

# Backup/Restore


- Backup and restore, on page 1
- Requirements: backup and restore configuration, on page 3
- Guidelines and limitations for backup and restore, on page 4
- Best practices for backup and restore, on page 6
- Backing up Firewall Management Centers or managed devices, on page 8
- Restoring Firewall Management Centers and managed devices, on page 14
- Manage backups and remote storage, on page 30
- Manage backup and restoration for multi-instance devices, on page 33
- History for backup and restore, on page 36


# Backup and restore

A backup and restore system is a disaster recovery mechanism that

- enables periodic backups to a secure remote location as part of system maintenance planning,
- provides the ability to recover from disasters, and
- supports both on-demand and scheduled backup operations.

### Backup types and contents

Device backups are always configuration-only. Firewall Management Center backups vary by type.

***Table 1: Firewall Management Center backups***

| Backup Type | Backed Up | Not Backed Up |
|---|---|---|
| Configurations | Most configurations are backed up.<br><br>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:<br>• Remote storage settings.<br>• Audit log server certificate settings.<br>• Public and private AMP cloud connections. |

| Backup Type | Backed Up | Not Backed Up |
|---|---|---|
| Events | All events in the Firewall Management Center database. | Intrusion event review status is not backed up. Restored intrusion events do not appear on Reviewed Events pages. |
| Threat Intelligence Director (TID) data. | For more information, see *About Backing Up and Restoring Threat Intelligence Director Data* in the *Cisco Secure Firewall Management Center Device Configuration Guide*. | |
| Reports | — | Reports stored on the Firewall Management Center are not backed up as part of any backup. You should store reports in a secure remote location. |

Restoring configurations overwrites *all* backed-up configurations, with very few exceptions. On the Firewall Management Center, 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 these restore considerations:

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

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

  The Firewall Management Center 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 Firewall Management Center configuration restore process does not overwrite clean and custom detection file lists used by Malware Defense. Instead, it merges existing file lists with the file lists in the backup. To replace file lists, delete existing file lists before you restore.

You can perform on-demand backups for the Firewall Management Center and many Firewall Threat Defense devices from the Firewall Management Center.

For more information, see Backing up Firewall Management Centers or managed devices, on page 8.

You can use the scheduler on Firewall Management Center to automate backups. You can also schedule remote device backups from the Firewall Management Center.

The Firewall Management Center 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 Scheduling.

You can store backups locally. However, we recommend you back up Firewall Management Centers 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 Firewall Management Center to manage them.

For more information, see Remote storage devices and Manage backups and remote storage, on page 30.

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

For more information, see Restoring Firewall Management Centers and managed devices, on page 14.

# Requirements: backup and restore configuration

## Platform requirements

Ensure that you use supported platforms for backup and restore operations.

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

***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** | **YES** |
| Threat defense virtual, on-prem/private cloud | VMware<br>HyperFlex<br>Nutanix<br>OpenStack | VMware | VMware |
| Threat defense virtual, public cloud | — | — | — |

## Restore platform requirements

Ensure that a replacement managed device meets these hardware requirements.

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

### Version requirements

Ensure that both old and new appliances run compatible software versions before restoring backups.

- 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 Firewall Management Center 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 this happens, it is reported in the Message Center. 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

Ensure that you have appropriate domain permissions for backup and restore operations.

- To back up or restore the Firewall Management Center: Global only.
- To back up a device from the Firewall Management Center: Global only.
- To 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 is for disaster recovery/RMA

Use backup and restore primarily 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 Firewall Management Centers. This makes it easier to replace Firewall Management Centers 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 Firewall Management Center on a freshly reimaged Firewall Management Center.

If you are restoring without reimaging and if you had registered Firewall Threat Defense on the Firewall Management Center after backing up, then when you register the device again on the restored Firewall Management Center, 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 Firewall Management Center backup that is restored to.

### Backup and restore is not configuration import/export

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.

A backup file contains information that uniquely identifies an appliance, and cannot be shared. For example, Firewall Threat Defense device backups include the device's management IP address and all information the device needs to connect to its managing Firewall Management Center. Do not restore the Firewall Threat Defense backup to a device being managed by a different Firewall Management Center; the restored device will attempt to connect to the Firewall Management Center specified in the backup.

### Restore is individual and local

Restore to Firewall Management Centers and managed devices individually and locally.

- You cannot batch-restore to high availability or clustered Firewall Management Centers or devices.
- You cannot use the Firewall Management Center to restore a device. For the Firewall Management Center, you can use the web interface to restore. For Firewall Threat Defense devices, you must use the Firewall Threat Defense CLI, except for the ISA 3000 zero-touch restore, which uses an SD card and the reset button.
- While restoring the Firewall Management Center 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 Firewall Management Center user accounts to log into and restore one of its managed devices. The Firewall Management Center 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 Threat Defense unit that is being restored.

Otherwise, the HA peers may enter a split-brain state.

## Recommendation: 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/ Secure Firewall 6100 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/ Secure Firewall 6100 chassis to return to a known good configuration or to recover from a system failure.

- 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

## When to back up

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

- Regular scheduled or on-demand backups. As part of your disaster recovery plan, we recommend that you perform periodic backups.
- After SLR changes. Back up the Firewall Management Center after you make changes to Specific Licensing Reservations (SLRs).
- Before upgrade or reimage. If an upgrade fails catastrophically, you may have to reimage and restore.
- During backup and restore process, some of major Management Center and Threat Defense processes which impact the connectivity to each other are not available. Therefore, ensure that parallel actions are not initiated when major processes are paused, stopped, or restarted during a backup and restore.
- After upgrade. Back up after you upgrade, so you have a snapshot of your freshly upgraded deployment.

## Maintaining backup file security

We recommend you back up Firewall Management Centers and devices to a secure remote location and verify transfer success.

- Backups are stored as unencrypted archive (.tar) files.
- Private keys in PKI objects are decrypted before they are backed up and reencrypted with a randomly generated key when you restore the backup.

## Backup and restoration in Firewall Management Center high-availability deployments

In Firewall Management Center high availability deployments, backing up one Firewall Management Center does not back up the other. You should regularly back up both peers.

## Backup and restoration in Firewall Threat Defense high-availability deployments

In the Firewall Threat Defense high availability deployment, you should back up the device pair from the Firewall Management Center, but restore individually and locally from the Firewall Threat Defense CLI.

- Do *not* suspend or break high availability before you restore.
- Do *not* run the **restore** CLI command on both peers at the same time.
- When both peers fail, before the devices are decommissioned, ensure that unregister them both from the Firewall Management Center.

## Backup and restoration in Firewall Threat Defense cluster deployments

In the Firewall Threat Defense clustering deployment, you should back up the entire cluster from the Firewall Management Center, but restore nodes individually and locally from the Firewall Threat Defense CLI.

- Do *not* suspend or break clustering before you restore.
- Do *not* run the **restore** CLI command on multiple nodes at the same time.

## Backup and restoration for firepower 4100/9300 chassis

To restore Firewall Threat Defense 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.

## Prebackup tasks

Before you back up, you should update the VDB and SRU on the Firewall Management Center and check disk space.

- We always recommend you use the latest vulnerability database (VDB) and intrusion rules (SRU).
- Before you begin a backup, make sure you have enough disk space on the appliance or on your remote storage server.

## Prerestoration tasks

Before restore, you should revert any licensing changes made since you took the backup, disconnect faulty appliances, avoid unregistering managed devices, and reimage when necessary.

- Revert any licensing changes made since you took the backup to avoid license conflicts.
- Disconnect the management interface, and for devices, the data interfaces to avoid IP conflicts.
- Do *not* unregister managed devices from the Firewall Management Center, even if you physically disconnect an appliance from the network.
- In an RMA scenario, we recommend you reimage if the replacement appliance is already configured.

## Postrestoration tasks

After restoration, perform these tasks: reconfigure everything that was not restored, update the vulnerability database and intrusion rules, and deploy restored Management Center and its Threat Defense devices.

- Reconfigure licensing, remote storage, and audit log server certificate settings.
- Update the vulnerability database (VDB) and intrusion rules (SRU) on the Firewall Management Center.
- If you are restoring a Threat Defense device, you must perform force deployment after restoration is complete.

  If you are restoring Firewall Management Center:

  - If you have performed restoration with the latest Firewall Management Center backup and no configuration changes are deployed to the managed Threat Defense devices after the backup, you are not required to perform deployment after restoration.
  - For all other conditions, you must perform force deployment.



**Note** For information about how to force deploy, see refer the "Redeploy Existing Configurations to a Device" section in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

# Backing up Firewall Management Centers or managed devices

A backup is a data protection mechanism that

- allows you to perform on-demand or scheduled backups for supported appliances,
- can be performed without requiring a backup profile for devices from the Firewall Management Center, and
- requires backup profiles for Firewall Management Center backups.

### Backup profile creation

The on-demand backup process allows you to create a new backup profile.

# Back up the Firewall Management Center

Use this procedure to create an immediate backup of your Firewall Management Center to ensure system configurations, events, and threat intelligence data are preserved.

Use this procedure to perform an on-demand Firewall Management Center 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: backup and restore configuration, 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 **Administration** > **Advanced** > **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.

Firewall Management Center 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**. In high availability of Firewall Management Centers, if you choose to back up configuration only on an active Firewall Management Center, by default, both the active and standby Firewall Management Centers are backed up into a single unified backup file. For information of unified backup of Firewall Management Center in high availability, see Unified backups of management centers in high availability.
- **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 Backup and restore, on page 1.

**Step 4** Note the **Storage Location** for Firewall Management Center 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 30.

**Step 5** (Optional. Not available when Firewall Management Center is in HA) Enable **Copy when complete** to copy completed Firewall Management Center 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. This option can be used to copy the same backup file to a secondary remote storage.

**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 Firewall Management Center to connect to a mail server: Configure 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.

The Message Center now displays detailed backup status for the management center and its devices. You can also cancel in-progress device backups.

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 Firewall Management Center may write temporary files to the remote server. These files are cleaned up at the end of the backup process.

The backup process creates a backup file containing your selected system data and stores it in the configured location. You can monitor the backup completion through the Message Center notifications.

### 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 Firewall Management Center

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

Device backups protect your configuration and allow you to restore device settings if needed. You can save backups to local storage or to a remote network location.

### 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: backup and restore configuration, 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: Export an FXOS configuration file, on page 12.

Follow these steps to back up a device from the management center:

## Procedure

**Step 1** Select **Administration** > **Advanced** > **Backup & Restore**, then click **Managed Device Backup**.

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

For clustering, choose the cluster. You cannot perform backups on individual nodes.

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

- Local storage in Firewall Management Center at `/var/sf/remote-backup/`.
- Local storage in Firewall Threat Defense 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 30.

**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 :

- **Remote Server** (default): Saves the backup to the configured location in the remote server.

  For clusters, this option is always selected. You cannot opt to save in the device. The individual node backup files are copied to the Firewall Management Center and then bundled into a single compressed tar file before it is copied to any remote storage.

- **Threat Defense**: 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 Firewall Management Center. Choose whether you want to save the backup to Firewall Management Center or to the device :

- **Management Center** (default): Saves the backup to the Firewall Management Center in `/var/sf/remote-backup/`.

  For clusters, this option is always selected. You cannot opt to save in the device.

- **Threat Defense**: 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.

You can click **Cancel** to cancel an in-progress backup.

The device backup completes and the backup file is saved to your selected location. You can monitor the backup progress in the Message Center.

### What to do next

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

## Export an FXOS configuration file

Export configuration files to create backups of logical device and platform settings for disaster recovery or system migration purposes.

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 Secure Firewall Chassis Manager to export FXOS configurations when you back up Firewall 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 Secure Firewall 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 and password the system should use to log in to the remote server. 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, Firewall Chassis Manager will display an error stating that **property pwd of org-root/cfg-exp-policy-default is out of range**.

**f.** In the **Location** field, enter the full path to where you want the configuration file exported including the filename.

The configuration file is created and exported to the specified location.

The configuration file is exported to the specified location with the logical device and platform configuration settings for backup or migration purposes.

# Create a backup profile

Create a backup profile to save backup preferences including what to back up, where to store the backup file, and notification settings. This allows for consistent backup configurations and enables scheduled backups.

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

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

When you perform an on-demand Firewall Management Center 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.

**Before you begin**

Follow these steps to create a backup profile without performing an on-demand backup:

**Procedure**

**Step 1** Select **Administration** > **Advanced** > **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 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 30.

**Step 5** (Optional) Enable **Copy when complete** to copy completed Firewall Management Center 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 Firewall Management Center to connect to a mail server: Configure a mail relay host and notification address.

**Step 7** Click **Save**.

The backup profile is created and available for use in on-demand backups and scheduled backup configurations.

# Restoring Firewall Management Centers and managed devices

Restoring Firewall Management Centers and managed devices is a recovery process that

- uses different interfaces depending on the device type
- requires the web interface for Firewall Management Center, and
- requires the CLI for Firewall Threat Defense devices.

### Restoration methods

The restoration process varies by device type. You cannot use the Firewall Management Center to restore a device.

## Restore Firewall Management Center from Backup

This task restores Firewall Management Center from backup files to recover system configurations, events, and TID data when needed.

When you restore Firewall Management Center 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 Firewall Management Center. 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 Firewall Management Center from backup. For more information on backup and restore in Firewall Management Center HA deployments, see Replace Firewall Management Centers 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: backup and restore configuration, 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 Firewall Management Center you want to restore.

**Step 2** Select **Administration** > **Advanced** > **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 30.

**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 Firewall Management Center reboots.

The Firewall Management Center is restored from the selected backup file with the chosen components.

### 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. When the restored VDB is different from the system VDB, the Message Center indicates the version of the restored 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 configurations:
  - If you have performed restoration with the latest Firewall Management Center backup and no configuration changes are deployed to the managed Threat Defense devices after the backup, you are not required to perform deployment after restoration.

- For all other conditions, you must perform force deployment.

**Note** For information about how to force deploy, see refer the "Redeploy Existing Configurations to a Device" section in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

# Restore Firewall Threat Defense from Backup

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. It assumes you have access to a successful backup of the device or devices you are replacing; see Back up a Device from the Firewall Management Center, on page 10.

This procedure applies to all platforms except for the Firepower 4100/9300 and Firewall Threat Defense Virtual. For zero-touch restore on the ISA 3000 using an SD card, see Zero-Touch Restore Firewall Threat Defense from Backup: ISA 3000, on page 19.

For high availability and clustered 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 Firewall Management Center, even when disconnecting a device from the network. For Firewall Threat Defense high availability and clustered devices, do *not* suspend or break high availability or clustering . 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: backup and restore configuration, 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 Firewall Management Center in `/var/sf/remote-backup`.
- In a remote storage location.

For Firewall Threat Defense high availability and clustered 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. For clusters, control and data node backup files are bundled together in a single compressed file. You must extract the files, which also indicate the device role.

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 30.

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 Firewall Threat Defense high availability deployments, this includes the failover link. For clustering, this includes the cluster control 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 Firewall Management Center, even when disconnecting a device from the network. For Firewall Threat Defense high availability and clustered devices, do *not* suspend or break high availability or clustering . 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 Firewall Threat Defense high availability deployments, connect the failover link. For clustering, connect the cluster control 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 Firewall Threat Defense 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 Firewall Management Center 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 Firewall Management Center. The replacement device should be unmanaged from the physical network and the new hardware as well as the replacing Firewall Threat Defense patch should have the same version. The Firewall Threat Defense CLI does not have an upgrade command. To patch:

a) From the Firewall Management Center 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 Firewall Management Center.

If you do not unregister, you will have a ghost device registered to the Firewall Management Center 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`. For clustered devices, extract the appropriate backup file from the backup bundle.

**Step 9** From the Firewall Threat Defense CLI, restore the backup.

Access the Firewall Threat Defense 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 Firewall Threat Defense high availability and clustering deployments, make sure you choose the appropriate backup file: primary vs secondary, or control vs. data. 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 Firewall Management Center 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 Firewall Management Center. 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.

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

**Note** When you restore a Firewall Threat Defense backup to one of the Firewall Threat Defense high availability (HA) nodes, any mismatch of encryption configuration between two nodes put the Firewall Threat Defense HA into active-active mode, which prevents the IPsec tunnel from being established.

Both the primary and secondary nodes must use the same encryption method to establish an IPsec tunnel. Disable HA on the restored Firewall Threat Defense. Then, use Firewall Management Center to deploy the Firewall Threat Defense HA pair, ensuring that both nodes use the same encryption method as the restored Firewall Threat Defense and then enable the HA in restored Firewall Threat Defense.

**Step 13** Connect the device's data interfaces.

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

The device has been successfully restored from backup and is operational with the restored configuration.

### What to do next

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

# Zero-Touch Restore Firewall Threat Defense from Backup: ISA 3000

This procedure allows you to replace a failed ISA 3000 device, either standalone or in an HA pair, using a backup stored on an SD card.

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 Firewall Management Center, on page 10.

For high availability and clustered  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 Firewall Management Center, even when disconnecting a device from the network. For Firewall Threat Defense high availability and clustered  devices, do *not* suspend or break high availability or clustering . 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: backup and restore configuration, 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 Firewall Threat Defense HA deployments, this includes the failover link.

**Note** Do *not* unregister from the Firewall Management Center, even when disconnecting a device from the network. For Firewall Threat Defense high availability and clustered devices, do *not* suspend or break high availability or clustering . 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 Firewall Threat Defense 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 Secure Firewall software version, *including the same patch version*, as the faulty device. If you need to patch the device, you can connect to Secure Firewall Device Manager (Firewall Device Manager) to install the patch.

This procedure assumes you have a factory default configuration. If you already configured the device, you can log into Firewall Device Manager 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 Firewall Device Manager 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 Firewall Device Manager; 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 and then do the following:

a) 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 Firewall Device Manager to install a patch, you can reboot from the **Device** > **System Settings** > **Reboot/Shutdown** page. From the Firewall Threat Defense 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 Firewall Management Center 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.

b) Log into the Firewall Management Center and wait for the replacement device to connect.

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

**Step 7** Before you deploy, perform any post-restore tasks and resolve any post-restore issues:

- Resolve licensing conflicts or orphan entitlements. Contact Cisco TAC.
- Re-add/re-enroll all VPN certificates. The restore process removes VPN certificates from Firewall Threat Defense devices, including certificates added after the backup was taken. See *Managing VPN Certificates* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

**Step 8** 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 *Cisco Secure Firewall Management Center Device Configuration Guide*.

**Note** When you restore a Firewall Threat Defense backup to one of the Firewall Threat Defense high availability (HA) nodes, any mismatch of encryption configuration between two nodes put the Firewall Threat Defense HA into active-active mode, which prevents the IPsec tunnel from being established.

Both the primary and secondary nodes must use the same encryption method to establish an IPsec tunnel. Disable HA on the restored Firewall Threat Defense. Then, use Firewall Management Center to deploy the Firewall Threat Defense HA pair, ensuring that both nodes use the same encryption method as the restored Firewall Threat Defense and then enable the HA in restored Firewall Threat Defense.

**Step 9** Connect the device's data interfaces.

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

The replacement device is restored with the backed-up configuration and reconnects to the management center. The device is ready for deployment with the current configuration.

### What to do next

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

# Restore Firewall Threat Defense 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 or as a cluster. It assumes you have access to successful backups of:

- The logical device or devices you are replacing; see Back up a Device from the Firewall Management Center, on page 10.
- FXOS configurations; see Export an FXOS configuration file, on page 12.

For high availability and clustered 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 Firewall Management Center, even when disconnecting a device from the network. For Firewall Threat Defense high availability and clustered devices, do *not* suspend or break high availability or clustering . 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: backup and restore configuration, 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 Firewall Management Center in `/var/sf/remote-backup`.
- In a remote storage location.

For Firewall Threat Defense high availability and clustered 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. For clusters, control and data node backup files are bundled together in a single compressed file. You must extract the files, which also indicate the device role.

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 30.

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 Firewall Threat Defense high availability deployments, this includes the failover link. For clustering, this includes the cluster control 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 Firewall Management Center, even when disconnecting a device from the network. For Firewall Threat Defense high availability and clustered devices, do *not* suspend or break high availability or clustering . 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 Firewall Threat Defense high availability deployments, connect the failover link. For clustering, connect the cluster control 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 Firewall Chassis Manager to import your backed-up FXOS configurations: Importing a Configuration File, on page 26.

**Step 8** Use Firewall 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 Firewall Management Center 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 Firewall Management Center 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 Firewall Management Center. The replacement device should be unmanaged from the physical network and the new hardware as well as the replacing Firewall Threat Defense patch should have the same version. The Firewall Threat Defense CLI does not have an upgrade command. To patch:

a) From the Firewall Management Center 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 Firewall Management Center.

   If you do not unregister, you will have a ghost device registered to the Firewall Management Center 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`. For clustered devices, extract the appropriate backup file from the backup bundle.

**Step 11** From the Firewall Threat Defense CLI, restore the backup.

Access the Firewall Threat Defense 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 Firewall Threat Defense high availability and clustering deployments, make sure you choose the appropriate backup file: primary vs secondary, or control vs. data. 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 Firewall Management Center 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 Firewall Management Center. 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 Firewall Threat Defense devices, including certificates added after the backup was taken. See *Managing VPN Certificates* in the *Cisco Secure Firewall 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 *Cisco Secure Firewall Management Center Device Configuration Guide*.

**Note** When you restore a Firewall Threat Defense backup to one of the Firewall Threat Defense high availability (HA) nodes, any mismatch of encryption configuration between two nodes put the Firewall Threat Defense HA into active-active mode, which prevents the IPsec tunnel from being established.

Both the primary and secondary nodes must use the same encryption method to establish an IPsec tunnel. Disable HA on the restored Firewall Threat Defense. Then, use Firewall Management Center to deploy the Firewall Threat Defense HA pair, ensuring that both nodes use the same encryption method as the restored Firewall Threat Defense and then enable the HA in restored Firewall Threat Defense.

**Step 15** Connect the device's data interfaces.

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

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 Firewall 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 Firewall 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. 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.

d) Enter the username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
e) 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, Firewall Chassis Manager will display an error stating that `property pwd of org-root/cfg-exp-policy-default is out of range .`

f) In the **File Path** field, enter the full path to the configuration file including the file name.
g) 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 Firewall Threat Defense Virtual from Backup

This task restores a faulty or failed Firewall Threat Defense Virtual device from a backup, ensuring business continuity and minimal downtime.

Use this procedure to replace a faulty or failed Firewall Threat Defense Virtual device.

For high availability and clustered 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 Firewall Management Center, even when disconnecting a device from the network. For Firewall Threat Defense high availability and clustered devices, do *not* suspend or break high availability or clustering . 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: backup and restore configuration, 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 Firewall Management Center in `/var/sf/remote-backup`.
- In a remote storage location.

For Firewall Threat Defense high availability and clustered 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. For clusters, control and data node backup files are bundled together in a single compressed file. You must extract the files, which also indicate the device role.

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 30.

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 Firewall Threat Defense 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 Firewall Management Center 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 Firewall Management Center. The replacement device should be unmanaged from the physical network and the new hardware as well as the replacing Firewall Threat Defense patch should have the same version. The Firewall Threat Defense CLI does not have an upgrade command. To patch:

a) From the Firewall Management Center 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 Firewall Management Center.

   If you do not unregister, you will have a ghost device registered to the Firewall Management Center 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`. For clustered devices, extract the appropriate backup file from the backup bundle.

**Step 7** From the Firewall Threat Defense CLI, restore the backup.

Access the Firewall Threat Defense 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 Firewall Threat Defense high availability and clustering deployments, make sure you choose the appropriate backup file: primary vs secondary, or control vs. data. 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 Firewall Management Center 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 Firewall Management Center. 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 Firewall Threat Defense devices, including certificates added after the backup was taken. See *Managing VPN Certificates* in the *Cisco Secure Firewall 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 *Cisco Secure Firewall Management Center Device Configuration Guide*.

**Note** When you restore a Firewall Threat Defense backup to one of the Firewall Threat Defense high availability (HA) nodes, any mismatch of encryption configuration between two nodes put the Firewall Threat Defense HA into active-active mode, which prevents the IPsec tunnel from being established.

Both the primary and secondary nodes must use the same encryption method to establish an IPsec tunnel. Disable HA on the restored Firewall Threat Defense. Then, use Firewall Management Center to deploy the Firewall Threat Defense HA pair, ensuring that both nodes use the same encryption method as the restored Firewall Threat Defense and then enable the HA in restored Firewall Threat Defense.

**Step 11** Add and configure data interfaces.

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

The Firewall Threat Defense Virtual device is successfully restored from backup and returns to operational status with all previous configurations and policies intact.

### What to do next

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

# Manage backups and remote storage

This task allows you to manage backup files stored on appliances, including transferring files to and from remote storage locations, enabling or disabling remote storage, and performing file operations such as upload, download, and deletion.

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 31.

**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.

### Procedure

**Step 1** Select **Administration** > **Advanced** > **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 Firewall Management Center system configuration. | Click **Enable Remote Storage for Backups**.<br>This option appears only after you configure remote storage. Toggling it here also toggles it in the system configuration (**Administration** > **Configuration** > **Remote Storage Device**).<br>**Tip**<br>To quickly access your remote storage configuration, click **Remote Storage** at the upper right of the Backup Management page. |
| Move a file between the Firewall Management Center and the remote storage location. | Click **Move**.<br>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.<br>When you move a backup file from remote storage to the Firewall Management Center, where it is stored on the Firewall Management Center depends on the kind of backup:<br>• Firewall Management Center backups: `/var/sf/backup`<br>• 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**.<br>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**.<br>Unlike moving a backup file, this does not delete the backup from the Firewall Management Center. Store your downloaded backup in a secure location. |

You have successfully managed backup files on your system. The selected operations have been completed, including enabling remote storage, transferring files, or performing file management tasks as specified.

# Backup storage locations

This reference provides information about backup storage options for Firewall Management Centers and managed devices.

*Table 4: Backup storage locations*

| Location | Details |
|---|---|
| Remote, by mounting a network volume (NFS, SMB, SSHFS). | In the Firewall Management Center's system configuration, you can mount an NFS, SMB, or SSHFS network volume as remote storage for Firewall Management Center and device backups; see Remote storage devices.)<br><br>After you do this, all subsequent Firewall Management Center backups *and Firewall Management Center-initiated device backups* are copied to that volume, but you can still use the Firewall Management Center to manage them (restore, download, upload, delete, move).<br><br>Note that only the Firewall Management Center mounts the network volume. Managed device backup files are routed through the Firewall Management Center. Make sure you have the bandwidth to perform a large data transfer between the Firewall Management Center 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). | For the Firewall Management Center, you can use a **Copy when complete** option to securely copy (SCP) completed backups to a remote server.<br><br>When using SCP, you (administrator) must add and verify the remote storage server's SSH host key. If the key is not configured, the file transfer will fail. For more information on key configuration, see Configure SSH for remote storage.<br><br>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.<br><br>This option is useful if you want to store backups locally *and* SCP them to a remote location.<br><br>**Note**<br>If you configure SSHFS remote storage in the Firewall Management Center system configuration, do *not* copy backup files to the same directory using **Copy when complete**. |
| Local, on the Firewall Management Center. | If you do not configure remote storage by mounting a network volume, you can save backup files on the Firewall Management Center:<br><br>• Firewall Management Center backups are saved to `/var/sf/backup`.<br><br>• Device backups are saved to `/var/sf/remote-backup` on the Firewall Management Center if you choose **Management Center** as the **Save in** option when you perform the backup. |
| Local, on the device internal flash memory. | Device backup files are saved to `/var/sf/backup` on the device if you choose **Threat Defence** as the **Save in** option when you perform the backup. |

| Location | Details |
|---|---|
| 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. |

# Manage backup and restoration for multi-instance devices

This section describes how to back up and restore instances on the Secure Firewall 3100/4200. These devices support multiple instances. Use the backup and restore process primarily in Return Material Authorization (RMA) scenarios. If you have a faulty or failed physical appliance, contact Cisco TAC for replacement hardware before beginning the restore process.

Use the configuration export feature to create a file with chassis configuration settings for your Secure Firewall 3100/4200 chassis. You can export this file to a remote server or your local computer. Later, import the configuration file to restore the configuration settings to your Secure Firewall 3100/4200 chassis to return to a known good configuration.

## Back up and restore a single Secure Firewall 3100/4200 instance

Ensure that you can migrate or recover a Secure Firewall instance by backing up its configuration and restoring it to a new chassis.

This task applies when you need to move an instance from one chassis (chassis 1) to another (chassis 2), such as during hardware replacement or recovery.

**Before you begin**

- Verify that both chassis have the same software version, device images, and network modules.
- Ensure that the second chassis (chassis 2) does not use a duplicate management IP address.

Follow these steps to back up and restore your Secure Firewall 3100 or 4200 instance:

### Procedure

**Step 1** Back up the instance on the device.

Use the Firewall Management Center to create a backup file for the instance.

For details about taking a backup, refer to Back up the Firewall Management Center, on page 8

**Note** Firewall Management Center backup files are stored at `/var/sf/backup/`

Example backup file: instance1_20260211105205.tar

**Step 2** Export the chassis configuration.

Export the current configuration through the Firewall Management Center.

For guidance, refer to "Import or Export the Chassis Configuration" section in the Multi-Instance Mode chapter of the *Cisco Secure Firewall Management Center Device Configuration Guide*

**Step 3** Import the chassis configuration to chassis 2.

Before importing, ensure that chassis 2 has:

- The same chassis software version
- The same images as the managed device instance
- The same network modules
- No duplicate management IP address.

Deploy the configuration to the chassis.

After deploying, the instance will have only the base configuration.

**Step 4** After the new instance is online, restore the instance backup on chassis 2.

**a.** Connect to managed device instance using the CLI:

```
firepower-3110# connect ftd instance1
```

**b.** Enter expert mode:

```
> expert
admin@firepower:~$ sudo su
root@firepower:~#
```

**c.** Change to the backup directory:

```
root@firepower:~# cd /var/sf/backup
```

**d.** Download backup file.

```
root@firepower:/var/sf/backup# wget
https://<server-ip>/<path>/instance1_20260211105205.tar --no-check-certificate
```

You can use any method such as SCP, HTTP, or similar file transfer protocols for downloading.

**e.** Exit back to Firewall Threat Defense CLI. Then restore the backup.

```
> restore remote-manager-backup instance1_20260211105205.tar
```

Wait for the restore process to complete.

The instance automatically restarts services. The device and restored instance enter deployment state. Deployment takes approximately 2–3 minutes, during which policies and configurations are re-applied. The sftunnel connection with Firewall Management Center re-establishes automatically, and the backup instance functions as the restored instance. If the UUID and registration key remain valid, manual re-registration is not required.

# Back up and restore a multi-instance HA pair for RMA

Enable recovery of a Secure Firewall High Availability (HA) pair after replacing a faulty chassis by backing up configurations and restoring them to a new chassis.

This task applies when you are recovering a faulty instance of a chassis in a HA pair. For a Return Material Authorization (RMA) procedure, restore the faulty instance onto a new chassis.

Perform this task when one chassis in a Secure Firewall HA pair fails and needs replacement as part of an RMA process.

An HA pair typically includes two multi-instance managed devices running on two different chassis. One device is active and another, standby. If any chassis fails, its configuration must be imported to new hardware, and the HA pair regrouped.

For example, in a HA pair of multi-instance managed devices, the active device hosts instance1 and the standby device hosts instance2. If one of the chassis becomes faulty, import the configuration from the faulty chassis to a replacement chassis. Then regroup the HA pair by restoring the configuration on the failed managed device.

**Before you begin**

- Verify that both chassis (the faulty and the replacement one) have the same software version, device images, and network modules.
- Ensure that the replacement chassis does not use a duplicate management IP address.

This procedure describes the processes for backing up and restoring a multi-instance device in a HA configuration.

## Procedure

**Step 1** Back up the instance configuration on the failed device, using the Firewall Management Center.

For detailed backup instructions, refer to Back up the Firewall Management Center, on page 8

Confirm backup files are generated for the failed device.

Save the backup files, such as FTD01_active_backup.tar

**Step 2** Export the configuration of the faulty chassis to the replacement chassis.

a) Log in to the chassis manager of the faulty chassis.
b) Choose **System** > **Configuration** > **Export**.
c) Export the complete chassis configuration.
d) Log in to the chassis manager of replacement chassis.
e) Choose **System** > **Configuration** > **Import**.

The chassis export contains only the chassis-level configuration. It does not contain the complete instance configuration of the multi-instance device. The instance configuration is restored separately, using the managed device backup.

f) Deploy the imported configuration on the managed device.

Track the instance provisioning task in Firewall Management Center and check that the instance becomes online.

**Step 3** Restore the device backup to the new instance on replacement chassis.

a) Connect to the instance on chassis3.

**Example:**

```
firepower-3130# connect ftd instance1
```

b) Enter expert or root mode.

**Example:**

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

c) Change to backup directory and download the correct backup file.

**Example:**

```
root@firepower:~# cd /var/sf/backup
root@firepower:/var/sf/backup# wget https://<server-ip>/<path>/FTD01_primary_backup.tar
 --no-check-certificate
```

d) Exit back to Firewall Threat Defense CLI. Then restore the backup.

**Example:**

```
> restore remote-manager-backup FTD01_primary_backup.tar
```

**Note** Do not manually recreate HA from Firewall Management Center or un-register the HA pair from the Firewall Management Center.

e) Wait for the restore command to complete execution.

During the restoration of the backup, the services on the managed device restart, the sftunnel restarts, the instance reboots automatically, and the device reconnects to the Firewall Management Center.

The HA pair or device enters a **deployment required** or **pending deployment** state in the Firewall Management Center.

### What to do next

Verify the HA pair recovery in Firewall Management Center.

Confirm all configurations are applied to the managed devices in the HA pair, and connectivity is restored.

# History for backup and restore

This reference provides a chronological history of backup and restore features, including deprecated functionality and version-specific changes across different releases.

*Table 5: History for backup and restore*

| Feature | Minimum Firewall Management Center | Minimum Firewall Threat Defense | Details |
|---|---|---|---|
| Support for cross chassis export and import of configuration for back up and restoration of multi-instance devices | 10.1.0 | 10.1.0 | Use the configuration export and import features across different chassis to back up and restore instances on your multi-instance managed devices. You can back up and restore a single instance or a faulty instance in a high availability pair of multi-instance managed devices. Before you back up and restore, ensure that the faulty and replacement chassis have the same software version, device images, and network modules. |
| Deprecated: Cisco AMP Cloud connection backups. | 7.7.0<br>7.6.1<br>7.4.3<br>7.2.10<br>7.0.7 | Any | Public and private AMP cloud connections are no longer backed up. You must reconfigure them after restore. |
| Deprecated: Backup of locally stored reports on the management center. | 7.6.0<br>7.4.3<br>7.2.11<br>7.0.8 | Any | Locally stored reports are no longer backed up. You should store reports in a secure remote location. |
| Single backup file for high availability Firewall Management Centers | 7.4.1<br>7.2.6 | Any | When performing a configuration-only backup of the active Firewall Management Center in a high availability pair, the system now creates a single backup file which you can use to restore either unit. |
| Back up and restore device clusters | 7.3.0 | Any | You can now use the Firewall Management Center to back up device clusters, except in the public cloud. To restore, use the device CLI.<br>New/modified screens: **System** > **Tools** > **Backup/Restore** > **Managed Device Backup**<br>New/modified commands: **restore remote-manager-backup** |
| 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. |

| Feature | Minimum Firewall Management Center | Minimum Firewall Threat Defense | Details |
|---|---|---|---|
| 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.<br>For supported platforms, see Requirements: backup and restore configuration, on page 3.<br>New/modified screens: **System** > **Tools** > **Backup/Restore** > **Managed Device Backup**<br>New/modified FTD CLI commands: **restore** |