



System Management

The following topics explain how to perform system management tasks such as updating system databases and backing up and restoring the system.

- [Installing Software Updates, on page 1](#)
- [Backing Up and Restoring the System, on page 6](#)
- [Rebooting the System, on page 10](#)
- [Troubleshooting the System, on page 10](#)
- [Uncommon Management Tasks, on page 18](#)

Installing Software Updates

You can install updates to the system databases and to the system software. The following topics explain how to install these updates.

Updating System Databases

The system uses several databases to provide advanced services. Cisco provides updates to these databases so that your security policies use the latest information available.

Overview of System Database Updates

FTD uses the following databases to provide advanced services.

Intrusion rules

As new vulnerabilities become known, the Cisco Talos Intelligence Group (Talos) releases intrusion rule updates that you can import. These updates affect intrusion rules, preprocessor rules, and the policies that use the rules.

Intrusion rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules, provide new rule categories and default variables, and modify default variable values.

For changes made by an intrusion rule update to take effect, you must redeploy the configuration.

Intrusion rule updates may be large, so import rules during periods of low network use. On slow networks, an update attempt might fail, and you will need to retry.

Geolocation database (GeoDB)

The Cisco Geolocation Database (GeoDB) is a database of geographical data (such as country, city, coordinates) associated with routable IP addresses.

GeoDB updates provide updated information on physical locations that your system can associate with detected routable IP addresses. You can use geolocation data as a condition in access control rules.

The time needed to update the GeoDB depends on your appliance; the installation usually takes 30 to 40 minutes. Although a GeoDB update does not interrupt any other system functions (including the ongoing collection of geolocation information), the update does consume system resources while it completes. Consider this when planning your updates.

Vulnerability database (VDB)

The Cisco Vulnerability Database (VDB) is a database of known vulnerabilities to which hosts may be susceptible, as well as fingerprints for operating systems, clients, and applications. The firewall system correlates the fingerprints with the vulnerabilities to help you determine whether a particular host increases your risk of network compromise. The Cisco Talos Intelligence Group (Talos) issues periodic updates to the VDB.

The time it takes to update vulnerability mappings depends on the number of hosts in your network map. You may want to schedule the update during low system usage times to minimize the impact of any system downtime. As a rule of thumb, divide the number of hosts on your network by 1000 to determine the approximate number of minutes to perform the update.

After you update the VDB, you must redeploy configurations before updated application detectors and operating system fingerprints can take effect.

URL Category/Reputation Database

The system obtains the URL category and reputation database from Cisco Collective Security Intelligence (CSI). If you configure URL filtering access control rules that filter on category and reputation, requested URLs are matched against the database. You can configure database updates and some other URL filtering preferences on **System Settings > Cloud Preferences**. You cannot manage URL category/reputation database updates the same way you manage updates for the other system databases.

Updating System Databases

You can manually retrieve and apply system database updates at your convenience. Updates are retrieved from the Cisco support site. Thus, there must be a path to the internet from the system's management address.



Note In May 2022 we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The FDM does not and has never used the information in the IP package. This split saves significant disk space in locally managed FTD deployments. If you are getting the GeoDB from Cisco yourself, make sure you get the country code package, which has the same file name as the old all-in-one package: `Cisco_GEODB_Update-date-build`.

You can also set up a regular schedule to retrieve and apply database updates. Because these updates can be large, schedule them for times of low network activity.



Note While a database update is in progress, you might find that the user interface is sluggish to respond to your actions.

Before you begin

To avoid any potential impact to pending changes, deploy the configuration to the device before manually updating these databases.

Please be aware that VDB and URL category updates can remove applications or categories. You need to update any access control or SSL decryption rules that use these deprecated items before you can deploy changes.

Procedure

- Step 1** Click the name of the device in the menu, then click **View Configuration** in the Updates summary. This opens the Updates page. Information on the page shows the current version for each database and the last date and time each database was updated.
- Step 2** To manually update a database, click **Update Now** in the section for that database. After downloading and applying the update, the system automatically re-deploys policies to the device so that the system can use the updated information.
- Step 3** (Optional) To set up a regular database update schedule:
- Click the **Configure** link in the section for the desired database. If there is already a schedule, click **Edit**. The update schedules for the databases are separate. You must define the schedules separately.
 - Set the update start time:
 - The frequency of the update (Daily, Weekly, or Monthly).
 - For weekly or monthly, the days of the week or month you want the update to occur.
 - The time you want the update to start. The time you specify is adjusted for Daylight Savings Time, so it will move an hour forward or backward whenever the time is adjusted in your area. You must edit the schedule at the time change if you want to keep this exact time throughout the year.
 - Click **Save**.

Note If you want to remove a recurring schedule, click the **Edit** link to open the scheduling dialog box, then click the **Remove** button.

Upgrading the FTD Software

You can install the FTD software upgrades as they become available. The following procedure assumes that your system is already running the FTD software and that it is operating normally.

You cannot reimage a device, or migrate from ASA software to the FTD software, using this procedure.

Before you begin

Ensure that you deploy any pending changes, and wait until the deployment is complete (see the task list to verify). The system does not allow you to apply an upgrade if there are pending changes.

Then, log out from the FDM. Do not make any configuration changes while upgrading the software.

During upgrade, all events are erased.

Procedure

Step 1 Obtain the upgrade image and prepare it for installation.

a) Log into Cisco.com and download the upgrade image.

- Ensure that you obtain the appropriate upgrade file, whose file type is .sh. Do not download the system software package or the boot image.
- Verify that you are running the required baseline image for the upgrade.

b) Put the image on an HTTP server that you can reach from the management IP address.

Alternatively, you can use TFTP or SCP to download the file. If you choose one of those options, place the file on a server that supports those file transfer protocols.

Step 2 Use an SSH client to log into the management IP address using the **admin** user account and password.

Alternatively, you can connect to the Console port.

Step 3 Enter the **expert** command to access expert mode.

```
> expert
admin@firepower:~$
```

Step 4 Change the working directory (**cd**) to `/var/sf/updates/`.

```
admin@firepower:~$ cd /var/sf/updates/
admin@firepower:/var/sf/updates$
```

Step 5 Download the upgrade file from your HTTP server.

sudo wget url

For example, the following command downloads the fictitious `Cisco_FTD_Upgrade-6.2.0-181.sh` upgrade file from the `ftd` folder on the `files.example.com` HTTP server. Because the **sudo** command operates under root user, you see a stock warning, and you must re-enter the **admin** password before the command executes. Wait for the download to complete.

```
admin@firepower:/var/sf/updates$ sudo wget
http://files.example.com/ftd/Cisco_FTD_Upgrade-6.2.0-181.sh
```

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
```

```
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
```

```
Password: (enter admin password)
Connecting to files.example.com
|*****
*****
*****
*****
*****|

... (remaining output omitted)
```

Use the **tfpt** or **scp** commands instead if you are not using an HTTP server.

Step 6 Install the upgrade file.

```
sudo install_update.pl --detach /var/sf/updates/filename
```

You must include the full path to the upgrade file in the command. We recommend including the **--detach** keyword to ensure that the install process does not stop if your user session times out or is otherwise closed during the process. For example:

```
admin@firepower:/var/sf/updates$ sudo
install_update.pl --detach /var/sf/updates/Cisco_FTD_Upgrade-6.2.0-181.sh
(output omitted)
```

Step 7 Wait until installation is complete. The system reboots itself when installation is complete. Installation might take 30 minutes or more.

Step 8 Verify that the installation is complete.

Use an SSH client to log into the management IP address using the **admin** user account and password. The banner information includes a line (highlighted) that should show the new build number. For example, the following output indicates that the FTD version is now 6.2.0-181, which matches the example upgrade file. The **show version** command also shows software version information.

```
Password:

Last login: Fri May 6 14:42:18 2016 from 10.152.242.234

Copyright 2004-2016, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.1.0 (build 22)
Cisco ASA5512-X Threat Defense v6.2.0 (build 181)

>
```

Reimaging the Device

Reimaging a device involves wiping out the device configuration and installing a fresh software image. The intention of reimaging is to have a clean installation with a factory default configuration.

You would reimage the device in these circumstances:

- You want to convert the system from ASA Software to FTD Software. You cannot upgrade a device running an ASA image to one running a FTD image.
- The device is running a pre-6.1.0 image, and you want to upgrade to 6.1 or a later image and configure the device using the FDM. You cannot use the FMC to upgrade a pre-6.1 device and then switch to local management.
- The device is not functioning correctly and all attempts at fixing the configuration have failed.

For information on how to reimage a device, see *Reimage the Cisco ASA or Threat Defense Device* or the *Threat Defense Quick Start* guide for your device model. These guides are available at <http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html>.

Backing Up and Restoring the System

You can back up the system configuration so that you can restore the device if the configuration becomes corrupted due to subsequent miss-configuration or physical mishap.

You can restore a backup onto a replacement device only if the two devices are the same model and are running the same version of the software (including the build number, not just the same point release). Do not use the backup and restore process to copy configurations between appliances. A backup file contains information that uniquely identifies an appliance, so that it cannot be shared in this manner.



Note The backup does not include the management IP address configuration. Thus, when you recover a backup file, the management address is not replaced from the backup copy. This ensures that any changes you made to the address are preserved, and also makes it possible to restore the configuration on a different device on a different network segment.

Backups include the configuration only, and not the system software. If you need to completely reimage the device, you need to reinstall the software, then you can upload a backup and recover the configuration.

The configuration database is locked during backup. You cannot make configuration changes during a backup, although you can view policies, dashboards, and so forth. During a restore, the system is completely unavailable.

The table on the Backup and Restore page lists all existing backup copies that are available on the system, including the file name of the backup, the date and time it was created, and the file size. The type of backup (manual, scheduled, or recurring) is based on how you directed the system to create that backup copy.



Tip Backup copies are created on the system itself. You must manually download backup copies and store them on secure servers to ensure that you have the backup copies you need for disaster recovery. The system maintains up to 3 backup copies on the device. New backups replace the oldest backup.

The following topics explain how to manage backup and restore operations.

Backing Up the System Immediately

You can start a backup whenever you want.

Procedure

- Step 1** Click the name of the device in the menu, then click **View Configuration** in the Backup and Restore summary. This opens the Backup and Restore page. The table lists all existing backup copies that are available on the system.
- Step 2** Click **Manual Backup > Back Up Now**.
- Step 3** Enter a name for the backup and optionally a description. If you decide you want to perform the backup at a future time rather than immediately, you can click **Schedule** instead.
- Step 4** Click **Back Up Now**. The system starts the backup process. When the backup is complete, the backup file will appear in the table. You can then download the backup copy to your system and store it elsewhere, if desired. You can leave the Backup and Restore page after initiating the backup. However, the system will likely be sluggish, and you should consider pausing your work to allow the backup to complete. In addition, the system will acquire locks on the configuration database during parts or all of the backup, which can prevent you from making changes for the duration of the backup process.
-

Backing Up the System at a Scheduled Time

You can set up a scheduled backup to back up the system at a specific future date and time. A scheduled backup is a one-time occurrence. If you want to create a backup schedule to regularly create backups, configure a recurring backup instead of a scheduled backup.



Note If you want to delete the schedule for a future backup, edit the schedule and click **Remove**.

Procedure

- Step 1** Click the name of the device in the menu, then click **View Configuration** in the Backup and Restore summary.
- Step 2** Click **Scheduled Backup > Schedule a Backup**. If you already have a scheduled backup, click **Scheduled Backup > Edit**.
- Step 3** Enter a name for the backup and optionally a description.

Step 4 Select the date and time for the backup.

Step 5 Click **Schedule**.

When the selected date and time arrives, the system takes a backup. When completed, the backup copy is listed in the table of backups.

Setting Up a Recurring Backup Schedule

You can set up a recurring backup to back up the system on a regular schedule. For example, you could take a backup every Friday at midnight. A recurring backup schedule helps ensure that you always have a set of recent backups.



Note If you want to delete a recurring schedule, edit the schedule and click **Remove**.

Procedure

Step 1 Click the name of the device in the menu, then click **View Configuration** in the Backup and Restore summary.

Step 2 Click **Recurring Backup > Configure**.

If you already have a recurring backup configured, click **Recurring Backup > Edit**.

Step 3 Enter a name for the backup and optionally a description.

Step 4 Select the **Frequency** and the related schedule:

- **Daily**—Select the time of day. A backup is taken every day at the scheduled time.
- **Weekly**—Select the days of the week and the time of day. A backup is taken on each day you select at the scheduled time. For example, you could schedule backups for every Monday, Wednesday, and Friday at 23:00 hours (11 PM).
- **Monthly**—Select the days of the month and the time of day. A backup is taken on each day you select at the scheduled time. For example, you could schedule backups for the first (1), fifteenth (15), and twenty-eighth (28) days of the month at 23:00 hours (11 PM).

The time you specify is adjusted for Daylight Savings Time, so it will move an hour forward or backward whenever the time is adjusted in your area. You must edit the schedule at the time change if you want to keep this exact time throughout the year.

Step 5 Click **Save**.

When the selected dates and times arrive, the system takes a backup. When completed, the backup copy is listed in the table of backups.

The recurring schedule continues to take backups until you change or remove it.

Restoring a Backup

You can restore backups as needed so long as the device is running the same software version (including build number) as it was running when you took the backup. You can restore a backup onto a replacement device only if the two devices are the same model and are running the same version of the software (including build number).


If the backup copy you want to restore is not already on the device, you must upload the backup first before restoring it.

During a restore, the system is completely unavailable.



Note The backup does not include the management IP address configuration. Thus, when you recover a backup file, the management address is not replaced from the backup copy. This ensures that any changes you made to the address are preserved, and also makes it possible to restore the configuration on a different device on a different network segment.

Procedure


- Step 1** Click the name of the device in the menu, then click **View Configuration** in the Backup and Restore summary. This opens the Backup and Restore page. The table lists all existing backup copies that are available on the system.
- Step 2** If the backup copy that you want to restore is not in the list of available backups, click **Upload > Browse** and upload the backup copy.
- Step 3** Click the restore icon () for the file. You are asked to confirm the restore. By default, the backup copy will be deleted after the restore, but you can select **Do not remove the backup after restoring** to keep it before proceeding with the restore. The system will reboot after restore completes.
- Step 4** After the system is up and running, click the **Deploy** button and redeploy the configuration.



Managing Backup Files



As you create new backups, the backup files are listed on the Backup and Restore page. Backup copies are not retained indefinitely: as disk space usage on the device reaches the maximum threshold, older backup copies are deleted to make room for newer ones. In addition, when you install any upgrade other than a hot fix, all backup files are deleted. Thus, you should regularly manage the backup files to ensure that you have the specific backup copies you most want to keep.

You can do the following to manage your backup copies:

- Download files to secure storage—To download a backup file to your workstation, click the download icon () for the file. You can then move the file to your secure file storage.
- Upload a backup file to the system—If you want to restore a backup copy that is no longer available on the device, click **Upload > Browse File** and upload it from your workstation. You can then restore it.



Note Uploaded files may be renamed to match the original filename. Also, if there are more than 10 backup copies already on the system, the oldest one will be deleted to make room for the uploaded file. You cannot upload files that were created by an older software version.

- Restore a backup—To restore a backup copy, click the restore icon () for the file. The system is unavailable during restore, and will reboot after restore completes. You should deploy the configuration after the system is up and running.
- Delete a backup file—If you no longer want a particular backup, click the delete icon () for the file. You are asked to confirm the deletion. Once deleted, you cannot recover the backup file.

Rebooting the System

If you believe the system is not performing correctly and other efforts to resolve the problem have failed, you can reboot the device. You must reboot the device through the CLI; you cannot reboot the device through the FDM.

Procedure

- Step 1** Use an SSH client to open a connection to the management IP address and log into the device CLI with a username that has configuration CLI access. For example, the **admin** username.
- Step 2** Enter the **reboot** command.

Example:

```
> reboot
```

Troubleshooting the System

The following topics address some system-level troubleshooting tasks and capabilities. For information on troubleshooting a specific feature, such as access control, see the chapter for the feature.

Pinging Addresses to Test Connectivity

Ping is a simple command that lets you determine if a particular address is alive and responsive. This means that basic connectivity is working. However, other policies running on a device could prevent specific types of traffic from successfully getting through a device. You can use **ping** by logging into the device CLI.



Note Because the system has multiple interfaces, you can control the interface used for pinging an address. You must ensure that you are using the right command, so that you are testing the connectivity that matters. For example, the system must be able to reach the Cisco license server through the virtual Management interface, so you must use the **ping system** command to test the connection. If you use **ping**, you are testing whether an address can be reached through the data interfaces, which might not give you the same result.

The normal ping uses ICMP packets to test the connection. If your network prohibits ICMP, you can use a TCP ping instead (for data interface pings only).

Following are the main options for pinging network addresses.

Pinging an address through the virtual Management interface

Use the **ping system** command.

ping system *host*

The host can be an IP address or fully-qualified domain name (FQDN), such as `www.example.com`. Unlike pings through the data interfaces, there is no default count for system pings. The ping continues until you stop it using Ctrl+c. For example:

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

Pinging an address through a data interface using the routing table

Use the **ping** command. Without specifying an interface, you are testing whether the system can generically find a route to the host. Because this is how the system normally routes traffic, this is typically what you want to test.

ping *host*

Specify the IP address of the host. If you only know the FQDN, use the **nslookup fqdn-name** command to determine the IP address. For example:

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```



Note You can specify the timeout, repeat count, packet size, and even the data pattern to send. Use the help indicator, `?`, in the CLI to see the available options.

Pinging an address through a specific data interface

Use the **ping interface** *if_name* command if you want to test connectivity through a specific data interface. You can also specify the diagnostic interface using this command, but not the virtual management interface.

ping interface *if_name* *host*

Specify the IP address of the host. If you only know the FQDN, use the **nslookup** *fqdn-name* command to determine the IP address. For example:

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Pinging an address through a data interface using TCP ping

Use the **ping tcp** command. A TCP ping sends SYN packets and considers the ping successful if the destination sends a SYN-ACK packet.

ping tcp [**interface** *if_name*] *host* *port*

You must specify the host and TCP port. If you only know the FQDN, use the **nslookup** *fqdn-name* command to determine the IP address.

You can optionally specify the interface, which is the source interface of the ping, not the interface through which to send the pings. This type of ping always uses the routing table.

A TCP ping sends SYN packets and considers the ping successful if the destination sends a SYN-ACK packet. For example:

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```



Note You can also specify the timeout, repeat count, and the source address for the TCP ping. Use the help indicator, `?`, in the CLI to see the available options.

Tracing Routes to Hosts

If you are having problems sending traffic to an IP address, you can trace the route to the host to determine if there is a problem on the network path. A traceroute works by sending UDP packets on an invalid port, or ICMPv6 echoes, to a destination. The routers along the way to the destination respond with an ICMP Time Exceeded Message, and report that error to traceroute. Each node receives three packets, so you get three chances per node to get an informative result. You can use **traceroute** by logging into the device CLI.



Note There are separate commands for tracing a route through a data interface (**traceroute**) or through the virtual management interface (**traceroute system**). Ensure that you use the right command.

The following table describes the possible result per packet as displayed in the output.

Output Symbol	Description
*	No response was received for the probe within the timeout period.
<i>nn</i> msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
!N.	ICMP network unreachable.
!H	ICMP host unreachable.
!P	ICMP protocol unreachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

Tracing a route through the virtual management interface

Use the **traceroute system** command.

traceroute system *destination*

The host can be an IPv4/IPv6 address or fully-qualified domain name (FQDN), such as `www.example.com`. For example:

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1 192.168.0.254 (192.168.0.254) 0.213 ms 0.310 ms 0.328 ms
 2 10.88.127.1 (10.88.127.1) 0.677 ms 0.739 ms 0.899 ms
 3 lab-gw1.example.com (10.89.128.25) 0.638 ms 0.856 ms 0.864 ms
 4 04-bb-gw1.example.com (10.152.240.65) 1.169 ms 1.355 ms 1.409 ms
 5 wan-gw1.example.com (10.152.240.33) 0.712 ms 0.722 ms 0.790 ms
 6 wag-gw1.example.com (10.152.240.73) 13.868 ms 10.760 ms 11.187 ms
 7 rbb-gw2.example.com (172.30.4.85) 7.202 ms 7.301 ms 7.101 ms
 8 rbb-gw1.example.com (172.30.4.77) 8.162 ms 8.225 ms 8.373 ms
 9 sbb-gw1.example.com (172.16.16.210) 7.396 ms 7.548 ms 7.653 ms
10 corp-gw2.example.com (172.16.16.58) 7.413 ms 7.310 ms 7.431 ms
11 dmzbb-gw2.example.com (172.16.0.78) 7.835 ms 7.705 ms 7.702 ms
12 dmzdcc-gw2.example.com (172.16.0.190) 8.126 ms 8.193 ms 11.559 ms
13 dcz05n-gw1.example.com (172.16.2.106) 11.729 ms 11.728 ms 11.939 ms
```

```
14 www1.example.com (172.16.4.161) 11.645 ms 7.958 ms 7.936 ms
```

Tracing a route through a data interface

Use the **traceroute** command.

traceroute *destination*

Specify the IP address of the host. If you only know the FQDN, use the **nslookup fqdn-name** command to determine the IP address. For example:

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 0 10.83.194.1 0 msec 10 msec 0 msec
 1 10.83.193.65 0 msec 0 msec 0 msec
 2 10.88.193.101 0 msec 10 msec 0 msec
 3 10.88.193.97 0 msec 0 msec 10 msec
 4 10.88.239.9 0 msec 10 msec 0 msec
 5 10.88.238.65 10 msec 10 msec 0 msec
 6 172.16.7.221 70 msec 70 msec 80 msec
 7 209.165.200.225 70 msec 70 msec 70 msec
```



Note You can specify the timeout, time to live, number of packets per node, and even the IP address or interface to use as the source of the traceroute. Use the help indicator, **?**, in the CLI to see the available options.

Troubleshooting NTP

The system relies on accurate and consistent time to function correctly and to ensure that events and other data points are handled accurately. You must configure at least one, but ideally three, Network Time Protocol (NTP) servers to ensure the system always has reliable time information.

The device summary connection diagram (click **Device** in the main menu) shows the status of the connection to the NTP server. If the status is yellow or orange, then there is an issue with the connection to the configured servers. If the connection problem persists (it is not just a momentary issue), try the following.

- First, ensure that you have at least three NTP servers configured on **Device > System Settings > NTP**. Although this is not a requirement, reliability is greatly enhanced if you have at least three NTP servers.
- Ensure that there is a network path between the management interface IP address (defined on **Device > System Settings > Management Interface**) and the NTP servers.
Log into the device CLI and use the **ping system** command to test whether there is a network path to each NTP server.
- Log into the device CLI and check the status of the NTP servers with the following commands.
 - **show ntp**—This command shows basic information about the NTP servers and their availability. However, the connectivity status in the FDM uses additional information to indicate the status, so there can be inconsistency in what this command shows and what the connectivity status diagram shows.

- **system support ntp**—This command includes the output of **show ntp** plus the output of the standard NTP command **ntpq**, which is documented with the NTP protocol. Use this command if you need to confirm NTP synchronization.

Look for the section “Results of ‘ntpq -pn.’ For example, you might see something like the following:

```
Results of 'ntpq -pn'
remote           : +216.229.0.50
refid            : 129.7.1.66
st              : 2
t               : u
when            : 704
poll            : 1024
reach           : 377
delay           : 90.455
offset          : 2.954
jitter          : 2.473
```

In this example, the + before the NTP server address indicates that it is a potential candidate. An asterisk here, *, indicates the current time source peer.

The NTP daemon (NTPD) uses a sliding window of eight samples from each one of the peers and picks out one sample, then the clock selection determines the true chimers and the false tickers. NTPD then determines the round-trip distance (the offset of a candidate must not be over one-half the round trip delay). If connection delays, packet loss, or server issues cause one or all the candidates to be rejected, you would see long delays in the synchronization. The adjustment also occurs over a very long period of time: the clock offset and oscillator errors must be resolved by the clock discipline algorithm and this can take hours.



Note If the refid is .LOCL., this indicates the peer is an undisciplined local clock, that is, it is using its local clock only to set the time. The FDM always marks the NTP connection yellow (not synchronized) if the selected peer is .LOCL. Normally, NTP does not select a .LOCL. candidate if a better one is available, which is why you should configure at least three servers.

Analyzing CPU and Memory Usage

To view system-level information about CPU and memory usage, select **Monitoring > System** and look for the CPU and Memory bar graphs. These graphs show information collected through the CLI using the **show cpu system** and **show memory system** commands.

If you log into the CLI, you can use additional versions of these commands to view other information. Typically, you would look at this information only if you are having persistent problems with usage, or at the direction of the Cisco Technical Assistance Center (TAC). Much of the detailed information is complex and requires TAC interpretation.

Following are some highlights of what you can examine. You can find more detailed information about these commands in [Cisco Firepower Threat Defense Command Reference](http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html) at http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html.

- **show cpu** displays data plane CPU utilization.

- **show cpu core** displays usage for each CPU core separately.
- **show cpu detailed** displays additional per-core and overall data plane CPU usage.
- **show memory** displays data plane memory usage.



Note Some of the keywords (not mentioned above) require that you first set up profiling or other features using the **cpu** or **memory** commands. Use these features at the direction of TAC only.

Viewing Logs

The system logs information for a wide variety of actions. You can use the **system support view-files** command to open a system log. Use this command while working with the Cisco Technical Assistance Center (TAC) so that they can help you interpret the output and to select the appropriate log to view.

The command presents a menu for selecting a log. Use the following commands to navigate the wizard:

- To change to a sub-directory, type in the name of the directory and press Enter.
- To select a file to view, enter **s** at the prompt. You are then prompted for a file name. You must type the complete name, and capitalization matters. The file list shows you the size of the log, which you might consider before opening very large logs.
- Press the space bar when you see **--More--** to see the next page of log entries; press Enter to see just the next log entry. When you reach the end of the log, you are taken to the main menu. The **--More--** line shows you the size of the log and how much of it you have viewed. **Use Ctrl+C to close the log and exit the command if you do not want to page through the entire log.**
- Type **b** to go up one level in the structure to the menu.

If you want to leave the log open so you can see new messages as they are added, use the **tail-logs** command instead of **system support view-files**.

The following example shows how view the `cisco/audit.log` file, which tracks attempts to log into the system. The file listing starts with directories at the top, then a list of files in the current directory.

```
> system support view-files

===View Logs===

=====
Directory: /ngfw/var/log
-----sub-dirs-----
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----files-----
2016-10-14 18:12:04.514783 | 5371          | SMART_STATUS_sda.log
```



```

2016-10-14 18:12:04.524783 | 353          | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517       | action_queue.log
2016-10-06 16:00:56.620019 | 1018         | br1.down.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

=====
Directory: /ngfw/var/log/cisco
-----files-----
2017-02-13 22:44:42.394907 | 472          | audit.log
2017-02-13 23:40:30.858198 | 903615       | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0            | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338     | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338     | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218     | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848       | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160     | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,

2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,

<remaining log truncated>

```

Creating a Troubleshooting File

Cisco Technical Assistance Center (TAC) personnel might ask you to submit system log information when you submit a problem report. This information assists them with diagnosing the problem. You do not need to submit a diagnostics file unless asked to do so.

The following procedure explains how to create and download the diagnostics file.

Procedure

-
- Step 1** Click the name of the device in the menu.
- Step 2** Under **Troubleshooting**, click **Request File to be Created** or **Re-Request File to be Created** (if you have created one before).
- The system starts generating the diagnostic file. You can go to other pages and return here to check status. When the file is ready, the date and time of the file creation is shown along with a download button.
- Step 3** When the file is ready, click the download button.

The file is downloaded to your workstation using your browser's standard download method.

Uncommon Management Tasks

The following topics cover actions you would not perform often, if ever. All of these actions result in erasing your device configuration. Ensure that the device is not currently providing critical services to a production network before making these changes.

Switching Between Local and Remote Management

You can configure and manage your device using the local FDM, which is hosted directly on the device, or remotely, using the FMC multiple device manager. You might want to use the remote manager if you want to configure features not supported by the FDM, or if you need the power and analysis capabilities available in the FMC.

You also must use the FMC if you want to run the device in transparent firewall mode.

You can switch between local and remote management without reinstalling the software. Before switching from remote to local management, verify that the FDM meets all of your configuration requirements.



Caution Switching managers erases the device configuration and returns the system to the default configuration. However, management IP address and hostname are preserved.

Before you begin

If you registered the device, especially if you enabled any feature licenses, you must unregister the device through the FDM before switching to remote management. Unregistering the device frees the base license and all feature licenses. If you do not unregister the device, those licenses remain assigned to the device in Cisco Smart Software Manager. See [Unregistering the Device](#).

Procedure

Step 1 Use an SSH client to open a connection to the **management IP address** and log into the device CLI with a username that has configuration CLI access. For example, the **admin** username.

Step 2 To switch from local to remote management:

- a) Verify you are currently in local management mode.

```
> show managers
Managed locally.
```

- b) Configure the remote manager.

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]
```

Where:

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}` specifies the DNS host name or IP address (IPv4 or IPv6) of the FMC that manages this device. If the FMC is not directly addressable, use **DONTRESOLVE**. If you use **DONTRESOLVE**, `nat_id` is required.
- `regkey` is the unique alphanumeric registration key required to register a device to the FMC.
- `nat_id` is an optional alphanumeric string used during the registration process between the FMC and the device. It is required if the hostname is set to **DONTRESOLVE**.

For example, to use the manager at 192.168.0.123 with the registration key **secret**, enter the following:

```
> configure manager add 192.168.0.123 secret
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before switching to remote management.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue [yes/no] yes
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status          :
```

Note While registration is still pending, you can use **configure manager delete** to cancel the registration and then **configure manager local** to return to local management.

- Log into the FMC and add the device.
See the FMC online help for details.

Step 3 To switch from remote management to local management:

- Verify you are currently in remote management mode.

```
> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status          :
```

- Delete the remote manager and go into no manager mode.

You cannot go directly from remote management to local management. Use the **configure manager delete** command to remove the manager.

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

- Configure the local manager.

configure manager local

For example:

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

You can now use a web browser to open the local manager at <https://management-IP-address>.

Changing the Firewall Mode

The FTD firewall can run in routed or transparent mode. A routed mode firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.

The local FDM supports routed mode only. If, however, you need to run the device in transparent mode, you can change the firewall mode and start managing the device with the FMC. Conversely, you can convert a transparent mode device to routed mode, and then you have the option to configure it with the local manager (you can also manage routed mode devices using FMC).

Regardless of local or remote management, you must use the device CLI to change the mode.

The following procedure explains how to change the mode when using the local manager, or when intending to use the local manager.



Caution Changing firewall mode erases the device configuration and returns the system to the default configuration. However, management IP address and hostname are preserved.

Before you begin

If you are converting to transparent mode, install the FMC before changing the firewall mode.

If you enabled any feature licenses, you must disable them in the FDM before deleting the local manager and switching to remote management. Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager. See [Enabling or Disabling Optional Licenses](#).

Procedure

-
- Step 1** Use an SSH client to open a connection to the **management IP address** and log into the device CLI with a username that has configuration CLI access. For example, the **admin** username.
- Step 2** To change the mode from routed to transparent and use remote management:
- a) Disable local management and enter no manager mode.

You cannot change the firewall mode while there is an active manager. Use the **configure manager delete** command to remove the manager.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

- b) Change the firewall mode to transparent.

configure firewall transparent

Example:

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

- c) Configure the remote manager.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

Where:

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} specifies the DNS host name or IP address (IPv4 or IPv6) of the FMC that manages this device. If the FMC is not directly addressable, use **DONTRESOLVE**. If you use **DONTRESOLVE**, *nat_id* is required.
- *regkey* is the unique alphanumeric registration key required to register a device to the FMC.
- *nat_id* is an optional alphanumeric string used during the registration process between the FMC and the device. It is required if the hostname is set to **DONTRESOLVE**.

For example, to use the manager at 192.168.0.123 with the registration key **secret**, enter the following:

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status         :
```

- d) Log into the FMC and add the device.

See the FMC online help for details.

Step 3 To change the mode from transparent to routed and convert to local management:

- a) Deregister the device from the FMC.
- b) Access the FTD device CLI, preferably from the console port.

Because changing the mode erases your configuration, the management IP address will revert to the default, so you might lose an SSH connection to the management IP address after changing modes.

- c) Change the firewall mode to routed.

configure firewall routed

Example:

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

- d) Enable the local manager.

configure manager local

For example:

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

You can now use a web browser to open the local manager at **https://management-IP-address**.

Resetting the Configuration

You can reset the system configuration to the factory default if you want to start over. Although you cannot directly reset the configuration, deleting and adding the manager clears the configuration.

If your intention is to wipe away the configuration and then recover a backup, ensure that you have already download the backup copy you want to restore. You will need to upload it after resetting the system so that you can restore it.

Before you begin

If you enabled any feature licenses, you must disable them in the FDM before deleting the local manager. Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager. See [Enabling or Disabling Optional Licenses](#).

Procedure

Step 1 Use an SSH client to open a connection to the management IP address and log into the device CLI with a username that has configuration CLI access. For example, the **admin** username.

Step 2 Use the **configure manager delete** command to remove the manager.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

Step 3 Configure the local manager.

configure manager local

For example:

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

You can now use a web browser to open the local manager at **<https://management-IP-address>**. By clearing the configuration, you will be prompted to complete the device setup wizard.
