

FAQ and Support

- Security Cloud Control Firewall Management platform maintenance schedule, on page 1
- Navigate from Security Cloud Control to Cloud-Delivered Firewall Management Center, on page 2
- What does the default action "Analyze all tunnel traffic" for prefiltering mean?, on page 2
- How Security Cloud Control processes personal information, on page 2
- Can I restore a backup from a different device?, on page 2
- Does deploying a new prefilter policy immediately affect ongoing sessions?, on page 3
- How do I keep my security databases and feeds up to date?, on page 3
- What version of Secure Firewall Threat Defense can I manage with Cloud-Delivered Firewall Management Center?, on page 3
- How do I exclude specific traffic (Webex, Zoom, etc) from the remote access VPN?, on page 4
- How do I prevent users from accessing undesirable external network resources, such as inappropriate websites?, on page 5
- Security Feed Questions, on page 5
- How do I setup Rate-Based Attack Prevention on the FTD using Snort 2?, on page 8
- Complete the initial configuration of a Secure Firewall Threat Defense device using the CLI, on page 10
- About Data Interfaces, on page 13
- End-of-Support for management of Secure Firewall Threat Defense devices, Version 7.2.*x* and 7.3.*x*, managed by Cloud-Delivered Firewall Management Center, on page 14

Security Cloud Control Firewall Management platform maintenance schedule

Security Cloud Control Firewall Management updates its platform every week with new features and quality improvements. Updates are made during a 3-hour period according to this schedule:

Day of the week	**Time of day** **(24-hour time, UTC)**
Thursday	09:00 UTC - 12:00 UTC

During the Security Cloud Control Firewall Management upgrade period, you can still access your organization and the Cloud-Delivered Firewall Management Center. Additionally, the devices that you have onboarded to Security Cloud Control Firewall Management continue to enforce their security policies.



Note

- During the maintenance period of the Security Cloud Control Firewall Management, refrain from creating or deploying configurations to the devices it manages.
- If there is any issue that stops Security Cloud Control Firewall Management from communicating, Cisco addresses that issue in all the affected tenants as quickly as possible, even if it is outside the maintenance window.

Navigate from Security Cloud Control to Cloud-Delivered Firewall Management Center

1. In the Security Cloud Control dashboard, click **Administration** > **Integrations** > **Firewall Management Center**.
2. With Cloud-Delivered Firewall Management Center selected, click **Devices** in the Management pane.

What does the default action "Analyze all tunnel traffic" for prefiltering mean?

“Analyze all tunnel traffic” means subject all network traffic to the rules in the access control policy after they have been analyzed by the prefilter policy.

How Security Cloud Control processes personal information

To learn how Security Cloud Control processes your personal identifiable information, see the Security Cloud Control Privacy Data Sheet.

Can I restore a backup from a different device?

Yes, if the devices are the same model, are running the same software version, have the same number of network modules, and the same number of physical interfaces.

Does deploying a new prefilter policy immediately affect ongoing sessions?

No. When you deploy a prefilter policy, its rules are not applied on the existing tunnel sessions. Hence, traffic on an existing connection is not bound by the new policy that is deployed. In addition, the policy hit count is incremented only for the first packet of a connection that matches a policy. Thus, the traffic on an existing connection that could match a policy is omitted from the hit count.

How do I keep my security databases and feeds up to date?

If the management center has internet access, the system can often obtain updates on security databases and feeds directly from Cisco. We recommend you schedule or enable automatic content updates whenever possible. Some updates are auto-enabled by the initial setup process or when you enable the related feature. Other updates you must schedule yourself. After initial setup, we recommend you review all auto-updates and adjust them if necessary.

- There are several security databases and feeds you should update:
- Vulnerability database (VDB)
- Geolocation database (GeoDB)
- Intrusion rules (SRU/LSP)
- Security Intelligence Feeds
- URL categories and reputations

What version of Secure Firewall Threat Defense can I manage with Cloud-Delivered Firewall Management Center?

Cloud-Delivered Firewall Management Center supports these versions of Secure Firewall Threat Defense:

- Verion 7.0.3 or later 7.0.x versions.
- Version 7.2 and later versions.



Note Software Version 7.1 is _not_ supported.

All hardware and virtual deployments which can run these software versions are supported.

How do I exclude specific traffic (Webex, Zoom, etc) from the remote access VPN?

You can exclude specific traffic from the remote access VPN using dynamic split tunneling based on DNS domain names.

Excluded domains are not blocked. Instead, traffic to those domains is kept outside the VPN tunnel. For example, you could send traffic to Cisco WebEx on the public Internet, thus freeing bandwidth in your VPN tunnel for traffic that is targeted to servers within your protected network.

Procedure

Step 1 From the Security Cloud Control home page, in the navigation bar, click **Security Devices**.

Step 2 Find the Secure Firewall Threat Defense device you want to add this rule to. You can use the filter or search field to find the device.

Step 3 Select the device, and in the Device Management pane at the right, click **Device Overview**.

Step 4 Configure the group policy to use Dynamic Split Tunnel.

a) Choose **Devices** > **Remote Access**.
b) Click **Edit** on the remote access VPN policy for which you want to configure dynamic split tunneling.
c) Click **Edit** on the required connection profile.
d) Click **Edit Group Policy**.

Step 5 Configure the Secure Client custom attribute in the Add/Edit Group Policy dialog box.

a) Click the Secure Client tab.
b) Click **Custom Attributes** and click +.
c) Choose **Dynamic Split Tunneling** from the Secure Client Attribute drop-down list.
d) Click + to create a new custom attribute object.
e) Enter the name for the custom attribute object.
f) Exclude domains—Specify domain names that will be excluded from the remote access VPN.
g) Click **Save**.
h) Click **Add**.

Step 6 Verify the configured custom attribute and click **Save**.

Step 7 When you are ready to deploy this change to the device, click **Deploy** in the menu bar at the top of the page.

How do I prevent users from accessing undesirable external network resources, such as inappropriate websites?

Procedure

Step 1	From the Security Cloud Control home page, click **Security Devices** in the navigation bar.
Step 2	Find the Secure Firewall Threat Defense device you want to add these rules to. You can use the filter or search field to find the device.
Step 3	Select the device and in the Policies pane at the right, click **Access Control**.
Step 4	Click the policy you want to update.
Step 5	Click **Add Rule**.
Step 6	Give the rule a name.
Step 7	In the **Action** field, select **Block**.
Step 8	Insert the rule into either the Mandatory or into the Default policy.
Step 9	Click the **URLs** tab.
Step 10	In the Categories section, check the categories you want to block and accept the default value for "Any Reputation".
Step 11	Click **Add URL**.
Step 12	If there are specific URLs that you want to block, you can do that by entering them in the **Manually Enter URL** field and then click **Add URL**.
Step 13	Click **Apply**.
Step 14	On the policy page, click **Save**.
Step 15	When you are ready to deploy this change to the device, click **Deploy** in the menu bar at the top of the page.



Note Note: This instruction assumes you have the URL filtering license

Security Feed Questions

Related Information

How do I update intrusion rules (SRU/LSP)?

Follow this procedure to configure recurring Intrusion Rule update downloads.

Procedure

Step 1 From the Cloud-Delivered Firewall Management Center home page, navigate **System (gear icon) > Updates > Rule Updates**.

Step 2 Under **Recurring Rule Update Imports**, check **Enable Recurring Rule Update Imports**.

Step 3 Specify the **Import Frequency** and start time.

Note As updates are published multiple times each week, it is recommended to check on a Daily basis.

Step 4 (Optional, but recommended) Check **Reapply all policies...** to deploy after each update.

Caution Deploying intrusion rule updates can cause a Snort restart in rare occasions. It is recommended to deploy intrusion rule updates during a maintenance window.

Step 5 Click **Save**.

Step 6 Deploy your changes when you are ready.

Caution Deploying intrusion rule updates can cause a Snort restart. We recommend you deploy intrusion rule updates during a maintenance window.

How do I update my Cisco vulnerability database (VDB)?

The initial setup on the management center automatically downloads and installs the latest VDB from Cisco as a one-time operation. It also schedules a weekly task to download the latest available software updates, which includes the latest VDB. We recommend you review this weekly task and adjust if necessary, by navigating in the Cloud-Delivered Firewall Management Center to **System gear icon** > **Tools** > **Scheduling**.

You can choose to update the VDB either manually or automate the download and updates by creating scheduled tasks in the system. We recommend that you choose the automated method, to ensure timely downloads and updates.

Before you begin

.

You must be in the global domain to perform this task.

Procedure

Step 1 To manually update the VDB, see Manually Update the VDB and follow the steps in the procedure.

Step 2 To automate VDB updates, see Vulnerability Database Update Automation. Ensure you create tasks for both download of VDB versions and installation.

How do I update my Geolocation database?

As a part of initial configuration, the system configures a weekly automatic Geolocation (GeoDB) update. If configuring the update fails, we recommend you configure regular GeoDB updates as described in this procedure.

Procedure

Step 1 From the Cloud-Delivered Firewall Management Center home page, **System (gear icon) > Updates > Updates > Geolocation Updates**.

Step 2 Under **Recurring Geolocation Updates**, check **Enable Recurring Weekly Updates from the Support Site**.

Step 3 Specify the **Update Start Time**.

Step 4 Click **Save**.

How do I update Security Intelligence feeds?

By default, the built-in feeds on Cloud-Delivered Firewall Management Center are updated every two hours, with updates being pushed immediately to managed devices.

To change the update configuration, perform the following steps:

Procedure

Step 1 From the Cloud-Delivered Firewall Management Center home page, navigate **Objects > Object Management**.

Step 2 Expand the Security Intelligence node, then choose the feed type whose frequency you want to change.

Step 3 Next to the feed you want to update, click the pencil icon to **Edit** the update frequency.



Note The system-provided URL feed is combined with the domain feed under DNS Lists and Feeds.

Step 4 Edit the **Update Frequency**.

Step 5 Click **Save**.

How do I update URL reputations?

If you Enable Automatic Updates, by default, automatic URL updates are enabled. The management center checks Talos updates every 30 minutes. If you need strict control over when the system contacts external resources, disable automatic updates and instead create a recurring task using the scheduler. Although daily updates tend to be small, if it has been more than five days since your last update, new URL filtering data may take up to 20 minutes to download, depending on your bandwidth. Then, it may take up to 30 minutes to perform the update itself.

Procedure

Step 1 From the Cloud-Delivered Firewall Management Center home page, navigate **Integration > Other Integrations**.

Step 2 Click **Cloud Services**.

Step 3 In the URL Filtering pane:

a) Enable URL filtering.

b) Enable automatic updates.

Step 4 Click **Save**.

How do I setup Rate-Based Attack Prevention on the FTD using Snort 2?

Dynamic rule states are policy-specific.

A **Revert** appears in a field when you enter an invalid value; click it to revert to the last valid value for that field or to clear the field if there was no previous value.

Note Dynamic rule states cannot enable disabled rules or drop traffic that matches disabled rules.

Procedure:

Procedure

Step 1 On the Security Cloud Control menu bar, click **Administration** > **Integrations** > **Firewall Management Center** to view the Services page.

Step 2 Choose Cloud-Delivered FMC and click the links in the Actions, Management, or System pane to navigate to Cloud-Delivered Firewall Management Center to perform various actions. See View Services Page Information.

Step 3 Choose **Policies > Access Control > Intrusion**.

Step 4 Click Snort 2 Version next to the policy you want to edit.

If View (View button) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 5 Click **Rules** immediately under **Policy Information** in the navigation pane.

Step 6 Choose the rule or rules where you want to add a dynamic rule state.

Step 7 Choose **Dynamic State > Add Rate-Based Rule State**.

Step 8 Choose a value from the Track By drop-down list.

Step 9 If you set Track By to Source or Destination, enter the address of each host you want to track in the Network field. You can specify a single IP address, address block, variable, or a comma-separated list comprised of any combination of these.

Step 10 Next to Rate, specify the number of rule matches per time period to set the attack rate:

Step 11 From the New State drop-down list, specify the new action to be taken when the conditions are met.

Step 12 Enter a value in the Timeout field.

After the timeout occurs, the rule reverts to its original state. Specify 0 or leave the Timeout field blank to prevent the new action from timing out.

Step 13 Click OK.

Note The system displays a Dynamic State next to the rule in the Dynamic State column. If you add multiple dynamic rule state filters to a rule, a number over the filter indicates the number of filters.

Note To delete all dynamic rule settings for a set of rules, choose the rules on the Rules page, then choose Dynamic State > Remove Rate-Based States. You can also delete individual rate-based rule state filters from the rule details for the rule by choosing the rule, clicking Show details, then clicking Delete by the rate-based filter you want to remove.

Step 14 To save changes you made in this policy since the last policy commit, click Policy Information, then click Commit Changes.

If you leave the policy without committing changes, changes since the last commit are discarded if you edit a different policy.

Complete the initial configuration of a Secure Firewall Threat Defense device using the CLI

Connect to the device's CLI to perform initial setup, including setting the management IP address, gateway, and other basic networking settings using the setup wizard. Ensure all DNS and firewall ports are accessible for communication.

The dedicated management interface is a special interface with its own network settings. If you do not want to use the management interface, you can use the CLI to configure a data interface instead.

This configuration is ideal for devices that are going to be onboarded with their CLI registration key.

Note Do **not** use this configuration procedure for devices that are onboarding with zero-touch provisioning.

Procedure

Step 1 Connect to the device's CLI, either from the console port or using SSH to the management interface. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

(Firepower and Secure Firewall hardware models) The console port connects to the FXOS CLI. The SSH session connects directly to the Firewall Threat Defense CLI.

Step 2 Log in with the username **admin** and the password **Admin123** .

At the console port, you connect to the FXOS CLI. The first time you log in to FXOS, you are prompted to change the password. This password is also used for the Firewall Threat Defense login for SSH.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default.

For Firepower and Secure Firewall hardware, see the Reimage Procedures in the Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense .

For the ISA 3000, see the Cisco Secure Firewall ASA and Threat Defense Reimage Guide .

Example:

```
firepower login:
                        admin
Password:
                        Admin123
Successful login attempts for user 'admin' : 1
[...]
Hello admin. You must change your password.
Enter new password:
                        ********
Confirm new password:
```

```
                         ********
Your password was updated successfully.
[...]
firepower#
```

Step 3 If you connected to FXOS on the console port, connect to the Firewall Threat Defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4 The first time you log in to the device, you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, to change the admin password. You are then presented with the CLI setup script.

Note You cannot repeat the CLI setup wizard unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See the threat defense command reference.

Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

Note The management interface settings are used even when you enable Firewall Threat Defense access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the management interface DNS servers, and not the data interface DNS servers.

See the following guidelines:

- **Configure IPv4 via DHCP or manually?**—If you want to use a data interface for Firewall Threat Defense access instead of the management interface, choose **manual**. Although you do not plan to use the management interface, you must set an IP address, for example, a private address. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.
- **Enter the IPv4 default gateway for the management interface**—If you want to use a data interface for Firewall Threat Defense access instead of the management interface, set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the FMC access data interface.
- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?**—Enter **YES** to configure the device for the device to be managed by either the Cloud-Delivered Firewall Management Center or Secure Firewall Device Manager.

  Manage the device locally?—Enter **NO** to configure the device for remote management with the On-Premises Firewall Management Center.

- **Configure firewall mode?**—We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration. Note that data interface Firewall Threat Defense access is only supported in routed firewall mode.

Step 5 (Optional) Configure a data interface for Cloud-Delivered Firewall Management Center access.

configure network management-data-interface

You are then prompted to configure basic network settings for the data interface.



Note You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

See the following details for using this command. See About Data Interfaces, on page 13 for more informatio.

- The original management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the management interface gateway to **data-interfaces**, this command will set it now.
- When you onboard the device for Firewall Threat Defense management through Security Cloud Control, Security Cloud Control discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. You can later make changes to the access interface configuration, but make sure you don't make changes that can prevent the device or Security Cloud Control from re-establishing the management connection. If the management connection is disrupted, the device includes the **configure policy rollback** command to restore the previous deployment.
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  Also, local DNS servers are only retained if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in Security Cloud Control, including the DNS servers, to match the device configuration.
- You can change the management interface after you onboard the Firewall Threat Defense for Firewall Threat Defense management through threat defense, to either the management interface or another data interface.
- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow FMC access from any network, if you wish to change
 the FMC access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 6 (Optional) Limit data interface access to Security Cloud Control on a specific network.

configure network management-data-interface client *ip_address netmask*

By default, all networks are allowed.

About Data Interfaces

You can use either the dedicated management interface or a regular data interface for communication with the device. Security Cloud Control access on a data interface is useful if you want to manage the FTD remotely from the outside interface, or you do not have a separate management network. Security Cloud Control supports high availability on the FTD managed remotely from the data interface.

FTD management access from a data interface has the following limitations:

- You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.

- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the FTD and the WAN modem.
- The interface must be in the global VRF only.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using Security Cloud Control. Because the management interface gateway will be changed to be the data interfaces, you also cannot SSH to the management interface from a remote network unless you add a static route for the management interface using the **configure network static-routes** command. For FTDv on Amazon Web Services, a console port is not available, so you should maintain your SSH access to the management interface: add a static route for Management before you continue with your configuration. Alternatively, be sure to finish all CLI configuration (including the **configure manager add** command) before you configure the data interface.

End-of-Support for management of Secure Firewall Threat Defense devices, Version 7.2.*x* and 7.3.*x*, managed by Cloud-Delivered Firewall Management Center

Which version of Threat Defense will Cloud-Delivered Firewall Management Center stop managing?

Cloud-Delivered Firewall Management Center will stop managing Threat Defense devices running Versions 7.2.*x* and 7.3.*x*, from July 24, 2027.

Why is this change necessary?

This change is necessary to ensure compatibility and security for our customers' systems. As we upgrade our systems, it is essential that the latest versions of Threat Defense devices are supported to maintain reliability and performance.

From July 24, 2027, can I use my existing Threat Defense 7.2.*x* and 7.3.*x* devices?

We will not support the management of Threat Defense devices running Versions 7.2.*x* and 7.3.*x* from Cloud-Delivered Firewall Management Center after July 24, 2027. You will not be able to make or deploy changes to devices running 7.2.*x* and 7.3.*x*, or earlier versions, except to upgrade or unregister them. Impacted devices will remain visible in Cloud-Delivered Firewall Management Center in read-only mode, and new changes cannot be deployed to the devices.

What are the recommended upgrade options?

You are required to upgrade to at least Versions 7.4.*x*. The Cisco-recommended version is 7.6.6.

Can I register new Threat Defense 7.2.*x* and 7.3.*x* devices?

While the system will allow you to register new Threat Defense running Versions 7.2.*x* and 7.3.*x* devices to Cloud-Delivered Firewall Management Center, from July 24, 2027, these newly registered devices will be in read-only mode only. You are required to upgrade to Version 7.4.*x* or to Cisco-recommended Version 7.6.6 prior to registration or the July 24, 2027, deadline.

What will happen if I don't upgrade?

From July 24, 2027, you will not be able to make or deploy changes to Threat Defense devices running Versions 7.2.x and 7.3.*x* and earlier, except to upgrade or unregister. Failing to upgrade leaves you vulnerable to compatibility issues, security issues, and possible downtime. To minimize disruption, you are required to upgrade now.

Will there be any impact on my existing systems or applications?

Upgrading is unlikely to have any significant impact on your current deployment. If you face any issues during the upgrade process, contact Cisco Technical Assistance (TAC) - https://mycase.cloudapps.cisco.com/case.

For assistance in upgrading, Cisco offers the LevelUp program. You can request assistance using the following link: https://cloud.path.cisco.com/lp-a01-secure-firewall-levelup

How do I upgrade?

For information about upgrading Threat Defense devices, go to https://www.cisco.com/go/ftd-cdfmc-upgrade.

Are there costs associated with upgrade?

The software upgrade has no additional cost. However, Cisco Firepower 4110, 4120, 4140, and 4150 devices running Threat Defense Version 7.2.x require a hardware refresh because they cannot be upgraded to a supported version. Contact your Cisco account team for assistance with the hardware refresh.

Is there an exception for customers who are not able to complete the device upgrade before July 24, 2027?

No, there are no exceptions to this requirement.

What if I'm unsure about how to proceed?

Reach out to Cisco Technical Assistance Center (TAC) (or the Cisco account team) for clarifications.