Backup/Restore

About Backup and Restore

The ability to recover from a disaster is an essential part of any system maintenance plan. As part of your disaster recovery plan, we recommend that you perform periodic backups to a secure remote location.

What Is Backed Up?

Device backups are always configuration-only. Management center backups are as follows.

Table 1: Management Center Backups

Backup Type	Backed Up	Not Backed Up
Configurations	Most configurations are backed up. Configuration backups also include locally stored reports. In a multidomain deployment, you must back up configurations. You cannot back up events or TID data only.	These configurations are not backed up and must be reconfigured after restore: • Remote storage settings. • Audit log server sertificate settings. • Public and private AMP cloud connections, in Version.
Events	All events in the FMC database.	Intrusion event review status is not backed up. Restored intrusion events do not appear on Reviewed Events pages.

Backup Type	Backed Up	Not Backed Up
Threat Intelligence Director (TID) data.	For more information, see *About Backing Up and Restoring TID Data* in the Firepower Management Center Device Configuration Guide.	

What Is Restored?

Restoring configurations overwrites *all* backed-up configurations, with very few exceptions. On the FMC, restoring events and TID data overwrites *all* existing events and TID data, with the exception of intrusion events.

Make sure you understand and plan for the following:

- You cannot restore what is not backed up, as decribed above.
- Restoring fails VPN certificates.

  The FTD restore process removes VPN certificates and all VPN configurations from FTD devices, including certificates added after the backup was taken. After you restore the FTD device, you must re-add/re-enroll all VPN certificates, and redeploy the device.
- Restoring to a configured FMC — instead of factory-fresh or reimaged — merges intrusion events and file lists.

  The FMC event restore process does not overwrite intrusion events. Instead, the intrusion events in the backup are added to the database. To avoid duplicates, delete existing intrusion events before you restore.

  The FMC configuration restore process does not overwrite clean and custom detection file lists used by AMP for Networks. Instead, it merges existing file lists with the file lists in the backup. To replace file lists, delete existing file lists before you restore.

On-Demand Backups

You can perform on-demand backups for the FMC and many FTD devices from the FMC.

For more information, see Backing Up FMCs or Managed Devices, on page 9.

Scheduled Backups

You can use the scheduler on FMC to automate backups. You can also schedule remote device backups from the FMC.

The FMC setup process schedules weekly configuration-only backups, to be stored locally. This is not a substitute for full off-site backups—after initial setup finishes, you should review your scheduled tasks and adjust them to fit your organization's needs.

For more information, see Scheduled Backups.

Storing Backup Files

You can store backups locally. However, we recommend you back up FMCs and managed devices to a secure remote location by mounting an NFS, SMB, or SSHFS network volume as remote storage. After you do this, all subsequent backups are copied to that volume, but you can still use the FMC to manage them.

For more information, see Remote Storage Device and Manage Backups and Remote Storage, on page 28.

Restoring from Backup

You restore the FMC from the Backup Management page. You must use the FTD CLI to restore FTD devices, except for the ISA 3000 zero-touch restore, which uses an SD card and the reset button.

For more information, see Restoring FMCs and Managed Devices, on page 14.

Requirements for Backup and Restore

Backup and restore have the following requirements.

Platform Requirements: Backup

This table lists backup support by platform. Device backup is supported for both application and container instances.

Table 2: Backup Support by Platform

Platform	Backup Supported?		
	Standalone	**High Availability**	**Clusters**
Management center, hardware and virtual	**YES**	**YES**	—
Threat defense hardware	**YES**	**YES**	—
Threat defense virtual, on-prem/private cloud	VMware HyperFlex Nutanix OpenStack	VMware	—
Threat defense virtual, public cloud	—	—	—

Platform Requirements: Restore

A replacement managed device must be the same model as the one you are replacing, with the same number of network modules and same type and number of physical interfaces.

For FMCs, you can use backup and restore not only in an RMA scenario, but also to migrate configurations and events between FMCs. For details, including supported target and destination models, see the Cisco Secure Firewall Management Center Model Migration Guide.

Version Requirements

As the first step in any backup, note the patch level. To restore a backup, the old and the new appliance must be running the same software version, including patches. To restore to a Firepower 4100/9300 chassis, you must be running a compatible FXOS.

For FMC backups, you are *not* required to have the same VDB or SRU. Note, however, that restoring a backup replaces the existing VDB with the VDB in the backup file. If the restored SRU or the VDB version is older than the one available on the Cisco Support & Download site, we recommend you install the newer version.

License Requirements

Address licensing or orphan entitlements concerns as described in the best practices and procedures. If you notice licensing conflicts, contact Cisco TAC.

Domain Requirements

To:

- Back up or restore the FMC: Global only.
- Back up a device from the FMC: Global only.
- Restore a device: None. Restore devices locally at the CLI.

In a multidomain deployment you cannot back up only events/TID data. You must also back up configurations.

Guidelines and Limitations for Backup and Restore

Backup and restore has the following guidelines and limitations.

Backup and Restore is for Disaster Recovery/RMA

Backup and restore is primarily intended for RMA scenarios. Before you begin the restore process of a faulty or failed physical appliance, contact Cisco TAC for replacement hardware.

You can also use backup and restore to migrate configurations and events between FMCs. This makes it easier to replace FMCs due to technical or business reasons such as a growing organization, migration from a physical to a virtual implementation, hardware refresh, and so on.

Restore on a Reimaged Management Center

Always restore the FMC on a freshly reimaged FMC. If you are restoring without reimaging and if you had registered FTD on the FMC after backing up, then when you register the device again on the restored FMC, you will encounter device registration failure due to certification error. This error occurs due to the mismatch in the restored certificate database and the non-reimaged FMC backup that is restored to.

Backup and Restore is not Configuration Import/Export

A backup file contains information that uniquely identifies an appliance, and cannot be shared. Do not use the backup and restore process to copy configurations between appliances or devices, or as a way to save configurations while testing new ones. Instead, use the import/export feature.

For example, FTD device backups include the device's management IP address and all information the device needs to connect to its managing FMC. Do not restore the FTD backup to a device being managed by a different FMC; the restored device will attempt to connect to the FMC specified in the backup.

Restore is Individual and Local

You restore to FMCs and managed devices individually and locally. This means:

- You cannot batch-restore to high availability FMCs or devices.
- You cannot use the FMC to restore a device. For the FMC, you can use the web interface to restore. For FTD devices, you must use the FTD CLI, except for the ISA 3000 zero-touch restore, which uses an SD card and the reset button.
- While restoring the FMC from backup the health policy is also restored. However, any updates to the health monitoring settings are not deployed to devices. You must redeploy all health policies after a successful restore to avoid any discrepancy in health monitoring.
- You cannot use FMC user accounts to log into and restore one of its managed devices. The FMC and devices maintain their own user accounts.

Strong Encryption in the Restore Device

Ensure that the same strong encryption configuration that was available during the backup is present in the FTD unit that is being restored. Otherwise, the HA peers may enter a split-brain state.

Configuration Import/Export Guidelines for Firepower 4100/9300

You can use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server or your local computer. You can later import that configuration file to quickly apply the configuration settings to your Firepower 4100/9300 chassis to return to a known good configuration or to recover from a system failure.

Guidelines and Restrictions

- Do not modify the contents of the configuration file. If a configuration file is modified, configuration import using that file might fail.
- Application-specific configuration settings are not contained in the configuration file. You must use the configuration backup tools provided by the application to manage application-specific settings and configurations.
- When you import a configuration to the chassis, all existing configuration on the chassis (including any logical devices) are deleted and completely replaced by the configuration contained in the import file.
- Except in an RMA scenario, we recommend you only import a configuration file to the same chassis where the configuration was exported.
- The platform software version of the Firepower 4100/9300 chassis where you are importing should be the same version as when the export was taken. If not, the import operation is not guaranteed to be successful. We recommend you export a backup configuration whenever the chassis is upgraded or downgraded.
- The Firepower 4100/9300 chassis where you are importing must have the same Network Modules installed in the same slots as when the export was taken.
- The Firepower 4100/9300 chassis where you are importing must have the correct software application images installed for any logical devices defined in the export file that you are importing.
- To avoid overwriting existing backup files, change the file name in the backup operation or copy the existing file to another location.

Note You must backup the logicl APP separately as the FXOS import/export will backup only the FXOS configuration. The FXOS configuration import will cause logical device reboot and it rebuilds the device with the factory default configuration.

Best Practices for Backup and Restore

Backup and restore has the following best practices.

When to Back Up

We recommend backing up during a maintenance window or other time of low use.

While the system collects backup data, there may be a temporary pause in data correlation (FMC only), and you may be prevented from changing configurations related to the backup. If you include event data, event-related features such as eStreamer are not available.

You should back up in the following situations:

- Regular scheduled or on-demand backups.

  As part of your disaster recovery plan, we recommend that you perform periodic backups.

  The FMC setup process schedules weekly configuration-only backups, to be stored locally. This is not a substitute for full off-site backups—after initial setup finishes, you should review your scheduled tasks and adjust them to fit your organization's needs. For more information, see Scheduled Backups.

- After SLR changes.

  Back up the FMC after you make changes to Specific Licensing Reservations (SLRs). If you make changes and then restore an older backup, you will have issues with your Specific Licensing return code and can accrue orphan entitlements.

- Before upgrade or reimage.

  If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly.

Note Restoring from a backup does not reset the password that you had configured after the reimage or an RMA.

- After upgrade.

  Back up after you upgrade, so you have a snapshot of your freshly upgraded deployment. We recommend you back up the FMC *after* you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.

Maintaining Backup File Security

Backups are stored as unencrypted archive (.tar) files.

Private keys in PKI objects—which represent the public key certificates and paired private keys required to support your deployment—are decrypted before they are backed up. The keys are reencrypted with a randomly generated key when you restore the backup.

Note We recommend you back up FMCs and devices to a secure remote location and verify transfer success. Backups left locally may be deleted, either manually or by the upgrade process, which purges locally stored backups.

Especially because backup files are unencrypted, do *not* allow unauthorized access. If backup files are modified, the restore process will fail. Keep in mind that anyone with the Admin/Maint role can access the Backup Management page, where they can move and delete files from remote storage.

In the FMC's system configuration, you can mount an NFS, SMB, or SSHFS network volume as remote storage. After you do this, all subsequent backups are copied to that volume, but you can still use the FMC to manage them. For more information, see Remote Storage Device and Manage Backups and Remote Storage, on page 28.

Note that only the FMC mounts the network volume. Managed device backup files are routed through the FMC. Make sure you have the bandwidth to perform a large data transfer between the FMC and its devices. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Backup and Restore in FMC High Availability Deployments

In FMC high availability deployments, backing up one FMC does not back up the other. You should regularly back up both peers. Do not restore one HA peer with the backup file from the other. A backup file contains information that uniquely identifies an appliance, and cannot be shared.

Note that you can replace an HA FMC without a successful backup. For more information on replacing HA FMCs, both with and without successful backups, see Replacing FMCs in a High Availability Pair.

Backup and Restore in FTD High Availability Deployments

In the FTD high availability deployment, you should:

- Back up the device pair from the FMC, but restore individually and locally from the FTD CLI.

  The backup process produces unique backup files each peer. Do not restore one peer with the backup file from the other. A backup file contains information that uniquely identifies an appliance, and cannot be shared.

  The device's role is also noted in its backup file name. When you restore, make sure you choose the appropriate backup file: primary vs secondary.

- Do *not* suspend or break high availability before you restore.

  Maintaining the high availability configuration ensures replacement devices can easily reconnect after restore. Note that you will have to resume high availability synchronization to make this happen.

- Do *not* run the **restore** CLI command on both peers at the same time.

  Assuming you have successful backups, you can replace either or both peers. Any physical replacement tasks you can perform simultaneously: unracking, reracking, and so on. However, do *not* run the **restore** command on the second device until the restore process completes for the first device, including the reboot.

- When both peers fail, before the devices are decommissioned, ensure that unregister them both from the FMC.

Note that you can replace a high availability device without a successful backup.

Backup and Restore for Firepower 4100/9300 Chassis

To restore FTD software on a Firepower 4100/9300 chassis, the chassis must be running a compatible FXOS version. When you back up a Firepower 4100/9300 chassis, we strongly recommend you also back up FXOS configurations. For additional best practices, see Configuration Import/Export Guidelines for Firepower 4100/9300 , on page 5.

Before Backup

Before you back up, you should:

- Update the VDB and SRU on the FMC.

  We always recommend you use the latest vulnerability database (VDB) and intrusion rules (SRU). Before you back up the FMC, check the Cisco Support & Download site for newer versions.

- Check disk space.

  Before you begin a backup, make sure you have enough disk space on the appliance or on your remote storage server. The space available is displayed on the Backup Management page.

  Backups can fail if there is not enough space. Especially if you schedule backups, make sure you regularly prune backup files or allocate more disk space to the remote storage location.

Before Restore

Before restore, you should:

- Revert licensing changes.

  Revert any licensing changes made since you took the backup.

  Otherwise, you may have license conflicts or orphan entitlements after the restore. However, do *not* unregister from Cisco Smart Software Manager (CSSM). If you unregister from CSSM, you must unregister again after you restore, then re-register.

  After the restore completes, reconfigure licensing. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.

- Disconnect faulty appliances.

  Disconnect the management interface, and for devices, the data interfaces.

  Restoring FTD devices sets the management IP address of the replacement device to the management IP address of the old device. To avoid IP conflicts, disconnect the old device from the management network before you restore the backup on its replacement.

  Note that restoring the FMC does *not* change the management IP address. You must set that manually on the replacement — just make sure you disconnect the old appliance from the network before you do.

- Do *not* unregister managed devices.

  Whether you are restoring the FMC or managed device, do not unregister devices from the FMC, even if you physically disconnect an appliance from the network.

If you unregister, you will need to redo some device configurations, such as security zone to interface mappings. After you restore, the FMC and devices should begin communicating normally.

- Reimage.

  In an RMA scenario, the replacement appliance will arrive configured with factory defaults. However, if the replacement appliance is already configured, we recommend you reimage. Reimaging returns most settings to factory defaults, including the system password. You can only reimage to major versions, so you may need to patch after you reimage.

  If you do not reimage, keep in mind that FMC intrusion events and file lists are merged rather than overwritten.

After Restore

After restore, you should:

- Reconfigure anything that was not restored.

  This can include reconfiguring licensing, remote storage, and audit log server certificate settings. You also must re-add/re-enroll failed FTD VPN certificates.

- Update the VDB and SRU on the FMC.

  We always recommend you use the latest vulnerability database (VDB) and intrusion rules (SRU). This is especially important for the VDB, because the VDB in the backup will overwrite the VDB on the replacement FMC.

- Deploy.

  Whether you are restoring the FMC or device, you must deploy. For a restored device, you may need to force deploy: see *Redeploy Existing Configurations to a Device* in the Firepower Management Center Device Configuration Guide.

Backing Up FMCs or Managed Devices

You can perform on-demand or scheduled backups for supported appliances.

You do not need a backup profile to back up devices from the FMC. However, FMC backups require backup profiles. The on-demand backup process allows you to create a new backup profile.

Back up the FMC

Use this procedure to perform an on-demand FMC backup.

Before you begin

You must read and understand the requirements, guidelines, limitations, and best practices. You do not want to skip any steps or ignore security concerns. Careful planning and preparation can help you avoid missteps.

- Requirements for Backup and Restore, on page 3
- Guidelines and Limitations for Backup and Restore, on page 4
- Best Practices for Backup and Restore, on page 6

Procedure

Step 1 Select **System** (⚙) > **Tools** > **Backup/Restore**.

The Backup Management page lists all locally and remotely stored backups. It also lists how much disk space you have available to store backups. Backups can fail if there is not enough space.

Step 2 Choose whether to use an existing backup profile or start fresh.

FMC backups require that you use or create a backup profile.

- Click **Backup Profiles** to use an existing backup profile.

  Next to the profile you want to use, click the edit icon. You can then click **Start Backup** to begin the backup right now. Or, if you want to edit the profile, go on to the next step.

- Click to start fresh and create a new backup profile.

  Enter a **Name** for the backup profile.

Step 3 Choose what to back up:

- **Back Up Configuration**
- **Back Up Events**
- **Back Up Threat Intelligence Director**

In a multidomain deployment, you must back up configurations. You cannot back up events or TID data only. For details on what is and what is not backed up for each of these choices, see About Backup and Restore, on page 1.

Step 4 Note the **Storage Location** for FMC backup files.

This will either be local storage in `/var/sf/backup/`, or a remote network volume. For more information, see Manage Backups and Remote Storage, on page 28.

Step 5 (Optional) Enable **Copy when complete** to copy completed FMC backups to a remote server.

Provide a hostname or IP address, the path to the remote directory, and a username and password. To use an SSH public key instead of a password, copy the contents of the **SSH Public Key** field to the specified user's `authorized_keys` file on the remote server.

Note
This option is useful if you want to store backups locally and also SCP them to a remote location. If you configured SSH remote storage, do *not* copy backup files to the same directory using **Copy when complete**.

Step 6 (Optional) Enable **Email** and enter an email address to be notified when the backup completes.

To receive email notifications, you must configure the FMC to connect to a mail server: Configuring a Mail Relay Host and Notification Address.

Step 7 Click **Start Backup** to start the on-demand backup.

If you are not using an existing backup profile, the system automatically creates one and uses it. If you decide not to run the backup now, you can click **Save** or **Save As New** to save the profile. In either case, you can use the newly created profile to configure scheduled backups.

Note
If you configured remote storage and due to connectivity issues, backup to remote storage may fail. In such cases, if the local management center has atleast 30% of free space, the generated backup file is stored in the local, replacing the oldest local management center backup.

Step 8 Monitor progress in the Message Center.

While the system collects backup data, there may be a temporary pause in data correlation, and you may be prevented from changing configurations related to the backup. If you configured remote storage or enabled **Copy when complete**, the FMC may write temporary files to the remote server. These files are cleaned up at the end of the backup process.

What to do next

If you configured remote storage or enabled **Copy when complete**, verify transfer success of the backup file.

Back up a Device from the FMC

Use this procedure to perform an on-demand device backup.

Before you begin

You must read and understand the requirements, guidelines, limitations, and best practices. You do not want to skip any steps or ignore security concerns. Careful planning and preparation can help you avoid missteps.

- Requirements for Backup and Restore, on page 3
- Guidelines and Limitations for Backup and Restore, on page 4
- Best Practices for Backup and Restore, on page 6

If you are backing up a Firepower 4100/9300 chassis, it is especially important that you also back up FXOS configurations: Exporting an FXOS Configuration File, on page 12.

Procedure

Step 1 Select **System** (⚙) > **Tools** > **Backup/Restore**, then click **Managed Device Backup**.

Step 2 Select one or more **Managed Devices**.

Step 3 Determine where you want to store the backup file. It can be in one of these locations:

- Local storage in FMC at `/var/sf/remote-backup/`.
- Local storage in FTD at `/var/sf/backup`. For Cluster devices, this option is not available.

- Remote location in a remote network volume. For the ISA 3000, if you have an SD card installed, a copy of the backup will also be made on the SD card at `/mnt/disk3/backup`. For more information, see Manage Backups and Remote Storage, on page 28.

Step 4 If remote storage is configured and enabled. You can choose whether you want to save the backup to remote server or to the device using the **Retrieve to Management Center** check box:

- Enabled (default): Saves the backup to the configured location in the remote server.
- Disabled: Saves the backup to the device in `/var/sf/backup`.

Step 5 If you did not configure or did not enable remote storage, by default, the backup is saved to the local storage in the FMC. Choose whether you want to save the backup to FMC or to the device :

- Enabled (default): Saves the backup to the FMC in `/var/sf/remote-backup/`.
- Disabled: Saves the backup to the device in `/var/sf/backup`.

Step 6 Click **Start Backup** to start the on-demand backup.

Step 7 Monitor progress in the Message Center.

What to do next

If you configured remote storage, verify if the transfer of the backup file was successful.

Exporting an FXOS Configuration File

Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis to a remote server or your local computer.

Note This procedure explains how to use Firepower Chassis Manager to export FXOS configurations when you back up Firepower Threat Defense. For the CLI procedure, see the appropriate version of the Cisco Firepower 4100/9300 FXOS CLI Configuration Guide.

Before you begin

Review the Guidelines and Restrictions.

Procedure

Step 1 Choose **System** > **Configuration** > **Export** on the Firepower Chassis Manager.

Step 2 To export a configuration file to your local computer:

a) Click **Local**.

b) Click **Export**.
The configuration file is created and, depending on your browser, the file might be automatically downloaded to your default download location or you might be prompted to save the file.

Step 3 To export the configuration file to a remote server:

a) Click **Remote**.
b) Choose the protocol to use when communicating with the remote server. This can be one of the following: FTP, TFTP, SCP, or SFTP.
c) Enter the hostname or IP address of the location where the backup file should be stored. This can be a server, storage array, local drive, or any read/write media that the Firepower 4100/9300 chassis can access through the network.

   If you use a hostname rather than an IP address, you must configure a DNS server.

d) If you are using a non-default port, enter the port number in the **Port** field.
e) Enter the username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
f) Enter the password for the remote server username. This field does not apply if the protocol is TFTP.

   Note
   The password must not exceed 64 characters. If you enter a password more than 64 character, Firepower Chassis Manager will display an error stating that `property pwd of org-root/cfg-exp-policy-default is out of range.`

g) In the **Location** field, enter the full path to where you want the configuration file exported including the filename.
h) Click **Export**.
   The configuration file is created and exported to the specified location.

Create a Backup Profile

A backup profile is a saved set of preferences—what to back up, where to store the backup file, and so on.

FMC backups require backup profiles. Backup profiles are not required to back up a device from the FMC.

When you perform an on-demand FMC backup, if you do not pick an existing backup profile, the system automatically creates one and uses it. You can then use the newly created profile to configure scheduled backups.

The following procedure explains how to create a backup profile without performing an on-demand backup.

Procedure

Step 1 Select **System** (⚙) > **Tools** > **Backup/Restore**, then click **Backup Profiles**.

Step 2 Click **Create Profile** and enter a **Name**.

Step 3 Choose what to back up.

- **Back Up Configuration**
- **Back Up Events**
- **Back Up Threat Intelligence Director**

In a multidomain deployment, you must back up configurations. You cannot back up events or TID data only. For details on what is and what is not backed up for each of these choices, see About Backup and Restore, on page 1.

Step 4 Note the **Storage Location** for backup files.

This will either be local storage in `/var/sf/backup/`, or a remote network volume. For the ISA 3000, if you have an SD card installed, a copy of the backup will also be made on the SD card at `/mnt/disk3/backup`. For more information, see Manage Backups and Remote Storage, on page 28.

Step 5 (Optional) Enable **Copy when complete** to copy completed FMC backups to a remote server.

Provide a hostname or IP address, the path to the remote directory, and a username and password. To use an SSH public key instead of a password, copy the contents of the **SSH Public Key** field to the specified user's `authorized_keys` file on the remote server.

Note
This option is useful if you want to store backups locally and also SCP them to a remote location. If you configured SSHFS remote storage, do *not* copy backup files to the same directory using **Copy when complete**.

Step 6 (Optional) Enable **Email** and enter an email address to be notified when the backup completes.

To receive email notifications, you must configure the FMC to connect to a mail server: Configuring a Mail Relay Host and Notification Address.

Step 7 Click **Save**.

Restoring FMCs and Managed Devices

For the FMC, you use the web interface to restore from backup. For FTD devices, you must use the FTD CLI. You cannot use the FMC to restore a device.

The following sections explain how to restore FMCs and managed devices.

Restore FMC from Backup

When you restore FMC backups, you can choose to restore any or all of the components included in the backup file (events, configurations, TID data).

Note Restoring configuration data overwrites *all* configurations, with very few exceptions. Replacing configuration-only data does not restore event data, security logs, or operational history. It also reboots the FMC. Restoring events and TID data overwrites *all* existing events and TID data, with the exception of intrusion events. Make sure you are ready.

Use this procedure to restore the FMC from backup. For more information on backup and restore in FMC HA deployments, see Replacing FMCs in a High Availability Pair.

Before you begin

You must read and understand the requirements, guidelines, limitations, and best practices. You do not want to skip any steps or ignore security concerns. Careful planning and preparation can help you avoid missteps.

- Requirements for Backup and Restore, on page 3
- Guidelines and Limitations for Backup and Restore, on page 4
- Best Practices for Backup and Restore, on page 6

Procedure

Step 1 Log into the FMC you want to restore.

Step 2 Select **System** (⚙) > **Tools** > **Backup/Restore**.

The Backup Management page lists all locally and remotely stored backup files. You can click a backup file to view its contents.

If the backup file is not in the list and you have it saved on your local computer, click **Upload Backup**; see Manage Backups and Remote Storage, on page 28.

Step 3 Select the backup file you want to restore and click **Restore**.

Step 4 Select from the available components to restore, then click **Restore** again to begin.

Step 5 Monitor progress in the Message Center.

If you are restoring configurations, you can log back in after the FMC reboots.

What to do next

- If necessary, reconfigure any licensing settings that you reverted before the restore. If you notice licensing conflicts or orphan entitlements, contact Cisco TAC.
- If necessary, reconfigure remote storage and audit log server certificate settings. These settings are not included in backups.
- Update the SRU and VDB. If the restored SRU or the VDB version is older than the one available on the Cisco Support & Download site, ensure to update the VDB to the latest version before deploying any changes to the device.
- Deploy configuration changes; see the Firepower Management Center Device Configuration Guide.

Restore FTD from Backup: Firepower 1000/2100, Secure Firewall 3100, ISA 3000 (Non-Zero-Touch)

Device backup and restore is intended for RMA. Restoring configurations overwrites *all* configurations on the device, including the management IP address. It also reboots the device.

In case of hardware failure, this procedure outlines how to replace the Secure Firewall 1000/2100/3100/ISA 3000, standalone or high availability. It assumes you have access to a successful backup of the device or

devices you are replacing; see Back up a Device from the FMC, on page 11. For zero-touch restore on the ISA 3000 using an SD card, see Zero-Touch Restore FTD from Backup: ISA 3000, on page 18.

For high availability devices, you can use this procedure to replace all peers. To replace all, perform all steps on all devices simultaneously, except the **restore** CLI command itself.

Note Do *not* unregister from the FMC, even when disconnecting a device from the network. For FTD high availability devices, do *not* suspend or break high availability. Maintaining these links ensures replacement devices can automatically reconnect after restore.

Before you begin

You must read and understand the requirements, guidelines, limitations, and best practices. You do not want to skip any steps or ignore security concerns. Careful planning and preparation can help you avoid missteps.

- Requirements for Backup and Restore, on page 3
- Guidelines and Limitations for Backup and Restore, on page 4
- Best Practices for Backup and Restore, on page 6

Procedure

Step 1 Contact Cisco TAC for replacement hardware.

Obtain an identical model, with the same number of network modules and same type and number of physical interfaces. You can begin the RMA process from the Cisco Returns Portal.

Step 2 Locate a successful backup of the faulty device.

Depending on your backup configuration, device backups may be stored:

- On the faulty device itself in `/var/sf/backup`.
- On the FMC in `/var/sf/remote-backup`.
- In a remote storage location.

For FTD high availability devices, you back up the group as a unit. For high availability devices, the backup process produces unique backup files, with each device's role indicated in the backup file name.

If the only copy of the backup is on the faulty device, copy it somewhere else now. If you reimage the device, the backup will be erased. If something else goes wrong, you may not be able to recover the backup. For more information, see Manage Backups and Remote Storage, on page 28.

The replacement device will need the backup, but can retrieve it with SCP during the restore process. We recommend you put the backup somewhere SCP-accessible to the replacement device. Or, you can copy the backup to the replacement device itself.

Step 3 Remove (unrack) the faulty device.

Disconnect all interfaces. In FTD high availability deployments, this includes the failover link.

See the hardware installation and getting started guides for your model: http://www.cisco.com/go/ftd-quick.

Note
Do *not* unregister from the FMC, even when disconnecting a device from the network. For FTD high availability devices, do *not* suspend or break high availability. Maintaining these links ensures replacement devices can automatically reconnect after restore.

Step 4 Install the replacement device and connect it to the management network.

Connect the device to power and the management interface to the management network. In FTD high availability deployments, connect the failover link. However, do *not* connect the data interfaces.

See the hardware installation guide for your model: http://www.cisco.com/go/ftd-quick.

Step 5 (Optional) Reimage the replacement device.

In an RMA scenario, the replacement device will arrive configured with factory defaults. If the replacement device is not running the same major version as the faulty device, we recommend you reimage.

See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

Step 6 Perform initial configuration on the replacement device.

Access the FTD CLI as the `admin` user. A setup wizard prompts you to configure the management IP address, gateway, and other basic network settings.

Do not set the same management IP address as the faulty device. This can cause problems if you need to register the device in order to patch it. The restore process will correctly reset the management IP address.

See the initial configuration topics in the getting started guide for your model: http://www.cisco.com/go/ftd-quick.

Note
If you need to patch the replacement device, start the FMC registration process as described in the getting started guide. If you do not need to patch, do *not* register.

Step 7 Make sure the replacement device is running the same software version, *including patches*, as the faulty device.

Ensure that the existing device should not be deleted from the FMC. The replacement device should be unmanaged from the physical network and the new hardware as well as the replacing FTD patch should have the same version. The FTD CLI does not have an upgrade command. To patch:

a) From the FMC web interface, complete the device registration process.

   Create a new AC policy and use the default action "Network Discovery". Leave this policy as is; do not add any features or modifications. This is being used to register the device and deploy a policy with no features so that you do not require licenses, and you will then be able to patch the device. Once backup is restored, it should restore the licensing and policy into the expected state.

b) Patch the device: https://www.cisco.com/go/ftd-upgrade.

c) Unregister the freshly patched device from the FMC.

   If you do not unregister, you will have a ghost device registered to the FMC after the restore process brings your "old" device back up.

Step 8 Make sure the replacement device has access to the backup file.

The restore process can retrieve the backup with SCP, so we recommend you put the backup somewhere accessible. Or, you can manually copy the backup to the replacement device itself, to `/var/sf/backup`.

Step 9 From the FTD CLI, restore the backup.

Access the FTD CLI as the `admin` user. You can use the console or you can SSH to the newly configured management interface (IP address or hostname). Keep in mind that the restore process will change this IP address.

To restore:

- With SCP: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- From the local device: **restore remote-manager-backup** *backup tar-file*

In FTD high availability deployments, make sure you choose the appropriate backup file: primary vs secondary. The role is noted in the backup file name. If you are restoring all devices, do this sequentially. Do not run the **restore** command on the next device until the restore process completes for the first device, including the reboot.

Step 10 Log into the FMC and wait for the replacement device to connect.

When the restore is done, the device logs you out of the CLI, reboots, and automatically connects to the FMC. At this time, the device should appear out of date.

Step 11 Before you deploy, perform any post-restore tasks and resolve any post-restore issues:

- Resolve licensing conflicts or orphan entitlements. Contact Cisco TAC.
- Resume high availability synchronization. From the FTD CLI , enter `configure high-availability resume`. See *Suspend and Resume High Availability* in the Firepower Management Center Device Configuration Guide.
- Re-add/re-enroll all VPN certificates. The restore process removes VPN certificates from FTD devices, including certificates added after the backup was taken. See *Managing VPN Certificates* in the Firepower Management Center Device Configuration Guide.

Step 12 Deploy configurations.

You must deploy. After you restore a device, you must force deploy from the Device Management page. See *Redeploy Existing Configurations to a Device* in the Firepower Management Center Device Configuration Guide.

Step 13 Connect the device's data interfaces.

See the hardware installation guide for your model: http://www.cisco.com/go/ftd-quick.

What to do next

Verify that the restore succeeded and the replacement device is passing traffic as expected.

Zero-Touch Restore FTD from Backup: ISA 3000

Device backup and restore is intended for RMA. Restoring configurations overwrites *all* configurations on the device, including the management IP address. It also reboots the device.

In case of hardware failure, this procedure outlines how to replace the ISA 3000, either standalone or in an HA pair. It assumes you have a backup of the failed unit on an SD card; see Back up a Device from the FMC, on page 11.

For high availability devices, you can use this procedure to replace all peers. To replace all, perform all steps on all devices simultaneously, except the **restore** CLI command itself.

Note Do *not* unregister from the FMC, even when disconnecting a device from the network. For FTD high availability devices, do *not* suspend or break high availability. Maintaining these links ensures replacement devices can automatically reconnect after restore.

Before you begin

You must read and understand the requirements, guidelines, limitations, and best practices. You do not want to skip any steps or ignore security concerns. Careful planning and preparation can help you avoid missteps.

- Requirements for Backup and Restore, on page 3
- Guidelines and Limitations for Backup and Restore, on page 4
- Best Practices for Backup and Restore, on page 6

Procedure

Step 1 Contact Cisco TAC for replacement hardware.

Obtain an identical model, with the same number of network modules and same type and number of physical interfaces. You can begin the RMA process from the Cisco Returns Portal.

Step 2 Remove the SD card from the faulty device, and unrack the device.

Disconnect all interfaces. In FTD HA deployments, this includes the failover link.

Note
Do *not* unregister from the FMC, even when disconnecting a device from the network. For FTD high availability devices, do *not* suspend or break high availability. Maintaining these links ensures replacement devices can automatically reconnect after restore.

Step 3 Rerack the replacement device, and connect it to the management network. In FTD HA deployments, connect the failover link. However, do *not* connect the data interfaces.

If you need to reimage the device or apply a software patch, connect the power connector.

Step 4 (May be required) Reimage the replacement device.

In an RMA scenario, the replacement device will arrive configured with factory defaults. If the replacement device is not running the same major version as the faulty device, you need to reimage. Obtain the installer from https://www.cisco.com/go/isa3000-software.

See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide to reimage.

Step 5 (May be required) Make sure the replacement device is running the same Firepower software version, *including the same patch version*, as the faulty device. If you need to patch the device, you can connect to Firepower Device Manager (FDM) to install the patch.

The following procedure assumes you have a factory default configuration. If you already configured the device, you can log into FDM and go directly to the **Device** > **Upgrades** page to install the patch.

In either case, obtain the patch package from https://www.cisco.com/go/isa3000-software.

a) Connect your computer directly to the inside (Ethernet 1/2) interface, and access FDM on the default IP address: **https://192.168.95.1**.
b) Enter the **admin** username and the default password **Admin123**, then click **Login**.
c) Complete the setup wizard. Keep in mind that you are not going to retain anything you configure in FDM; you only want to get past any initial configuration so you can apply the patches, so it doesn't matter what you enter in the setup wizard.
d) Go to the **Device** > **Upgrades** page.

   The **System Upgrade** section shows the currently running software version.

e) Upload the patch file by clicking **Browse**.
f) Click **Install** to start the installation process.

   Information next to the icon indicates whether the device will reboot during installation. You are automatically logged out of the system. Installation might take 30 minutes or more.

   Wait before logging into the system again. The Device Summary, or System monitoring dashboard, should show the new version.

   Note
   Do not simply refresh the browser window. Instead, delete any path from the URL, and reconnect to the home page. This ensures that cached information gets refreshed with the latest code.

Step 6 Insert the SD card in the replacement device.

Step 7 Power on or reboot the device and shortly after it starts the bootup, depress and hold the Reset button for no fewer than 3 seconds and no longer than 15 seconds.

If you used FDM to install a patch, you can reboot from the **Device** > **System Settings** > **Reboot/Shutdown** page. From the FTD CLI, use the **reboot** command. If you have not yet attached power, attach it now.

Use a standard size #1 paper clip with wire gauge 0.033 inch or smaller to depress the Reset button. The restoration process is triggered during bootup. The device restores the configuration, and then reboots. The device will then register with the FMC automatically.

If you are restoring both devices in an HA pair, do this sequentially. Do not restore the second device until the restore process completes for the first device, including the reboot.

Step 8 Log into the FMC and wait for the replacement device to connect.

At this time, the device should appear out of date.

Step 9 Before you deploy, perform any post-restore tasks and resolve any post-restore issues:

- Resolve licensing conflicts or orphan entitlements. Contact Cisco TAC.
- Resume high availability synchronization. From the FTD CLI , enter `configure high-availability resume`. See *Suspend and Resume High Availability* in the Firepower Management Center Device Configuration Guide.

- Re-add/re-enroll all VPN certificates. The restore process removes VPN certificates from FTD devices, including certificates added after the backup was taken. See *Managing VPN Certificates* in the Firepower Management Center Device Configuration Guide.

Step 10 Deploy configurations.

You must deploy. After you restore a device, you must force deploy from the Device Management page. See *Redeploy Existing Configurations to a Device* in the Firepower Management Center Device Configuration Guide.

Step 11 Connect the device's data interfaces.

See the hardware installation guide for your model: http://www.cisco.com/go/ftd-quick.

What to do next

Verify that the restore succeeded and the replacement device is passing traffic as expected.

Restore FTD from Backup: Firepower 4100/9300 Chassis

Device backup and restore is intended for RMA. Restoring configurations overwrites *all* configurations on the device, including the management IP address. It also reboots the device.

In case of hardware failure, this procedure outlines how to replace a Firepower 4100/9300, standalone or in a High Availability pair. It assumes you have access to successful backups of:

- The logical device or devices you are replacing; see Back up a Device from the FMC, on page 11.
- FXOS configurations; see Exporting an FXOS Configuration File, on page 12.

For high availability devices, you can use this procedure to replace all peers. To replace all, perform all steps on all devices simultaneously, except the **restore** CLI command itself.

Note Do *not* unregister from the FMC, even when disconnecting a device from the network. For FTD high availability devices, do *not* suspend or break high availability. Maintaining these links ensures replacement devices can automatically reconnect after restore.

Before you begin

You must read and understand the requirements, guidelines, limitations, and best practices. You do not want to skip any steps or ignore security concerns. Careful planning and preparation can help you avoid missteps.

- Requirements for Backup and Restore, on page 3
- Guidelines and Limitations for Backup and Restore, on page 4
- Best Practices for Backup and Restore, on page 6

Procedure

Step 1 Contact Cisco TAC for replacement hardware.

Obtain an identical model, with the same number of network modules and same type and number of physical interfaces. You can begin the RMA process from the Cisco Returns Portal.

Step 2 Locate a successful backup of the faulty device.

Depending on your backup configuration, device backups may be stored:

- On the faulty device itself in `/var/sf/backup`.
- On the FMC in `/var/sf/remote-backup`.
- In a remote storage location.

For FTD high availability devices, you back up the group as a unit. For high availability devices, the backup process produces unique backup files, with each device's role indicated in the backup file name.

If the only copy of the backup is on the faulty device, copy it somewhere else now. If you reimage the device, the backup will be erased. If something else goes wrong, you may not be able to recover the backup. For more information, see Manage Backups and Remote Storage, on page 28.

The replacement device will need the backup, but can retrieve it with SCP during the restore process. We recommend you put the backup somewhere SCP-accessible to the replacement device. Or, you can copy the backup to the replacement device itself.

Step 3 Locate a successful backup of your FXOS configurations.

Step 4 Remove (unrack) the faulty device.

Disconnect all interfaces. In FTD high availability deployments, this includes the failover link.

See the hardware installation and getting started guides for your model: http://www.cisco.com/go/ftd-quick.

Note
Do *not* unregister from the FMC, even when disconnecting a device from the network. For FTD high availability devices, do *not* suspend or break high availability. Maintaining these links ensures replacement devices can automatically reconnect after restore.

Step 5 Install the replacement device and connect it to the management network.

Connect the device to power and the management interface to the management network. In FTD high availability deployments, connect the failover link. However, do *not* connect the data interfaces.

See the hardware installation guide for your model: http://www.cisco.com/go/ftd-quick.

Step 6 (Optional) Reimage the replacement device.

In an RMA scenario, the replacement device will arrive configured with factory defaults. If the replacement device is not running the same major version as the faulty device, we recommend you reimage.

See the instructions on restoring the factory default configuration in the appropriate Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide.

Step 7 Make sure FXOS is running a compatible version.

You must be running a compatible FXOS version before you re-add logical devices. You can use Firepower Chassis Manager to import your backed-up FXOS configurations: Importing a Configuration File, on page 24.

Step 8 Use Firepower Chassis Manager to add logical devices and perform initial configurations.

Do not set the same management IP addresses as the logical device or devices on the faulty chassis. This can cause problems if you need to register a logical device in order to patch it. The restore process will correctly reset the management IP address.

See the FMC deployment chapter in the getting started guide for your model: http://www.cisco.com/go/ftd-quick.

Note
If you need to patch a logical device, register to the FMC as described in the getting started guide. If you do not need to patch, do *not* register.

Step 9 Make sure the replacement device is running the same software version, *including patches*, as the faulty device.

Ensure that the existing device should not be deleted from the FMC. The replacement device should be unmanaged from the physical network and the new hardware as well as the replacing FTD patch should have the same version. The FTD CLI does not have an upgrade command. To patch:

a) From the FMC web interface, complete the device registration process.

   Create a new AC policy and use the default action "Network Discovery". Leave this policy as is; do not add any features or modifications. This is being used to register the device and deploy a policy with no features so that you do not require licenses, and you will then be able to patch the device. Once backup is restored, it should restore the licensing and policy into the expected state.

b) Patch the device: https://www.cisco.com/go/ftd-upgrade.

c) Unregister the freshly patched device from the FMC.

   If you do not unregister, you will have a ghost device registered to the FMC after the restore process brings your "old" device back up.

Step 10 Make sure the replacement device has access to the backup file.

The restore process can retrieve the backup with SCP, so we recommend you put the backup somewhere accessible. Or, you can manually copy the backup to the replacement device itself, to `/var/sf/backup`.

Step 11 From the FTD CLI, restore the backup.

Access the FTD CLI as the `admin` user. You can use the console or you can SSH to the newly configured management interface (IP address or hostname). Keep in mind that the restore process will change this IP address.

To restore:

- With SCP: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- From the local device: **restore remote-manager-backup** *backup tar-file*

In FTD high availability deployments, make sure you choose the appropriate backup file: primary vs secondary. The role is noted in the backup file name. If you are restoring all devices, do this sequentially. Do not run the **restore** command on the next device until the restore process completes for the first device, including the reboot.

Step 12 Log into the FMC and wait for the replacement device to connect.

When the restore is done, the device logs you out of the CLI, reboots, and automatically connects to the FMC. At this time, the device should appear out of date.

Step 13 Before you deploy, perform any post-restore tasks and resolve any post-restore issues:

- Resolve licensing conflicts or orphan entitlements. For additional assistance and support, contact Cisco TAC.
- Re-add/re-enroll all VPN certificates. The restore process removes VPN certificates from FTD devices, including certificates added after the backup was taken. See *Managing VPN Certificates* in the Firepower Management Center Device Configuration Guide.

Step 14 Deploy configurations.

You must deploy. After you restore a device, you must force deploy from the Device Management page. See *Redeploy Existing Configurations to a Device* in the Firepower Management Center Device Configuration Guide.

Step 15 Connect the device's data interfaces.

See the hardware installation guide for your model: http://www.cisco.com/go/ftd-quick.

What to do next

Verify that the restore succeeded and the replacement device is passing traffic as expected.

Importing a Configuration File

You can use the configuration import feature to apply configuration settings that were previously exported from your Firepower 4100/9300 chassis. This feature allows you to return to a known good configuration or to recover from a system failure.

Note This procedure explains how to use Firepower Chassis Manager to import FXOS configurations before you restore the software. For the CLI procedure, see the appropriate version of the Cisco Firepower 4100/9300 FXOS CLI Configuration Guide.

Before you begin

Review the Guidelines and Restrictions.

Procedure

Step 1 Choose **System** > **Tools** > **Import/Export** on the Firepower Chassis Manager.

Step 2 To import from a local configuration file:

a) Click **Local**.

b) Click **Choose File** to navigate to and select the configuration file that you want to import.

c) Click **Import**.
A confirmation dialog box opens asking you to confirm that you want to proceed and warning you that the chassis might need to restart.
d) Click **Yes** to confirm that you want to import the specified configuration file.
The existing configuration is deleted and the configuration specified in the import file is applied to the Firepower 4100/9300 chassis. If there is a breakout port configuration change during the import, the Firepower 4100/9300 chassis will need to restart.

Step 3 To import from a configuration file on a remote server:

a) Click **Remote**.
b) Choose the protocol to use when communicating with the remote server. This can be one of the following: FTP, TFTP, SCP, or SFTP.
c) If you are using a non-default port, enter the port number in the **Port** field.
d) Enter the hostname or IP address of the location where the backup file is stored. This can be a server, storage array, local drive, or any read/write media that the Firepower 4100/9300 chassis can access through the network.

If you use a hostname rather than an IP address, you must configure a DNS server.

e) Enter the username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
f) Enter the password for the remote server username. This field does not apply if the protocol is TFTP.

Note
The password must not exceed 64 characters. If you enter a password more than 64 character, Firepower Chassis Manager will display an error stating that `property pwd of org-root/cfg-exp-policy-default is out of range.`

g) In the **File Path** field, enter the full path to the configuration file including the file name.
h) Click **Import**.
A confirmation dialog box opens asking you to confirm that you want to proceed and warning you that the chassis might need to restart.
i) Click **Yes** to confirm that you want to import the specified configuration file.
The existing configuration is deleted and the configuration specified in the import file is applied to the Firepower 4100/9300 chassis. If there is a breakout port configuration change during the import, the Firepower 4100/9300 chassis will need to restart.

Restore FTDv from Backup

Use this procedure to replace a faulty or failed FTDv device.

For high availability devices, you can use this procedure to replace all peers. To replace all, perform all steps on all devices simultaneously, except the **restore** CLI command itself.

Note Do *not* unregister from the FMC, even when disconnecting a device from the network. For FTD high availability devices, do *not* suspend or break high availability. Maintaining these links ensures replacement devices can automatically reconnect after restore.

Before you begin

You must read and understand the requirements, guidelines, limitations, and best practices. You do not want to skip any steps or ignore security concerns. Careful planning and preparation can help you avoid missteps.

- Requirements for Backup and Restore, on page 3
- Guidelines and Limitations for Backup and Restore, on page 4
- Best Practices for Backup and Restore, on page 6

Procedure

Step 1 Locate a successful backup of the faulty device.

Depending on your backup configuration, device backups may be stored:

- On the faulty device itself in `/var/sf/backup`.
- On the FMC in `/var/sf/remote-backup`.
- In a remote storage location.

For FTD high availability devices, you back up the group as a unit. For high availability devices, the backup process produces unique backup files, with each device's role indicated in the backup file name.

If the only copy of the backup is on the faulty device, copy it somewhere else now. If you reimage the device, the backup will be erased. If something else goes wrong, you may not be able to recover the backup. For more information, see Manage Backups and Remote Storage, on page 28.

The replacement device will need the backup, but can retrieve it with SCP during the restore process. We recommend you put the backup somewhere SCP-accessible to the replacement device. Or, you can copy the backup to the replacement device itself.

Step 2 Remove the faulty device.

Shut down, power off, and delete the virtual machine. For procedures, see the documentation for your virtual environment.

Step 3 Deploy a replacement device.

See https://www.cisco.com/go/ftdv-quick.

Step 4 Perform initial configuration on the replacement device.

Use the console to access the FTD CLI as the `admin` user. A setup wizard prompts you to configure the management IP address, gateway, and other basic network settings.

Do not set the same management IP address as the faulty device. This can cause problems if you need to register the device in order to patch it. The restore process will correctly reset the management IP address.

See the CLI setup topics in the getting started guide: https://www.cisco.com/go/ftdv-quick.

Note
If you need to patch the replacement device, start the FMC registration process as described in the getting started guide. If you do not need to patch, do *not* register.

Step 5 Make sure the replacement device is running the same software version, *including patches*, as the faulty device.

Ensure that the existing device should not be deleted from the FMC. The replacement device should be unmanaged from the physical network and the new hardware as well as the replacing FTD patch should have the same version. The FTD CLI does not have an upgrade command. To patch:

a) From the FMC web interface, complete the device registration process.

Create a new AC policy and use the default action "Network Discovery". Leave this policy as is; do not add any features or modifications. This is being used to register the device and deploy a policy with no features so that you do not require licenses, and you will then be able to patch the device. Once backup is restored, it should restore the licensing and policy into the expected state.

b) Patch the device: https://www.cisco.com/go/ftd-upgrade.

c) Unregister the freshly patched device from the FMC.

If you do not unregister, you will have a ghost device registered to the FMC after the restore process brings your "old" device back up.

Step 6 Make sure the replacement device has access to the backup file.

The restore process can retrieve the backup with SCP, so we recommend you put the backup somewhere accessible. Or, you can manually copy the backup to the replacement device itself, to `/var/sf/backup`.

Step 7 From the FTD CLI, restore the backup.

Access the FTD CLI as the `admin` user. You can use the console or you can SSH to the newly configured management interface (IP address or hostname). Keep in mind that the restore process will change this IP address.

To restore:

- With SCP: **restore remote-manager-backup location** *scp-hostname username filepath backup tar-file*
- From the local device: **restore remote-manager-backup** *backup tar-file*

In FTD high availability deployments, make sure you choose the appropriate backup file: primary vs secondary. The role is noted in the backup file name. If you are restoring all devices, do this sequentially. Do not run the **restore** command on the next device until the restore process completes for the first device, including the reboot.

Step 8 Log into the FMC and wait for the replacement device to connect.

When the restore is done, the device logs you out of the CLI, reboots, and automatically connects to the FMC. At this time, the device should appear out of date.

Step 9 Before you deploy, perform any post-restore tasks and resolve any post-restore issues:

- Resolve licensing conflicts or orphan entitlements. For additional assistance and support, contact Cisco TAC.
- Re-add/re-enroll all VPN certificates. The restore process removes VPN certificates from FTD devices, including certificates added after the backup was taken. See *Managing VPN Certificates* in the Firepower Management Center Device Configuration Guide.

Step 10 Deploy configurations.

You must deploy. After you restore a device, you must force deploy from the Device Management page. See *Redeploy Existing Configurations to a Device* in the Firepower Management Center Device Configuration Guide.

Step 11 Add and configure data interfaces.

See the getting started guide: https://www.cisco.com/go/ftdv-quick.

What to do next

Verify that the restore succeeded and the replacement device is passing traffic as expected.

Manage Backups and Remote Storage

Backups are stored as unencrypted archive (.tar) files. The file name includes identifying information that can include:

- The name of the backup profile or scheduled task associated with the backup.
- The display name or IP address of the backed-up appliance.
- The appliance's role, such as a member of an HA pair.

We recommend you back up appliances to a secure remote location and verify transfer success. Backups left on an appliance may be deleted, either manually or by the upgrade process; upgrades purge locally stored backups. For more information on your options, see Backup Storage Locations, on page 29.

Caution Especially because backup files are unencrypted, do *not* allow unauthorized access. If backup files are modified, the restore process will fail. Keep in mind that anyone with the Admin/Maint role can access the Backup Management page, where they can move and delete files from remote storage.

The following procedure describes how to manage backup files.

Procedure

Step 1 Select **System** (⚙) > **Tools** > **Backup/Restore**.

The Backup Management page lists available backups. It also lists how much disk space you have available to store backups. Backups can fail if there is not enough space.

Step 2 Do one of the following:

Table 3: Remote Storage and Backup File Management

To	Do This
Enable or disable remote storage for backups without having to edit the FMC system configuration.	Click **Enable Remote Storage for Backups**. This option appears only after you configure remote storage. Toggling it here also toggles it in the system configuration (**System** (⚙) > **Configuration** > **Remote Storage Device**). **Tip** To quickly access your remote storage configuration, click **Remote Storage** at the upper right of the Backup Management page. **Note** To store backup on the remote storage location, you must also enable the **Retrieve to Management Center** option (see Back up a Device from the FMC, on page 11).
Move a file between the FMC and the remote storage location.	Click **Move**. You can move a file back and forth as many times as you want. This will delete—not copy—the file from the current location. When you move a backup file from remote storage to the FMC, where it is stored on the FMC depends on the kind of backup: • FMC backups: `/var/sf/backup` • Device backups: `/var/sf/remote-backup`
View the contents of the backup.	Click the backup file.
Delete a backup file.	Choose a backup file and click **Delete**. You can delete both locally and remotely stored backup files.
Upload a backup file from your com puter.	Click **Upload Backup**, choose a backup file, and click **Upload Backup** again.
Download a backup to your computer.	Choose a backup file and click **Download**. Unlike moving a backup file, this does not delete the backup from the FMC. Store your downloaded backup in a secure location.

Backup Storage Locations

The following table describes backup storage options for FMCs and managed devices.

Table 4: Backup Storage Locations

Location	Details
Remote, by mounting a network volume (NFS, SMB, SSHFS).	**Note** Backup is stored on a remote storage location only when you have configured remote storage and enabled the **Retrieve to Management Center** option (see Back up a Device from the FMC, on page 11). In the FMC's system configuration, you can mount an NFS, SMB, or SSHFS network volume as remote storage for FMC and device backups; see Remote Storage Device.) After you do this, all subsequent FMC backups *and FMC-initiated device backups* are copied to that volume, but you can still use the FMC to manage them (restore, download, upload, delete, move). Note that only the FMC mounts the network volume. Managed device backup files are routed through the FMC. Make sure you have the bandwidth to perform a large data transfer between the FMC and its devices. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
Remote, by copying (SCP).	**Note** Backup is stored on a remote storage location only when you have configured remote storage and enabled the **Retrieve to Management Center** option (see Back up a Device from the FMC, on page 11). For the FMC, you can use a **Copy when complete** option to securely copy (SCP) completed backups to a remote server. Compared with remote storage by mounting a network volume, **Copy when complete** cannot copy to NFS or SMB volumes. You cannot provide CLI options or set a disk space threshold, and it does not affect remote storage of reports. You also cannot manage backup files after they are copied out. This option is useful if you want to store backups locally *and* SCP them to a remote location. **Note** If you configure SSHFS remote storage in the FMC system configuration, do *not* copy backup files to the same directory using **Copy when complete**.
Local, on the FMC.	If you do not configure remote storage by mounting a network volume, you can save backup files on the FMC: • FMC backups are saved to `/var/sf/backup`. • Device backups are saved to `/var/sf/remote-backup` on the FMC if you enable the **Retrieve to Management Center** option when you perform the backup.

Location	Details
Local, on the device internal flash memory.	Device backup files are saved to `/var/sf/backup` on the device if you: • Do not configure remote storage by mounting a network volume. • Do not enable **Retrieve to Management Center**.
Local, on the device SD card.	For the ISA 3000, when you back up the device to the local `/var/sf/backup` internal flash memory location, if you have an SD card installed, the backup is automatically copied to the SD card at `/mnt/disk3/backup/` for use with zero-touch restore.

History for Backup and Restore

Table 5: History for Backup and Restore

Feature	Minimum FMC	Minimum FTD	Details
Zero-touch restore for the ISA 3000 using the SD card.	7.0.0	7.0.0	When you perform a local backup, the backup file is copied to the SD card if present. To restore the configuration on a replacement device, simply install the SD card in the new device, and depress the Reset button for 3 to 15 seconds during the device bootup.
Back up and restore FTD container instances.	6.7.0	6.7.0	You can now use the FMC to perform on-demand remote backups of FTD container instances on the Firepower 4100/9300.
No longer need to match VDBs to restore.	6.6.0	Any	Restoring the FMC from backup now replaces the existing VDB with the VDB in the backup file. You no longer need to match VDB versions before you restore.
Automatically scheduled backups.	6.5.0	Any	For new or reimaged FMCs, the setup process creates a weekly scheduled task to back up FMC configurations and store them locally.
On-demand remote backups of managed devices.	6.3.0	6.3.0	You can now use the FMC to perform on-demand remote backups of certain managed devices. For supported platforms, see Requirements for Backup and Restore, on page 3. New/modified screens: **System** > **Tools** > **Backup/Restore** > **Managed Device Backup** New/modified FTD CLI commands: **restore**