Backup and 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.

On-Demand Backups

You can perform on-demand backups for the FMC and 7000/8000 series devices from the FMC.

You can also use the local web interface on a 7000/8000 series device to perform on-demand backups. Local backup management on 7000/8000 series devices is slightly different and has fewer options than backup management on the FMC, but in general works in the same way. Note that you can use the FMC to back up these devices remotely.

For more information, see Backing Up FMCs or Managed Devices, on page 7.

Scheduled Backups

You can use the scheduler on an FMC or 7000/8000 series device to automate backups. You cannot schedule remote device backups from the FMC.

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 Management and Manage Backups and Remote Storage, on page 14.

Restoring the FMC and Managed Devices

You restore the FMC and 7000/8000 series devices from the local Backup Management page.

For more information, see Restoring FMCs and Managed Devices, on page 12.

What Is Backed Up?

FMC backups can include:

- Configurations.

  All configurations you can set on the FMC web interface are included in a configuration backup, with the exception of remote storage and audit log server certificate settings. In a multidomain deployment, you must back up configurations. You cannot back up events or TID data only.

- Events.

  Event backups include all events in the FMC database. However, FMC event backups do not include intrusion event review status. Restored intrusion events do not appear on Reviewed Events pages.

- Threat Intelligence Director (TID) data.

  For more information, see About Backing Up and Restoring TID Data.

7000/8000 series device backups are always configuration-only.

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.

  FMC configuration backups do not include remote storage and audit log server certificate settings, so you must reconfigure these after restore. Also, because FMC event backups do not include intrusion event review status, restored intrusion events do not appear on Reviewed Events pages.

- 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.

Requirements for Backup and Restore

Backup and restore has the following requirements.

Model Requirements: Backup

You can back up:

- FMCs
- 7000/8000 series devices

Backup is *not* supported for:

- Firepower Threat Defense
- NGIPSv
- ASA FirePOWER

If you need to replace a device where backup and restore is not supported, you must manually recreate device-specific configurations. However, backing up the FMC does back up policies and other configurations that you deploy to managed devices, as well as events already transmitted from the devices to the FMC.

Model Requirements: Restore

A replacement appliance must be the same model as the one you are replacing. Replacement managed devices should have the same number of network modules and same type and number of physical interfaces.

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 Firepower version, including patches.

For FMC backups, you must also have the same VDB. You are *not* required to have the same SRU.

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.

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.

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.

Restore is Individual and Local

You restore to cloud-delivered Firewall Management Centers and threat defensemanaged devices individually and locally. This means:

- You cannot batch-restore to high availability (HA) FMCs or devices. The restore procedures in this guide explain how to restore in an HA environment.
- You cannot use the cloud-delivered Firewall Management Center to restore a device. For the cloud-delivered Firewall Management Center and 7000/8000 series devices, you can use the local web interface to restore.
- You cannot use an cloud-delivered Firewall Management Center user account to log into and restore one of its managed devices. cloud-delivered Firewall Management Centers and devices maintain their own user accounts.

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 (cloud-delivered Firewall Management Center 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 backups.

  As part of your disaster recovery plan, we recommend that you perform periodic backups. To automate this process, see Scheduled Backups.

- 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.

- After upgrade.

  Back up after you upgrade, so you have a snapshot of your freshly upgraded deployment. We recommend you back up the cloud-delivered Firewall Management Center *after* you upgrade its managed devices, so your new cloud-delivered Firewall Management Center 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.

Caution We recommend you back up cloud-delivered Firewall Management Centers 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 cloud-delivered Firewall Management Center'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 cloud-delivered Firewall Management Center to manage them. For more information, see Remote Storage Management and Manage Backups and Remote Storage, on page 14.

Note that only the cloud-delivered Firewall Management Center mounts the network volume. Managed device backup files are routed through the cloud-delivered Firewall Management Center. Make sure you have the bandwidth to perform a large data transfer between the cloud-delivered Firewall Management Center 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 an cloud-delivered Firewall Management Center high availability deployment, backing up one cloud-delivered Firewall Management Center 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 cloud-delivered Firewall Management Center without a successful backup. For more information on replacing HAcloud-delivered Firewall Management Centers, both with and without successful backups, see Replacing FMCs in a High Availability Pair.

Before Backup

Before you back up, you should:

- Update the VDB and SRU on the cloud-delivered Firewall Management Center.

  We always recommend you use the latest vulnerability database (VDB) and intrusion rules (SRU). Before you back up an cloud-delivered Firewall Management Center, check the Cisco Support & Download site for newer versions.

  This is especially important for the VDB, because the VDB versions must match to restore a backup. Because you cannot downgrade the VDB, you do not want a situation where your replacement cloud-delivered Firewall Management Center has a newer VDB than the backed up cloud-delivered Firewall Management Center.

- 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.

  Note that restoring an cloud-delivered Firewall Management Center or 7000/8000 series device 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 an FMC or managed device, do not unregister devices from the cloud-delivered Firewall Management Center, 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 cloud-delivered Firewall Management Center 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 cloud-delivered Firewall Management Center 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.

- Update the VDB and SRU on the cloud-delivered Firewall Management Center.

  We always recommend you use the latest vulnerability database (VDB) and intrusion rules (SRU).

- Deploy.

  After you restore an cloud-delivered Firewall Management Center, deploy to all managed devices. After you restore a device, deploy to that device. You *must* deploy. If the a device or devices are not marked out of date, force deploy from the Device Management page: Redeploy Existing Configurations to a Device.

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 7000/8000 series devices from the FMC. However, FMC backups require backup profiles, as do local backups on 7000/8000 series devices.. The on-demand backup process allows you to create a new backup profile.

For more information, see:

- Back up the FMC, on page 7
- Back up a Device from the FMC, on page 9
- Back up a 7000/8000 Series Device Locally, on page 10
- Create a Backup Profile, on page 11
- Scheduled Backups

Back up the FMC

Use this procedure to perform an on-demand FMC backup. To back up a 7000/8000 series device from its local web interface, see Back up a 7000/8000 Series Device Locally, on page 10.

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 4

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 **Firepower Management Backup** 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 14.

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.

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 backup of a 7000/8000 series device from the FMC. At this time, backup and restore is not supported for Firepower Threat Defense.

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 4

Procedure

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

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

Step 3 Note the **Storage Location** for device backup files.

This will either be local storage in `/var/sf/remote-backup/`, or a remote network volume. For more information, see Manage Backups and Remote Storage, on page 14.

Step 4 If you did not configure remote storage, choose whether you want to **Retrieve to Management Center**.

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

Step 5 Click **Start Backup** to start the on-demand backup.

Step 6 Monitor progress in the Message Center.

What to do next

If you configured remote storage, verify transfer success of the backup file.

Back up a 7000/8000 Series Device Locally

Use this procedure to perform a local, on-demand backup for a 7000/8000 series device. Device backups are always configuration-only.

Note that local backup management on 7000/8000 series devices is slightly different and has fewer options than backup management on the FMC, but in general works in the same way. Unless you have a specific need (such as scheduling backups), we recommend you use the FMC to back up these devices remotely.

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 4

Procedure

Step 1 On the device's local web interface, select **System** > **Tools** > **Backup/Restore**.

The Backup Management page lists all locally 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.

7000/8000 series local backups require that you use or create a backup profile. When you perform an on-demand 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.

- 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 **Device Backup** to start fresh and create a new backup profile.

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

Step 3 (Optional) Enable **Copy when complete** to copy completed backups to a remote server.

This is your only option for remote storage for 7000/8000 series local backups.

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.

Step 4 (Optional) Enable **Email** and enter an email address to be notified when the backup completes.

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

Step 5 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.

Step 6 Monitor progress in the Message Center.

While the system collects backup data, you may be prevented from changing configurations related to the backup. If you enabled **Copy when complete**, the device 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 enabled **Copy when complete**, verify transfer success of the backup file.

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 and 7000/8000 series local backups require backup profiles. Backup profiles are not required to back up a device from the FMC.

When you perform an on-demand FMC or 7000/8000 series local 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. Note that you cannot schedule 7000/8000 series device backups from the FMC.

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 (FMC only) Choose what to back up.

7000/8000 series backups are always configuration-only.

- **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.

For FMC backup profiles, this will either be local storage in `/var/sf/backup/`, or a remote network volume. For 7000/8000 local backup profiles, this is always `/var/sf/backup/`. For more information, see Manage Backups and Remote Storage, on page 14.

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 and 7000/8000 series devices, you use the local web interface to restore from backup. You cannot use the FMC to restore a device.

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

- Restore an FMC from Backup, on page 12
- Replacing FMCs in a High Availability Pair
- Restore a 7000/8000 Series Device from Backup, on page 13

Restore an FMC from Backup

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

Note Restoring configurations overwrites *all* configurations, with very few exceptions. 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 an FMC from backup. For more information on backup and restore in an FMC HA deployment, see Replacing FMCs in a High Availability Pair. To restore a 7000/8000 series device, see Restore a 7000/8000 Series Device from Backup, on page 13.

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 4

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 14.

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.
- (Optional) Update the SRU and VDB. If the SRU or the VDB available on the Cisco Support & Download site is newer than the version currently running, we recommend you install the newer version.
- Deploy configuration changes; see Deploy Configuration Changes.

Restore a 7000/8000 Series Device from Backup

This procedure explains how to use the 7000/8000 series local web interface to restore from backup. Restoring overwrites *all* configurations, with very few exceptions. It also reboots the device.

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 4

Procedure

Step 1 Log into the device you want to restore.

Step 2 Select **System** > **Tools** > **Backup/Restore**.

The Backup Management page lists all locally 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 14.

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

Step 4 Make sure **Replace Configuration Data** is enabled, then click **Restore** again to begin.

Device backups are always configuration-only.

Step 5 Monitor progress in the Message Center until the device reboots.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

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 15.

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 1: 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 9).
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 computer.	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.

Backup Storage Locations

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

Table 2: 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 9). 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 Management.) 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 9). For the FMC and for 7000/8000 series *local* backups, 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. It is also your only option for remote storage for 7000/8000 series local backups. **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. Note that you cannot save 7000/8000 series local backups to the FMC.

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**.