC	Network Admission Control	731, 732
nacpolicy	NAC Policy	731
nacsettings	NAC Settings to apply NAC Policy	732
—	NAT and PAT	305
—	Network Access Point	713
NP	Network Processor	319
—	NP SSL	725
OSPF	OSPF Routing	318, 409, 503, 613
—	Password Encryption	742
—	Phone Proxy	337
RIP	RIP Routing	107, 312

Class	Definition	Syslog Message ID Numbers
rm	Resource Manager	321
—	Smart Call Home	120
session	User Session	106, 108, 201, 202, 204, 302, 303, 304, 305, 314, 405, 406, 407, 500, 502, 607, 608, 609, 616, 620, 703, 710
SNMP	SNMP	212
—	ScanSafe	775
SSL	SSL Stack	725
svc	SSL VPN Client	722
sys	System	199, 211, 214, 216, 306, 307, 315, 414, 604, 605, 606, 610, 612, 614, 615,701, 711, 741
—	Threat Detection	733
tag-switching	Service Tag Switching	779
transactional-rule-engine-tre	Transactional Rule Engine	780
uc-IMS	UC-IMS	339
vm	VLAN Mapping	730
vpdn	PPTP and L2TP Sessions	213, 403, 603
VPN	IKE and IPsec	316, 320, 402, 404, 501, 602, 702, 713, 714, 715
vpnc	VPN Client	611
vpnfo	VPN Failover	720
vpnlb	VPN Load Balancing	718
—	VXLAN	778
webfo	WebVPN Failover	721
webvpn	WebVPN and Secure Client	716

Guidelines for logging

Restrictions for IPv6 logging

- IPv6 is supported. Syslog message can be sent using TCP or UDP.
- Ensure that the interface configured for sending syslogs is enabled, IPv6 capable, and the syslog server is reachable through the designated interface.
- You cannot use IPv6 for secure logging.

Syslog server configuration guidelines

- The syslog server must run a server program called syslogd. Windows includes a syslog server as part of its operating system.
- The syslog server operates based on the syslog-ng process of the firewall system. Do not use external configuration files, such as the *scwx.conf* file from SecureWorks. Because these files are not compatible with the device, using them causes parsing errors and the syslog-ng process fails.
- You can configure up to 16 syslog servers.
- Assign only one list or class to each syslog server and location.
- Do not configure Firewall Management Center as a primary syslog server. The Firewall Management Center can log some syslogs. However, it does not have adequate storage provision to accommodate large amounts of information from connection events for every sensor, especially when multiple sensors are used and all send syslogs.
- The syslog server should be reachable through the Firewall Threat Defense device. Configure the device to deny ICMP unreachable messages on the interface through which the syslog server is reachable, and to send syslogs to the same server. Enable logging for all severity levels. To prevent the syslog server from crashing, suppress the generation of syslogs 313001, 313004, and 313005.
- To view logs generated by the Firewall Threat Defense device, you must specify a logging output destination. If you enable logging without specifying a logging output destination, the Firewall Threat Defense device generates messages but does not save them to a location from which you can view them. You must specify each different logging output destination separately.
- The Firewall Threat Defense syslog supports one-way TLS for secure logging. It does not support client certificate authentication, trustpoint configuration for syslog, or mutual TLS (X.509 certificate authentication).

Interfaces for syslog configuration

- Determining the egress interface for the syslog:
  - If the specified management-only interface has management-access enabled, the management center will perform route table lookups and determine the egress interface (could be data or management) based on best routing logic.
  - If you configure a management-only interface as logging host, that does not have management-access enabled, the management center will use the interface regardless of routing table entries.

    Thus, for the management center to always uses a dedicated management path for syslog traffic, configure the management interface without management-access, and then specify the interface in the logging host:

    ```
    interface <management-interface>
    management-only ----->Do not include management-access
    ```

```
logging host <management-interface> <syslog-server-ip>
```

- When the syslog rate exceeds 50,000 messages per second, ensure that a data interface is used as egress interface rather than a management interface.
- Configure the data interface as the syslog source interface for production monitoring and auditing. Use the management interface only for temporary testing. This approach ensures optimal syslog reliability and prevents rate-limiting on the management interface.

TCP and UDP connections for syslog

- If you use TCP as the transport protocol, the system opens 4 connections to the syslog server to ensure that messages are not lost. If you collect messages from many devices and the combined connection overhead is too much for the server, use UDP instead.
- The number of UDP connections for syslog is directly related to the number of CPUs on the hardware platform and the number of syslog servers you configure. At any point in time, there can be as many UDP syslog connections as there are CPUs times the number of configured syslog servers. The global UDP connection idle timeout applies to these sessions, and the default duration is two minutes. You can adjust this setting to close sessions more quickly, but the timeout applies to all UDP connections, not just syslog. This is the intended behavior.
- When the Firewall Threat Defense device sends syslogs via TCP, the connection takes about one minute to initiate after the syslogd service restarts.
- When the TCP logging host goes down, it takes approximately six minutes to change its connection status from *Connected* to *Not connected*. Logging relies on TCP to detect the channel state; until then, logging sends the logs through the channel. During this time, when you execute the **show log**, the output would display the TCP logging host as connected. Once the TCP channel is closed, the TCP logging host state is updated to *Not connected*.

Configure syslog logging for Firewall Threat Defense devices

This task enables you to configure syslog logging for Firewall Threat Defense devices, allowing you to monitor and manage system events efficiently.

Syslog logging helps track security events and system activity on your devices. If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages.

See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 46 for more information about platform settings that apply to security event syslog messages.

Before you begin

See requirements in Guidelines for logging, on page 43.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **Syslog** from the table of contents.

Step 3 Click **Logging Setup** to enable logging, specify FTP server settings, and specify Flash usage. For more information, see Configure logging and basic settings, on page 47.

Step 4 Click **Logging Destinations** to enable logging to specific destinations and to specify filtering on message severity level, event class, or on a custom event list. For more information, see Enable logging destinations, on page 48.

You must enable a logging destination to see messages at that destination.

Step 5 Click **E-mail Setup** to specify the e-mail address that is used as the source address for syslog messages that are sent as e-mail messages. For more information, see Configure syslog messages to be sent to an e-mail address, on page 49.

Step 6 Click **Events List** to define a custom event list that includes an event class, a severity level, and an event ID. For more information, see Create a custom event list, on page 50.

Step 7 Click **Rate Limit** to specify the volume of messages being sent to all configured destinations and define the message severity level to which you want to assign rate limits. For more information, see Configure syslog rate limits, on page 51.

Step 8 Click **Syslog Settings** to specify the logging facility, enable the inclusion of a time stamp, and enable other settings to set up a server as a syslog destination. For more information, see Configure syslog settings, on page 52.

Step 9 Click **Syslog Servers** to specify the IP address, protocol used, format, and security zone for the syslog server that is designated as a logging destination. For more information, see Configure a syslog server, on page 54.

After you complete these steps, your Firewall Threat Defense device sends system events to the specified destinations for monitoring and analysis.

Firewall Threat Defense platform settings that apply to security event syslog messages

Security events include connection, Security Intelligence, intrusion, and file and malware events. Some syslog settings configured on the **Syslog** page and its tabs apply to syslog messages for security events. However, most settings only apply to messages for events related to system health and networking. This reference lists the settings that apply to syslog messages for security events.

Settings that apply to syslog messages for security events:

- **Logging Setup** tab:
  - **Send syslogs in EMBLEM format**
- **Syslog Settings** tab:
  - **Enable Timestamp on Syslog Messages**
  - **Timestamp Format**
  - **Enable Syslog Device ID**
- **Syslog Servers** tab:
  - All options on the **Add Syslog Server** form and the list of configured servers.

Configure logging and basic settings

Enable logging and configure syslog settings so the system generates and manages logs for data plane events. This setup ensures log data is archived and available for analysis or reporting.

Perform this task when you need to generate syslog messages for data plane events and manage log storage on your device. You can manipulate saved logging data. You can also specify actions for certain syslog messages, extract data for reporting, or track statistics using scripts.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 46.

Before you begin

- Determine where logs should be stored, such as an FTP server or flash memory.
- Understand the desired logging level (critical, alerts, emergencies, errors, etc)
- Identify if logging should be enabled on standby or failover units.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Logging Setup** in your device's configuration interface.

Step 3 Enable logging and configure basic logging settings.

- **Enable Logging**—Turns on the data plane system logging.
- **Enable Logging on the Failover Standby Unit**—Turns on logging for the standby device, if available.
- **Send syslogs in EMBLEM format**—Enables EMBLEM format logging for every logging destination. If you enable EMBLEM, you must use the UDP protocol to publish syslog messages. EMBLEM is not compatible with TCP.

  The EMBLEM syslog format is a Cisco-specific convention that is built upon the RFC 3164 and RFC 5424 standards. When EMBLEM is enabled, the syslog message prints a colon (:) after the <PRI> field, which differs from the RFC 5424 format.

  Note
  Syslog messages in RFC5424 format, typically displays the priority value (PRI). However, in Firewall Management Center, if you want to display the PRI value in the syslog messages of the managed Firewall Threat Defense device, ensure to enable the EMBLEM format. Also, the device ID does not appear in EMBLEM-formatted syslog messages.

- **Send debug messages as syslogs**—Redirects debug trace output to the syslog. The syslog message number is 711001 and the default logging level is set to debug. To view these messages, ensure logging is enabled at the console and configured for the debug syslog message number and level.
- **Memory Size of Internal Buffer**—Specify the size of the internal buffer to which syslog messages are saved if the logging buffer is enabled. When the buffer fills up, it is overwritten. The default is 4096 bytes. The range is 4096 to 52428800 bytes.

Step 4 (Optional) Configure the syslog message logging to the Firewall Management Center.

a) Enable VPN logging by checking the **Enable Logging to Secure Firewall Management Center** check box.

b) Choose the syslog severity level for the logging messages in the **Logging Level** drop-down list.

- The logging level for the VPN messages is set to **errors** by default.

  VPN troubleshooting syslogs can add excessive load on the Firewall Management Center. Hence, enable this option with caution. Also, when you configure a device with site-to-site or remote access VPN, it automatically enables sending VPN syslogs to the management center by default. We recommend that you limit the logging level to **error** and above to restrict the excessive flow of syslogs to the Firewall Management Center, especially in case of RAVPN, where multiple devices are involved.

For information on the levels, see Syslog message severity levels, on page 39.

Step 5 (Optional) Save log buffer contents to an FTP server before the buffer is overwritten.

- Enable **FTP Server Buffer Wrap** and enter the necessary destination information in the following fields.
- **IP Address**—Select the host network object that contains the IP address of the FTP server.
- **User Name**—Enter the username to use when connecting to the FTP server.
- **Path**—Enter the path, relative to the FTP root, where the buffer contents should be saved.
- **Password/ Confirm**—Enter and confirm the password used to authenticate the username to the FTP server.

Step 6 (Optional) Save log buffer contents to flash memory before overwriting.

- Check the **Flash** checkbox
- Specify **Maximum flash to be used by logging (KB)** (range: 4-8044176 KB).
- Specify **Minimum free space to be preserved (KB)** (range: 0-8044176 kilobytes.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Logging is enabled and syslog messages are generated and stored based on your configuration. Log data is archived as specified and is accessible for further analysis or reporting.

Enable logging destinations

Enable logging destinations to ensure that syslog messages are received at the specified destination. This task allows you to control which messages are sent by applying message filters to each destination.

To see messages at a logging destination, enable the destination and specify a message filter.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 46.

Before you begin

Before you begin, ensure you have access to the system and the necessary permissions to configure logging destinations.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Logging Destinations**.

Step 3 Click **Add** to enable a destination and apply a logging filter, or edit an existing destination.

Step 4 In the **Logging Destinations** dialog box, select a destination and configure the filter for that destination:

a) Choose the destination to enable in the **Logging Destination** drop-down list. You can create one filter for each destination. Examples include Console, E-Mail, Internal buffer, SNMP trap, SSH Sessions, and Syslog servers.

Note
Console and SSH session logging works in the diagnostic CLI only. Enter **system support diagnostic-CLI**.

b) In **Event Class**, choose the filter that will apply to all classes not listed in the table.

You can configure these filters:

- **Filter on severity** —Select the severity level. Messages at this level or higher are sent to the destination
- **Use Event List** —Select the event list that defines the filter. You create these lists on the **Event Lists** page.
- **Disable Logging** —Prevents messages from being sent to this destination.

c) To create filters for each event class, click **Add** for a new filter or edit an existing filter. Select the event class and severity level to limit messages in that class. Click **OK** to save the filter.

For an explanation of the event classes, see Syslog message classes and associated message ID numbers, on page 41.

d) Click **OK**.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing this task, the selected logging destinations will receive syslog messages according to the filters you have configured.

Configure syslog messages to be sent to an e-mail address

Enable syslog messages to be delivered as e-mails to designated recipients so administrators receive important system notifications directly through e-mail.

You can set up a list of recipients for syslog messages to be sent as e-mails.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 46.

Before you begin

- Configure an SMTP server on the platform settings page
- Configure logging and basic settings, on page 47
- Setup Email as the Logging Destination

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Email Setup**.

Step 3 Specify the e-mail address that is used as the source address for syslog messages that are sent as e-mail messages.

Step 4 Click **Add** to enter a new e-mail address recipient of the specified syslog messages.

Step 5 Set the desired severity level for syslog messages for each recipient.

The severity filter ensures only messages of the specified level and higher are sent via e-mail. For information on the levels, see Syslog message severity levels, on page 39.

Step 6 Click **OK**.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Syslog messages are sent as e-mails to the specified recipients according to the configured severity level.

Create a custom event list

Create a custom event list to control which syslog messages are sent to a logging destination. This allows you to filter messages based on event class, severity, and message identifier for more granular control.

An event list is a custom filter you can apply to a logging destination, allowing greater control over which messages are sent. Normally, you filter messages for a destination based solely on severity. Using an event list, you can fine-tune filters using event class, severity, and message ID.

Creating a custom event list is a two-step process. You create a custom list in the **Event Lists**, and then use the event list to define the logging filter for the various types of destination, in the **Logging Destinations**.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 46.

Before you begin

Ensure you have access to the system where syslog event lists can be configured.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Events List**.

Step 3 Click **Add** to create a new list or click an existing list to edit.

a) Enter a unique name for the event list in the **Name** field; avoid spaces.

b) Set criteria to filter messages by severity or event class, select the **Severity/Event Class** tab and add or edit entries.

For information on the available classes see Syslog message classes and associated message ID numbers, on page 41.

For information on the levels, see Syslog message severity levels, on page 39.

Certain event classes do not apply to devices in transparent mode. If you configure these options, the system does not use or deploy them.

c) To identify messages specifically by message ID, select the **Message ID** and add or edit the IDs.

You can enter a range of IDs using a hyphen, for example, 100000-200000. Each message ID you enter must contain six digits. For information on how the initial three digits map to features, see Syslog message classes and associated message ID numbers, on page 41.

For specific message numbers, see Cisco ASA Series Syslog Messages.

d) Click **OK** to save the event list.

Step 4 Click **Logging Destinations** and add or edit the destination that should use the custom event list filter.

See Enable logging destinations, on page 48.

Step 5 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

The system creates the custom event list and applies it to the logging destination you select.

Configure syslog rate limits

Limit the rate at which syslog messages are generated, reducing log flooding and ensuring that important messages are not lost.

Syslog message generation can overwhelm logging systems if not managed properly. Configure rate limits for severity levels or specific message IDs to ensure efficient log management. When limits set for severity level and message ID conflict, the message ID limit takes precedence.

Tip If you are configuring devices to send syslog messages about security events (such as connection and intrusion events), most Firewall Threat Defense platform settings do not apply to these messages. See Firewall Threat Defense platform settings that apply to security event syslog messages , on page 46.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Rate Limit**.

Step 3 To limit message generation by severity level, click **Logging Level** > **Add**, then configure these options:

- **Logging Level**—Specify the severity level for the rate limit. For information on the levels, see Syslog message severity levels, on page 39.
- **Number of messages**—The maximum number of messages of the specified type allowed in the specified time period.
- **Interval**—The number of seconds before the rate limit counter resets.

Step 4 Click **OK**.

Step 5 To limit message generation by syslog message ID, click **Syslog Level** > **Add**, then configure these options:

- **Syslog ID**—Specify the syslog message ID to be rate limited. For specific message numbers, see Cisco ASA Series Syslog Messages.
- **Number of messages**—Enter the maximum number of messages allowed in the specified interval.
- **Interval**—Set the interval (in seconds) for the rate limit counter to reset.

Step 6 Click **OK**.

Step 7 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Syslog message generation is limited based on configured severity levels or message IDs, preventing excessive log messages and supporting efficient log management.

Configure syslog settings

Configure syslog settings to manage how syslog messages are generated and sent to external syslog servers. You can specify the facility code, timestamp, device ID, and control message severity and suppression.

General syslog settings let you choose what information is included in syslog messages sent to syslog servers. This information includes the facility code, timestamp, device ID, severity levels, and message suppression. If you configure devices to send syslog messages about security events (such as connection and intrusion events), some settings do not apply to messages that relate to security events. See *Threat Defense Platform*

Settings That Apply to Security Event Syslog Messages in the *Cisco Secure Firewall Management Center Administration Guide*.

Before you begin

Make sure you have access to the device and the permissions needed to change syslog settings.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Syslog Settings**.

Step 3 Choose a system log facility from the **Facility** list as required by your syslog server.

Most UNIX systems use the default LOCAL4(20). Change the facility if your network devices use the same codes. In most cases, you do not need to set the facility value for security event logs.

Step 4 Select the **Enable timestamp on each syslog message** check box to include the date and time a message was generated in the syslog message.

Step 5 Select the desired **Timestamp Format**:

- **Legacy (MMM dd yyyy HH:mm:ss)**: Default format without a timezone (always UTC).
- **RFC 5424 (yyyy-MM-ddTHH:mm:ssZ)**: Uses ISO 8601 with "Z" indicating UTC.

Step 6 To add a device identifier at the start of messages, check the **Enable Syslog Device ID** check box and select the identifier type:

- **Interface**—Use the IP address of a specific interface.

  Note
  VTI tunnel interfaces are not supported for Syslog.

- **User Defined ID**—Enter a custom text string (up to 16 characters).
- **Host Name**—Use the device's hostname.

Step 7 Use the Syslog Message table to adjust severity or suppress messages:

Change a message's severity level or disable its generation if necessary. By default, syslog entries for NetFlow are enabled and appear in the table.

a) To suppress redundant messages due to NetFlow, select **Netflow Equivalent Syslogs**.

This adds the messages to the table as suppressed messages.

Note
If any of these syslog equivalents are already in the table, your existing rules are not overwritten.

b) To add a rule, click **Add**.
c) Select the message number (Syslog ID) to change, from the **Syslog ID** drop-down list.
d) Choose the new severity level from the **Logging Level** drop-down list or select **Suppressed** to disable the generation of the message. Usually, you do not change both the severity level and disable the message. However, you can modify both fields if you want.
e) Click **OK** to add the rule to the table.

Step 8 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

- Deploy configuration changes; see Deploy configuration changes.

Configure a syslog server

This task enables you to configure a syslog server for your device, allowing you to collect and monitor system-generated messages for security and operational visibility.

To configure a syslog server to handle messages generated from your system, perform this task.

If you want this syslog server to receive security events such as connection and intrusion events, see also Firewall Threat Defense platform settings that apply to security event syslog messages , on page 46.

Before you begin

- See requirements in Guidelines for logging, on page 43.
- Make sure your devices can reach your syslog collector on the network.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Syslog** > **Syslog Server**.

Step 3 Check the **Allow user traffic to pass when TCP syslog server is down (Recommended)** check box, to allow traffic if any syslog server that is using the TCP protocol is down.

Note

- This option is enabled by default. Unless required, we recommend that you allow connections through the threat defense device when the external TCP syslog server is unreachable by the device.
- When the **Allow user traffic to pass when TCP syslog server is down** option is disabled in Firewall Management Center version 6.2.x or earlier, it remains in the Disabled state even after upgrading to version 6.3 or later. You must manually enable this option.
- If this option is disabled and more than one TCP syslog server is configured on the device, user traffic is allowed if at least one server is reachable by thethreat defense device. This option only blocks traffic when none of the configured TCP syslog servers are reachable. The device generates a syslog message that describes the root cause of denied traffic.

```
%FTD-3-414003: TCP Syslog Server intf : IP_Address /port not responding. New connections
are denied based on logging permit-hostdown policy
```

Step 4 In the **Message queue size (messages)** field, enter the queue size for storing syslog messages on the security appliance when the syslog server is busy. The minimum is 1 message. The default is 512. Specify 0 to allow an unlimited number of messages to be queued (subject to available block memory).

If the number of messages exceeds the configured queue size, the excess messages are dropped, resulting in missing syslog entries. To determine the ideal queue size, you need to identify the available block memory. Use the **show blocks** command to know the current memory utilization. For more information on the command and its attributes, see *Cisco Secure Firewall ASA Series Command Reference Guide*. Contact Cisco TAC for assistance.

Step 5 Click **Add** to add a new syslog server.

a) In the **IP Address** drop-down list, select a network host object containing the IP address of the syslog server.

b) Choose the protocol, either TCP or UDP, and enter the port number used for communication between the Firewall Threat Defense device and the syslog server.

UDP is faster and uses fewer resources than TCP on the device.

The default port for UDP is 514. You must manually configure port 1470 for TCP. Valid non-default port values for either protocol are 1025 through 65535.

c) Check the **Log messages in Cisco EMBLEM format (UDP only)** check box to specify whether to log messages in Cisco EMBLEM format (available only if UDP is selected as the protocol).

The EMBLEM syslog format is a Cisco-specific convention that is built upon the RFC 3164 and RFC 5424 standards. Hence, when EMBLEM is enabled, the syslog message prints colon (:) after <PRI> field.

Note
Syslog messages in RFC5424 format typically displays the priority value, referred to as PRI. However, in Firewall Management Center, only when you enable logging in Cisco EMBLEM format, the PRI value in the syslog messages of the managed Firewall Threat Defense is displayed. Also, the device ID does not appear in EMBLEM-formatted syslog messages.

d) Check the **Enable Secure Syslog** check box to encrypt the connection between the device and server using SSL or TLS over TCP.

Note
You must select TCP as the protocol and its port value ranging between 1025 and 65535 to use this option. Upload the certificate required to communicate with the syslog server on the **Devices** > **Certificates** page. Then, upload the certificate from the Firewall Threat Defense device to the syslog server to complete the secure relationship and allow it to decrypt the traffic. The **Enable Secure Syslog** option is not supported on the device Management interface.

e) Select **Device Management Interface** or **Security Zones or Named Interfaces** to communicate with the syslog server.

- **Device Management Interface**: Send syslogs out of the Management interface. We recommend that you use this option when configuring syslog on Snort events.

  Note
  The **Device Management Interface** option does not support the **Enable Secure Syslog** option.

- **Security Zones or Named Interfaces**: Select the interfaces from the list of **Available Zones** and click **Add**.

  Important

The Firewall Threat Defense data plane (Lina) syslog messages cannot be sent out through the diagnostic interface. Configure other interfaces or the Management interface (Br1/Management0) to send out the data plane syslog messages.

f) Click **OK**.

Step 6 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

What to do next

- Deploy configuration changes; see Deploy configuration changes.

Configure timeouts

Configure timeout values for console sessions and protocol connections in a Threat Defense policy to manage session durations and optimize device resource usage.

You can set the global idle timeout durations for the connection and translation slots of various protocols. If the slot has not been used for the idle time specified, the resource is returned to the free pool.

You can also set a timeout for console sessions on the device.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Timeouts**.

Step 3 Configure the timeouts you want to change.

For any setting, select **Custom** to specify your own value or **Default** to use the system default value. In most cases, the maximum timeout is 1193 hours.

You can disable some timeouts by selecting **Disable**.

- **Console Timeout**—The idle time until a connection to the console is closed, range is 0 or 5 to 1440 minutes. The default is 0, which means the session does not time out. If you change the value, existing console sessions will continue to use the previous timeout value. The updated timeout will apply only to new connections.
- **Translation Slot (xlate)**—The idle time until a NAT translation slot is freed. This duration must be at least 1 minute. The default is 3 hours.
- **Connection (Conn)**—The idle time until a connection slot is freed. This duration must be at least 5 minutes. The default is 1 hour.
- **Half-Closed**—The idle time until a TCP half-closed connection closes. A connection is considered half-closed if both the FIN and FIN-ACK have been seen. If only the FIN has been seen, the regular connection timeout applies. The minimum is 30 seconds. The default is 10 minutes.

- **UDP**—The idle time until a UDP connection closes. This duration must be at least 1 minute. The default is 2 minutes.
- **ICMP**—The idle time after which general ICMP states are closed. The default (and minimum) is 2 seconds.
- **RPC/Sun RPC**—The idle time until a SunRPC slot is freed. This duration must be at least 1 minute. The default is 10 minutes.

  In a Sun RPC-based connection, if the parent connection is deleted or times out, a new child connection might not be treated as part of the parent–child relationship. As a result, the new connection could be evaluated according to the system's policy or rules. After the parent connection times out, existing child connections remain valid only until their own timeout value is reached.
- **H.225**—The idle time until an H.225 signaling connection closes. The default is 1 hour. To close a connection immediately after all calls are cleared, a timeout of 1 second (0:0:1) is recommended.
- **H.323**—The idle time after which H.245 (TCP) and H.323 (UDP) media connections close. The default (and minimum) is 5 minutes. Because the same connection flag is set on both H.245 and H.323 media connections, the H.245 (TCP) connection shares the idle timeout with the H.323 (RTP and RTCP) media connection.
- **SIP**—The idle time until a SIP signaling port connection closes. This duration must be at least 5 minutes. The default is 30 minutes.
- **SIP Media**—The idle time until a SIP media port connection closes. This duration must be at least 1 minute. The default is 2 minutes. The SIP media timer is used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.
- **SIP Disconnect**—The idle time after which SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message, between 0:0:1 and 0:10:0. The default is 2 minutes (0:2:0).
- **SIP Invite**—The idle time after which pinholes for PROVISIONAL responses and media xlates will be closed, between 0:1:0 and 00:30:0. The default is 3 minutes (0:3:0).
- **SIP Provisional Media**—The timeout value for SIP provisional media connections, between 1 and 30 minutes. The default is 2 minutes.
- **Floating Connection**—When multiple routes exist to a network with different metrics, the system uses the one with the best metric at the time of connection creation. If a better route becomes available, then this timeout lets connections be closed so a connection can be reestablished to use the better route. The default is 0 (the connection never times out). To make it possible to use better routes, set the timeout to a value between 0:0:30 and 1193:0:0. This timer does not apply to connections through virtual tunnel interfaces (VTI). If a connection through a VTI gets stuck, you must manually clear it.
- **Xlate PAT**—The idle time until a PAT translation slot is freed, between 0:0:30 and 0:5:0. The default is 30 seconds. You may want to increase the timeout if upstream routers reject new connections using a freed PAT port because the previous connection might still be open on the upstream device.
- **TCP Proxy Reassembly**—The idle timeout after which buffered packets waiting for reassembly are dropped, between 0:0:10 and 1193:0:0. The default is 1 minute (0:1:0).
- **ARP Timeout**—The number of seconds between ARP table rebuilds, from 60 to 4294967. The default is 14,400 seconds (4 hours).

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

The configured timeout values are applied to the Threat Defense policy. Sessions and protocol connections will now use the specified timeout durations after you deploy the policy.

Synchronize time on FTD devices

Use a Network Time Protocol (NTP) server to synchronize the clock settings on your devices. We recommend you configure all Firewall Threat Defenses managed by a Firewall Management Center to use the same NTP server as the Firewall Management Center. The Firewall Threat Defense gets its time directly FROM the configured NTP server. If the Firewall Threat Defense's configured NTP servers are not reachable for any reason, it synchronizes its time with the Firewall Management Center.

The device supports NTPv4.

Note If you are deploying Firewall Threat Defense on the Firepower 4100/9300 chassis, you must configure NTP on the Firepower 4100/9300 chassis so that Smart Licensing will work properly and to ensure proper timestamps on device registrations. You should use the same NTP server for the Firepower 4100/9300 chassis and the Firewall Management Center.

Before you begin

- If your organization has one or more NTP servers that your Firewall Threat Defense can reach, use the same NTP server or servers for your devices that you have configured for Time Synchronization on the **System** (⚙) > **Configuration** page on your Firewall Management Center.
- If you selected **Use the authenticated NTP server only** when configuring NTP server or servers for the Firewall Management Center, for your devices use only the NTP server or servers that are configured to authenticate with the Firewall Management Center. (The managed devices will use the same NTP servers as the Firewall Management Center, but their NTP connections will not use authentication.)
- If your device cannot reach an NTP server or your organization does not have one, use the **Via NTP FROM Management Center** option as discussed in this procedure.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Time Synchronization**.

Step 3 Configure one of these clock options:

- **Via NTP FROM Management Center**—(Default). The managed device gets time FROM the NTP servers you configured for the Firewall Management Center (except for authenticated NTP servers) and synchronizes time with those servers directly. However, if any of these are true, the managed device synchronizes time FROM the Firewall Management Center:

- The Firewall Management Center's NTP servers are not reachable by the device.
- The Firewall Management Center has no unauthenticated servers.

- **Via NTP FROM**—If your Firewall Management Center is using NTP servers on the network, select this option and enter the fully-qualified DNS name (such as NTP.example.com), or IPv4 or IPv6 address, of the same NTP servers you specified in **System** (⚙) > **Configuration** > **Time Synchronization**. If the NTP servers are not reachable, the Firewall Management Center acts as an NTP server.

When multiple NTP servers are configured, the device uses the NTP server that is deemed appropriate based on the criteria defined in RFC. Thus, the status "Being used" for a specific NTP server indicates that the server is currently used by the device.

Step 4 Click **Save**.

After completing these steps, the FTD device synchronizes its clock with the configured NTP server or, if unavailable, with the management center, ensuring accurate time for logs and system operations.

What to do next

- Deploy configuration changes; see Deploy configuration changes.

Configure a time zone for a device

By default, your device uses the UTC time zone. To set a different time zone for the device, use this procedure.

The time zone you specify is used only in policies that use time-based policy application.

Procedure

Step 1 Select **Devices** > **Platform Settings** and create or edit a Firewall Threat Defense policy.

You can also create time zone objects from the **Objects** > **Object Management** > **Time Zone** page.

Step 2 Create a new time zone object by clicking +.

Step 3 Select the time zone.

Step 4 Click **Save**.

What to do next

- Create time range objects, select applicable time ranges in access control and prefilter rules, and assign the parent policies to devices associated with the correct time zone.
- Deploy configuration changes; see Deploy configuration changes.

Configure UCAPL/CC compliance

Configure Unified Capabilities Approved Products List (UCAPL) or Common Criteria (CC) compliance to ensure your Secure Firewall Threat Defense device meets security certifications and export-controlled feature requirements.

Use this task when you need to enable security certifications compliance for your device. This is required for export-controlled features and may be necessary for regulatory or organizational compliance.

For more information about this setting and how to enable it for the Firewall Management Center, see the *Cisco Secure Firewall Management Center Administration Guide*.

Caution After you enable this setting, disabling it is not possible. To return the appliance to standard mode, reimage the appliance.

Before you begin

- Secure Firewall Threat Defense devices cannot use an evaluation license; your Smart Software Manager account must be enabled for export-controlled features.
- Secure Firewall Threat Defense devices must be deployed in routed mode.
- You must have administrative privileges to perform this task.
- Security certifications compliance mode cannot be changed if the Firewall Threat Defense device is in high availability. Change the security certifications compliance mode before you create the high availability pair.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Click **UCAPL/CC Compliance**.

Step 3 To *permanently* enable security certifications compliance on the appliance, you have two choices:

- To enable security certifications compliance in Common Criteria mode, choose **CC** from the drop-down list.
- To enable security certifications compliance in Unified Capabilities Approved Products List (UCAPL) mode, choose **UCAPL** from the drop-down list.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

After completing these steps, your device operates in the selected compliance mode (UCAPL or CC), and the policy is enforced once deployed.

Configure a performance profile

Configure the performance profile to control how CPU cores are allocated between the data plane and Snort processes on supported devices. This configuration optimizes device performance for VPN, improves intrusion prevention, or balances the workload.

The performance profile determines how the CPU cores on the device are assigned to two of the main system processes: the data plane (Lina) and Snort. The data plane handles VPN connections, routing, and basic layer 3/4 processing. Snort provides advanced inspection for intrusion and malware prevention, URL filtering, application filtering, and other deep packet inspection features.

If you use both basic and advanced features, keep the performance profile unchanged. The system is designed to provide a balanced assignment of cores to these processes. This assignment differs based on the hardware model.

However, if you use the device primarily for VPN, or for intrusion and other advanced inspection, you can skew the performance profile so that more cores are assigned to the more heavily used features. This change can improve system performance.

Before you begin

- These settings apply to systems running release 7.3+ only.
- Performance profile is supported on these device types:
  - Firepower 4100/9300
  - Secure Firewall Threat Defense Virtual
- Changing the performance profile is not supported on units in a cluster or high-availability group, or those configured for multi-instance.
- The minimum number for core allocation is 2. Cores are assigned in even numbers based on the selected performance profile.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **Performance Profile**.

Step 3 Select a profile:

- **Default**—This is the recommended setting and is the best option if you configure both VPN and intrusion inspection.
- **VPN Heavy with prefilter fastpath**—If you primarily use the device as a VPN endpoint or headend, and you configure rules in the prefilter policy to fastpath VPN traffic, you can choose this option to assign the majority of CPU cores to the data plane. The allocation is 90% data plane, 10% Snort.
- **VPN Heavy with inspection**—If you primarily use the device as a VPN endpoint or headend, but do not use the prefilter policy to fastpath VPN traffic, you can choose this option to assign the majority of CPU cores to the data plane. This option assumes that you leave intrusion inspection, URL filtering, and

other advanced functions that use Snort, to a different device in the network. The allocation is 60% data plane, 40% Snort.

- **IPS Heavy**—If you do not configure VPN, but you do use the device for intrusion prevention, you can choose this option to assign the majority of CPU core to the Snort process. The allocation is 30% data plane, 70% Snort.

Step 4 Click **Save**.

Step 5 Deploy the policy to apply your configuration.

Step 6 After deployment completes, reboot each affected device to apply the new core assignments.

After completing these steps, the device will use the selected performance profile and allocate CPU cores according to your configuration. The new core assignments take effect after you reboot the device.

History for platform settings

This reference provides a historical overview of feature additions, changes, and removals for platform settings in Secure Firewall releases. Use this information to track platform settings support and modifications across software versions.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Performance profile for CPU core allocation.	7.3.0	7.3.0	You can adjust the percentage of system cores assigned to the data plane and Snort to adjust system performance. The adjustment is based on your relative use of VPN and intrusion policies. If you use both, leave the core allocation to the default values. If you use the system primarily for VPN (without applying intrusion policies), or as an IPS (with no VPN configuration), you can skew the core allocation to the data plane (for VPN) or Snort (for intrusion inspection). We added the **Performance Profile** page to the platform settings policy.
TLS 1.3 in Remote Access VPN.	7.3.0	7.3.0	You can now use TLS 1.3 to encrypt remote access VPN connections. Use threat defense platform settings to specify that the device must use TLS 1.3 protocol when acting as a remote access VPN server. TLS 1.3 adds support for the following ciphers: • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 This feature requires Cisco Secure Client, Version 5.0 and above. New/modified screens: **Devices** > **Platform Settings** > **New Policy** > **Add/Edit Threat Defense Settings** > **SSL** > **TLS version**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Multiple DNS server groups for resolving DNS requests.	7.2.0	7.2.0	You can configure multiple DNS groups for the resolution of DNS requests from client systems. You can use these DNS server groups to resolve requests for different DNS domains. For example, you could have a catch-all default group that uses public DNS servers, for use with connections to the Internet. You could then configure a separate group to use internal DNS servers for internal traffic, for example, any connection to a machine in the example.com domain. Thus, connections to an FQDN using your organization's domain name would be resolved using your internal DNS servers, whereas connections to public servers use external DNS servers. We changed the **Platform Settings** > **DNS** page.
Network object support for HTTP, ICMP, and SSH platform settings.	7.1.0	7.1.0	You can now use network object groups that contain network objects for hosts or networks when configuring the IP addresses in the Threat Defense Platform Settings policy.
Support to specify trusted DNS servers.	7.1.0	7.1.0	The option to specify DNS servers that you can trust for address resolution while using direct internet access was introduced. We added a tab for configuring the trusted DNS servers when configuring direct internet access: **Devices** > **Platform Settings** > **DNS** > **Trusted DNS Servers**.
Platform settings using the MD5 authentication algorithm or DES encryption for SNMPv3 users can not be deployed to Firewall Threat Defense devices running Versions 7.0+.	7.0.0	7.0.0	The MD5 authentication algorithm and DES encryption for SNMPv3 users on Firewall Threat Defense were deprecated in Version 6.5. If your deployment includes SNMPv3 users using the MD5 authentication algorithm or DES encryption that were created using Version 6.4 or earlier, you can continue to use those users for Firewall Threat Defense devices running Version 6.7 or earlier. However, you cannot edit those users and retain the MD5 or DES settings, and you cannot create new users with the MD5 or DES settings. If your Firewall Management Center manages any Firewall Threat Defenses running Versions 7.0+, deploying a platform settings policy with SNMP v3 users using the MD5 authentication algorithm or DES encryption to those Firewall Threat Defenses will fail. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Hosts**
Specify SHA224 or SHA384 for SNMPv3 users' authorization algorithm.	7.0.0	7.0.0	You can now select SHA224 or SHA384 for SNMPv3 users' authorization algorithm. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users**
Specify time zone for device.	6.6.0	6.6.0	Specify a local time zone for a managed device, for use in time-based policy application. New/modified screens: **Devices** > **Platform Settings** > **Time Zone**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Specify the Management interface for SNMP communication.	6.6.0	6.6.0	You can now select the Management interface for communication between the device and the SNMP management station. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Hosts**
Specify SHA256 for SNMPv3 users' authorization algorithm.	6.6.0	6.6.0	You can now select SHA256 for SNMPv3 users' authorization algorithm. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users**
DES encryption and the MD5 authentication algorithm for SNMPv3 users on Firewall Threat Defense have been deprecated.	6.5.0	Any	We recommend that you not use the MD5 authentication algorithm or DES encryption for SNMPv3 users on Firewall Threat Defense devices, as these options have been deprecated. If your deployment includes SNMPv3 users using the MD5 authentication algorithm or DES encryption that were created using a Version 6.4 or earlier, you can continue to use those users. However, you cannot edit those users and retain the MD5 or DES settings, and you cannot create new users with the MD5 or DES settings. New/modified screens: **Devices** > **Platform Settings** > **SNMP** > **Users**
Allow user traffic to pass when TCP syslog server is down.	6.3.0	6.3.0	We recommend that you allow connections through the threat defense device when the external TCP syslog server is unreachable by the device. The **Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)** option in the Platform Settings is Enabled by default.
Limit number of SSH login failures.	6.3.0	6.3.0	When a user accesses any device via SSH and fails three successive login attempts, the device terminates the SSH session.
External authentication added for SSH.	6.2.3	6.2.3	You can now configure external authentication for SSH access to the Firewall Threat Defense using LDAP or RADIUS. New/modified screens: **Devices** > **Platform Settings** > **External Authentication**
Support for UC/APPL compliance mode.	6.2.1	6.2.1	You can enable security certifications compliance in CC mode or UCAPL mode. Enabling security certifications compliance does not guarantee strict compliance with all requirements of the security mode selected. For more information on hardening procedures, refer to the guidelines for this product provided by the certifying entity. New/modified screens: **Devices** > **Platform Settings** > **UC/APPL Compliance**
SSL settings for remote access VPN.	6.2.1	6.2.1	The Firewall Threat Defense device uses the Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS) to support secure message transmission for Remote Access VPN connection from remote clients. You can configure SSL versions and encryption algorithms that will be negotiated and used for message transmission during remote VPN access over SSL. New/modified screens: **Devices** > **Platform Settings** > **SSL**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
External authentication for SSH and HTML removed.	6.1.0	6.1.0	Due to changes to support converged management access, only local users are supported for SSH and HTML to data interfaces. Also, you can no longer SSH to the logical Diagnostic interface; instead you can SSH to the logical Management interface (which shares the same physical port). Previously, only external authentication was supported for SSH and HTML access to Diagnostic and data interfaces, while only local users were supported to the Management interface. New/modified screens: **Devices** > **Platform Settings** > **External Authentication**
Firepower Threat Defense support.	6.0.1	6.0.1	This feature was introduced. New/modified screens: **Devices** > **Platform Settings**