Backup/Restore

About Backup and Restore

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

On-Demand Backups

You can perform on-demand backups for Secure Firewall Threat Defense devices in Security Cloud Control.

For more information, see Back Up Managed Devices, on page 6.

Scheduled Backups

You can use the scheduler on Cloud-Delivered Firewall Management Center to automate backups. You can also schedule remote device backups from Security Cloud Control.

The Cloud-Delivered Firewall Management Center setup process schedules weekly configuration-only backups, to be stored in Cisco's secure cloud storage. This is not a substitute for full off-site backups. After initial setup finishes, you must review your scheduled tasks and adjust them to fit your organization's needs.

For more information, see Schedule Remote Device Backups.

Store Backup Files

When you back up a device, the Cloud-Delivered Firewall Management Center stores the backup files in its secure cloud storage.

Note   Cloud-Delivered Firewall Management Center stores only the 5 most recent Firewall Threat Defense backups per device.

To know how to download an existing backup file, see Step 3 in Restore a Firewall Threat Defense Device, on page 8.

For more information, see Back Up Managed Devices, on page 6.

Restore Managed Devices

You must use the Firewall Threat Defense CLI to restore the Firewall Threat Defense device.

For more information, see Restore Security Cloud Control-Managed Devices, on page 7.

What Is Backed Up?

Device backups are always configuration-only.

What Is Restored?

Restoring configurations overwrites *all* backed-up configurations.

Make sure you understand and plan for the following:

- You cannot restore what is not backed up.

- 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 a Firewall Threat Defense device, you must re-add/re-enroll all VPN certificates, and redeploy the device.

Requirements for Backup and Restore

Backup and restore have the following requirements:

Model Requirements: Backup

You can back up:

- Firewall Threat Defense standalone devices, native instances, container instances, HA pairs, and clusters

- Firewall Threat Defense Virtual for VMware devices, either standalone or HA pairs, and clusters

Backup is *not* supported for:

- Firewall Threat Defense Virtual implementations *other than* for VMware

If you must replace a device where backup and restore is not supported, you must manually recreate device-specific configurations.

Model Requirements: Restore

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

Version Requirements

As the first step in any backup, note the patch level. To restore a backup, the old and the new appliance must be running the same Firewall version, including patches.

License Requirements

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

Guidelines and Limitations for Backup and Restore

Backup and restore have the following guidelines and limitations.

⚠

Caution   Users with CLI access can access the Linux shell access with the **expert** command, which can present a security risk. For system security reasons, we strongly recommend:

- Only use the Linux shell under TAC supervision or when explicitly instructed by Firewall and Security Cloud Control user documentation.

- Restrict the list of users with Linux shell access..

- Do not add users directly in the Linux shell; only use the procedures in this chapter.

Backup and Restore Is for Disaster Recovery/Return Material Authorization

Backup and restore are primarily intended for Return Material Authorization (RMA) scenarios. Before you begin the restore process of a faulty or failed physical appliance, contact for replacement hardware.

Backup and Restore Is Not Configuration Import/Export

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

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 Security Cloud Control. Do not restore an FTD backup to a device being managed by a different manager; the restored device attempts to connect to the manager specified in the backup.

Restore Is Individual and Local

You restore threat defense devices individually and locally. This means:

- You cannot batch-restore to high availability (HA) devices. The restore procedures in this guide explain how to restore in an HA environment.

- You cannot use Security Cloud Control to restore a device. 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.

- You cannot use a Security Cloud Control user account to log into and restore one of its managed devices. Security Cloud Control and Firewall Threat Defense devices maintain their own user accounts.

Best Practices for Backup and Restore

Backup and restore have the following best practices.

When to Back Up

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

You must back up in the following situations:

- Regular backups.

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

- Before upgrade or reimage.

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

- After upgrade.

  Ensure that you back up the device after upgrade, so that you have a freshly upgraded device backup.

Maintaining Backup File Security

Backup files are stored as unencrypted archive (.tar) files; they should be stored in a secure repository.

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

Backup file should be stored securely.

Backup and Restore in Firewall Threat Defense High Availability Deployments

In a Firewall Threat Defense HA deployment, you must:

- Back up the device pair from the cloud-delivered Firewall Management Center, but restore individually and locally from the Firewall Threat Defense CLI.

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

  A Firewall Threat Defense HA device's role is noted in its backup file name. When you restore, make sure you choose the appropriate backup file: primary vs secondary.

- Do *not* suspend or break HA before you restore.

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

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

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

Backup and Restore in Firewall Threat Defense Clustering Deployments

In the Firewall Threat Defense clustering deployment, you must:

- Back up the entire cluster from the cloud-delivered Firewall Management Center, but restore nodes individually and locally from the threat defense CLI.

  The backup process produces a bundled tar file that includes unique backup files for each cluster node. Do not restore one node with the backup file from another. A backup file contains information that uniquely identifies a device, and cannot be shared.

  The node's role is noted in its backup file name. When you restore, make sure you choose the appropriate backup file: control or data.

  You cannot back up individual nodes. If a data node fails to back up, the management center will still back up all other nodes. If the control node fails to back up, the backup is canceled.

- All the nodes that are part of the cluster must be registered in the management center, for the backup to be successful.

- Do *not* suspend or break clustering before you restore. Maintaining the cluster configuration ensures replacement devices can easily reconnect after restore.

- Do *not* run the **restore** CLI command on multiple nodes at the same time. We recommend that you restore the control node first and wait until it rejoins the cluster before you restore any data nodes.

  Assuming you have successful backups, you can replace multiple nodes in the cluster. Any physical replacement tasks you can perform simultaneously: unracking, reracking, and so on. However, do *not* run the **restore** command on an additional node until the restore process completes for the previous node, including the reboot.

Before Restore

Before restore, you must:

- Revert licensing changes.

  Revert any licensing changes made since you took backup.

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

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

- Disconnect faulty appliances.

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

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

- Do *not* unregister managed devices.

Whether you are restoring a managed device, do not unregister devices from the Security Cloud Control, even if you physically disconnect an appliance from the network.

If you unregister, you must redo some device configurations, such as security zone to interface mappings. After you restore, Security Cloud Control and devices should begin communicating normally.

- Reimage.

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

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

After Restore

After restore, you must:

- Reconfigure anything that was not restored.

This can include reconfiguring licensing and audit log server certificate settings. You also must re-add/re-enroll failed Firewall Threat Defense VPN certificates.

- Deploy.

After you restore a device, deploy to that device. You *must* deploy. If the device or devices are not marked out of date, force deploy from the Device Management page.

Back Up Managed Devices

You can perform on-demand or scheduled backups for supported Secure Firewall Threat Defense devices using Cloud-Delivered Firewall Management Center without a backup profile.

For more information, see .

Related Information

Back Up a Firewall Threat Defense Device from Cloud-delivered Firewall Management Center

Use this procedure to perform an on-demand backup of any of the following devices:

- Firewall Threat Defense: Physical devices, standalone, HA, or cluster

• Firewall Threat Defense Virtual: VMware, standalone, HA, or cluster

Backup and restore is not supported for any other platforms or configurations.

Before you begin

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

- Requirements for Backup and Restore, on page 2
- Guidelines and Limitations for Backup and Restore, on page 3
- Best Practices for Backup and Restore, on page 4

⚠

Caution   Users with CLI access can access the Linux shell access with the **expert** command, which can present a security risk. For system security reasons, we strongly recommend:

- Only use the Linux shell under TAC supervision or when explicitly instructed by Firewall and Security Cloud Control user documentation.
- Restrict the list of users with Linux shell access..
- Do not add users directly in the Linux shell; only use the procedures in this chapter.

Procedure

Step 1   Log in to Security Cloud Control.

Step 2   From the Security Cloud Control menu, navigate **Administration** > **Firewall Management Center** to open the **Services** page.

Step 3   Select **Cloud-Delivered FMC** and in the **Actions** pane, click **Devices** to navigate to the Cloud-Delivered Firewall Management Center user interface.

Step 4   Select **System**(⚙) and then navigate **Tools** > **Backup/Restore**.

Step 5   Click **Managed Device Backup**.

Step 6   Select one or more Firewall Threat Defense devices in **Managed Devices**.

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

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

Step 8   Monitor the progress under **Tasks** in the **Notifications** pane.

Restore Security Cloud Control-Managed Devices

For Firewall Threat Defense devices, you must use the Firewall Threat Defense CLI to restore from backup. You cannot use the Firewall Management Center to restore a device.

Related Information:

Restore a Firewall Threat Defense Device

Firewall Threat Defense backup and restore is intended for RMA. Restoring the 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 firewall device, either standalone or in an HA pair. It assumes you have access to a successful backup of the device or devices you are replacing.

Note Do *not* unregister from the Security Cloud Control, even when disconnecting a device from the network. In a Firewall Threat Defense HA deployment, do *not* suspend or break HA. Maintaining these links ensures replacement devices can automatically reconnect after a restore.

In a Firewall Threat Defense HA deployment, you can use this procedure to replace either or both peers. To replace both, perform all steps on both devices simultaneously, except the restore CLI command itself. You cannot replace a Firewall Threat Defense HA device without a successful backup.

Note Starting from the next upgrade of Cloud-Delivered Firewall Management Center, Cisco will only store the 5 most recent Firewall Threat Defense backups per device and purge all the other backups. If you require the other backups for compliance purposes, we recommend that you download them to your private environment by May 31, 2025.

To know how to download an existing backup file, see Step 3 in the procedure below.

Before you begin

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

- Requirements for Backup and Restore, on page 2

- Guidelines and Limitations for Backup and Restore, on page 3

- Best Practices for Backup and Restore, on page 4

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 Navigate **System(⚙)** > **Tools** > **Backup/Restore**.

Step 3 Locate a successful backup of the faulty device from **Device Backups** under **Backup Management**.

Use **Download** that downloads the backup file(s) to your local storage or **Export Backup Links** that generates a URL to download the backup and exports it to a CSV file that gets downloaded. Use the URL to download

the backup to a secure location. Note that the URL is valid only for six hours, after which you must export it again to get a different URL.

In a Firewall Threat Defense HA deployment, you back up the pair as a unit but the backup process produces unique backup files for each device in the pair. The device's role is noted in the backup file name.

If the only copy of the backup is on the faulty device, copy it somewhere else now. If you reimage the device, the backup will be erased. If something else goes wrong, you may not be able to recover the backup.

The replacement device will need the backup, but can retrieve it with the secure copy (SCP) command 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 4   Remove (unrack) the faulty device and disconnect all interfaces. In threat defense HA deployments, this includes the failover link.

See the hardware installation and getttign started guides for your model: Cisco Firepower NGFW: Install and Upgrade Guides.

Note
Do not unregister from the management center, even when disconnecting a device from the network. In threat defense HA deployments, do not suspend or break HA. 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 HA deployments, connect the failover link. However, do *not* connect the data interfaces.

See the hardware installation guide for your model: Cisco Firepower NGFW: Install and Upgrade Guides.

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 Cisco Secure Firewall ASA and Threat Defense Reimage Guide.

Step 7   Perform initial configuration on the replacement device.

Access the Firewall Threat Defense CLI as the admin user. You can use the console or you can SSH to the factory-default management interface IP address (192.168.45.45). A setup wizard prompts you to configure the management IP address, gateway, and other basic network settings.

See the initial configuration topics in the getting started guide for your model: Cisco Firepower NGFW: Install and Upgrade Guides.

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

Step 8   Make sure the replacement device is running the same Firewall software version, including patches, as the faulty device.

The existing device should not be deleted from the 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 management center web interface, complete the device registration process: See *Add a Device to the Management Center* in Cisco Secure Firewall Management Center Device Configuration Guide.

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: Cisco Firewall Management Center Upgrade Guide.

c) Unregister the freshly patched device from the management center: See *Delete a Device from the Management Center* in Cisco Secure Firewall Management Center Device Configuration Guide.

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

Step 9   Make sure the replacement device has access to the backup file.

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

Step 10   From the FTD 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**

Step 11   Log in to Security Cloud Control and wait for the devices to connect.

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

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

Step 12   Before you deploy, perform any post-restore tasks and resolve any post-restore issues:

- Resolve licensing conflicts or orphan entitlements. Contact Cisco TAC.

- Resume HA synchronization.

- Re-add/re-enroll all VPN certificates. The restore process removes VPN certificates from FTD devices, including certificates added after the backup was taken.

Step 13   Deploy configurations.

You must deploy. If a restored device is not marked out of date, force deploy from the Device Management page.

Step 14   Connect the device's data interfaces.

See the hardware installation guide for your model: Cisco Secure Firewall Threat Defense: Install and Upgrade Guides.

Restore Firewall Threat Defense from Backup: Firewall Threat Defense Virtual

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

In Firewall Threat Defense HA and clustering deployments, 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. In Firewall Threat Defense HA and clustering deployments, do *not* suspend or break high availibility or clusters. Maintaining registration ensures that replacement devices can automatically reconnect after restore.

Before you begin

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

- Requirements for Backup and Restore, on page 2
- Guidelines and Limitations for Backup and Restore, on page 3
- Best Practices for Backup and Restore, on page 4

Procedure

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

Step 2 Locate a successful backup of the faulty device from **Device Backups** under **Backup Management**.

For clustering, node backup files are bundled together in a single compressed file for the cluster (*cluster_name.timestamp***.tar.gz**). Before you can restore nodes, you need to extract the individual node backup files (*node_name_***control_***timestamp***.tar** or *node_name_***data_***timestamp***.tar**).

Use **Download** that downloads the backup file(s) to your local storage or **Export Backup Links** that generates a URL to download the backup and exports it to a CSV file that gets downloaded. Use the URL to download the backup to a secure location. Note that the URL is valid only for six hours, after which you must export it again to get a different URL.

In Firewall Threat Defense HA deployments, you back up the pair as a unit, but the backup process produces unique backup files for each device in the pair. The device's role is noted in the backup file name.

If the only copy of the backup is on the faulty device, copy it somewhere else now. If you reimage the device, the backup will be erased. If something else goes wrong, you may not be able to recover the backup.

The replacement device needs 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 the faulty device.

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

Step 4 Deploy a replacement device.

See the Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide.

Step 5 Perform initial configuration on the replacement device.

Use the VMware console to access the Firewall Threat Defense Virtual 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: Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide.

Step 6 Make sure that the replacement device is running the same Firewall software version, including patches, as the faulty device.

Ensure that the existing device should not be deleted from the Security Cloud Control. The replacement device should be unmanaged from the physical network and the new hardware and the replacing Firewall Threat Defense Virtual patch should have the same version. The Firewall Threat Defense Virtual CLI does not have an upgrade command. To patch:

   a. Complete the Firewall Threat Defense Virtual registration process in Security Cloud Control.

   b. Patch the Firewall Threat Defense Virtual device.

   c. Unregister the freshly patched device from Security Cloud Control.

Step 7 Make sure that 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 clusters, make sure you extract the individual node backup file from the main cluster bundle.

Step 8 From the Firewall Threat Defense CLI, restore the backup.

Access the Firewall Threat Defense Virtual 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 HA 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 9 Log into Security Cloud Control and wait for the devices to connect.

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

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

Step 10 Before you deploy, perform any post-restore tasks and resolve any post-restore issues:

- Resolve licensing conflicts or orphan entitlements. Contact Cisco TAC.

- Resume HA synchronization.

- Re-add/re-enroll all VPN certificates. The restore process removes VPN certificates from Firewall Threat Defense Virtual devices, including certificates added after the backup was taken.

Step 11 Deploy configurations.

You must deploy. If a restored device is not marked out of date, force deploy from the Device Management page.

Step 12 Connect the device's data interfaces.

See the hardware installation guide for your model: Cisco Secure Firewall Threat Defense: Install and Upgrade Guides.