High Availability

The following topics describe how to configure Active/Standby high availability of Cisco Secure Firewall Management Centers:

- About Management Center High Availability, on page 1
- Requirements for Management Center High Availability, on page 7
- Prerequisites for Management Center High Availability, on page 9
- Establishing Management Center High Availability, on page 10
- Viewing Management Center High Availability Status, on page 15
- Configurations Synced on Management Center High Availability Pairs, on page 16
- Configuring External Access to the Management Center Database in a High Availability Pair, on page 17
- Using CLI to Resolve Device Registration in Management Center High Availability, on page 17
- Switching Peers in the Management Center High Availability Pair, on page 18
- Pausing Communication Between Paired Management Centers, on page 18
- Restarting Communication Between Paired Management Centers, on page 19
- Change the IP Address of the Management Center in a High Availability Pair, on page 19
- Disabling Management Center High Availability, on page 20
- Replacing Management Centers in a High Availability Pair, on page 20
- Restoring Management Center in a High Availability Pair (No Hardware Failure), on page 24
- History for Management Center High Availability, on page 27

About Management Center High Availability

To ensure the continuity of operations, the high availability feature allows you to designate redundant management centers to manage devices. The management centers support Active/Standby high availability where one appliance is the active unit and manages devices. The standby unit does not actively manage devices. The active unit writes configuration data into a data store and replicates data for both units, using synchronization where necessary to share some information with the standby unit.

Active/Standby high availability lets you configure a secondary management center to take over the functionality of a primary management center if the primary fails. When the primary management center fails, you must promote the secondary management center to become the active unit.

Event data streams from managed devices to both management centers in the high availability pair. If one management center fails, you can monitor your network without interruption using the other management center.

Note that management centers configured as a high availability pair do not need to be on the same trusted management network, nor do they have to be in the same geographic location.

Caution Because the system restricts some functionality to the active management center, if that appliance fails, you must promote the standby management center to active.

Note Triggering a switchover on management center immediately after a successful change deployment can lead to preview configuration not working on the new active management center. This does not impact policy deploy functionality. It is recommended to trigger a switchover on the management center after the necessary sync is completed.

Similarly, when management center HA synchronization is in degraded state, triggering a switchover or changing roles could make management center HA to damage the database and it can become catastrophic. We recommend that you immediately contact Cisco Technical Assistance Center (TAC) for further assistance to resolve this issue.

This HA synchronization can end up in degraded state due to various reasons. The Replacing Management Centers in a High Availability Pair, on page 20 section in this chapter covers some of the failure scenarios and the subsequent procedure to fix the issue. If the reason or scenario of degraded state matches to the scenarios explained, follow the steps to fix the issue. For other reasons, we recommend that you contact TAC.

About Remote Access VPN High Availability

If the primary device has Remote Access VPN configuration with an identity certificate enrolled using a CertEnrollment object, the secondary device must have an identity certificate enrolled using the same CertEnrollment object. The CertEnrollment object can have different values for the primary and secondary devices due to device-specific overrides. The limitation is only to have the same CertEnrollment object enrolled on the two devices before the high availability formation.

SNMP Behavior in Management Center High Availability

In an SNMP-configured HA pair, when you deploy an alert policy, the active management center sends the SNMP traps. When the primary management center fails, the secondary management center which becomes the active unit starts sending the SNMP traps without the need for any additional configuration.

Roles v. Status in Management Center High Availability

Primary/Secondary Roles

When setting up Secure Firewall Management Centers in a high availability pair, you configure one Secure Firewall Management Center to be primary and the other as secondary. During configuration, the primary unit's policies are synchronized to the secondary unit. After this synchronization, the primary Secure Firewall Management Center becomes the active peer, while the secondary Secure Firewall Management Center becomes the standby peer, and the two units act as a single appliance for managed device and policy configuration.

Active/Standby Status

The main differences between the two Secure Firewall Management Centers in a high availability pair are related to which peer is active and which peer is standby. The active Secure Firewall Management Center remains fully functional, where you can manage devices and policies. On the standby Secure Firewall Management Center, functionality is hidden; you cannot make any configuration changes.

Event Processing on Management Center High Availability Pairs

Since both management centers in a high availability pair receive events from managed devices, the management IP addresses for the appliances are not shared. This means that you do not need to intervene to ensure continuous processing of events if one of the management center fails.

AMP Cloud Connections and Malware Information

Although they share file policies and related configurations, management centers in a high availability pair share neither Cisco AMP cloud connections nor malware dispositions. To ensure continuity of operations, and to ensure that detected files' malware dispositions are the same on both management centers, both primary and secondary management centers must have access to the AMP cloud.

URL Filtering and Security Intelligence

URL filtering and Security Intelligence configurations and information are synchronized between Secure Firewall Management Centers in a high availability deployment. However, only the primary Secure Firewall Management Center downloads URL category and reputation data for updates to Security Intelligence feeds.

If the primary Secure Firewall Management Center fails, not only must you make sure that the secondary Secure Firewall Management Center can access the internet to update threat intelligence data, but you must also use the web interface on the secondary Secure Firewall Management Center to promote it to active.

User Data Processing During Management Center Failover

If the primary management center fails, the Secondary management center propagates to managed devices user-to-IP mappings from the TS Agent identity source; and propagates SGT mappings from the ISE/ISE-PIC identity source. Users not yet seen by identity sources are identified as Unknown.

After the downtime, the Unknown users are re identified and processed according to the rules in your identity policy.

Configuration Management on Management Center High Availability Pairs

In a high availability deployment, only the active management center can manage devices and apply policies. Both management centers remain in a state of continuous synchronization.

If the active management center fails, the high availability pair enters a degraded state until you manually promote the standby appliance to the active state. Once the promotion is complete, the appliances leave maintenance mode.

Management Center High Availability Disaster Recovery

In case of a disaster recovery situation, a manual switchover must be performed. When the primary management center - FMC1 fails, access the web interface of the secondary management center - FMC2 and switch peers.

This is applicable conversely also in case the secondary (FMC2) fails. For more information, see Switching Peers in the Management Center High Availability Pair, on page 18.

For restoring a failed management center, refer to Replacing Management Centers in a High Availability Pair, on page 20.

Single Sign-On and High Availability Pairs

Management Centers in a high availability configuration can support Single Sign-On, but you must keep the following considerations in mind:

- SSO configuration is not synchronized between the members of the high availability pair; you must configure SSO separately on each member of the pair.
- Both management centers in a high availability pair must use the same identity provider (IdP) for SSO. You must configure a service provider application at the IdP for each management center configured for SSO.
- In a high availability pair of management centers where both are configured to support SSO, before a user can use SSO to access the secondary management center for the first time, that user must first use SSO to log into the primary management center at least once.
- When configuring SSO for management centers in a high availability pair:
  - If you configure SSO on the primary management center, you are not required to configure SSO on the secondary management center.
  - If you configure SSO on the secondary management center, you are required to configure SSO on the primary management center as well. (This is because SSO users must log in to the primary management center at least once before logging into the secondary management center.)

Related Topics

Configure SAML Single Sign-On

Management Center High Availability Behavior During a Backup

When you perform a Backup on a management center high availability pair, the Backup operation pauses synchronization between the peers. During this operation, you may continue using the active management center, but not the standby peer.

After Backup is completed, synchronization resumes, which briefly disables processes on the active peer. During this pause, the High Availability page briefly displays a holding page until all processes resume.

Management Center High Availability Split-Brain

If the active management center in a high-availability pair goes down (due to power issues, network/connectivity issues), you can promote the standby management center to an active state. When the original active peer comes up, both peers can assume they are active. This state is defined as 'split-brain'. When this situation occurs, the system prompts you to choose an active appliance, which demotes the other appliance to standby.

If the active management center goes down (or disconnects due to a network failure), you may either break high availability or switch roles. The standby management center enters a degraded state.

Note Whichever appliance you use as the intended standby loses all of its device registrations and policy configurations when you resolve split-brain. For example, you would lose modifications to any policies that existed on the intended standby but not on the intended active. If the management center is in a high availability split-brain scenario where both appliances are active, and you register managed devices and deploy policies before you resolve split-brain, you must export any policies and unregister any managed devices from the intended standby management center before re-establishing high availability. You may then register the managed devices and import the policies to the intended active management center.

Troubleshooting Management Center High Availability

This section lists troubleshooting information for some common management center high availability operation errors.

Error	Description	Solution
You must reset your password on the active management center before you can log in to the standby.	You attempted to log into the standby management center when a force password reset is enabled for your account.	As the database is read-only for a standby management center, reset the password on the login page of the active management center.
500 Internal	May appear when attempting to access the web interface while performing critical management center high availability operations, including switching peer roles or pausing and resuming synchronization.	Wait until the operation completes before using the web interface.
System processes are starting, please wait Also, the web interface does not respond.	May appear when the management center reboots (manually or while recovering from a power down) during a high availability or data synchronization operation.	**1.** Access the management center shell and use the `manage_hadc.pl` command to access the management center high availability configuration utility. **Note** Run the utility as a root user, using `sudo`. **2.** Pause mirroring operations by using option 5. Reload the management center web interface. **3.** Use the web interface to resume synchronization. Choose **Integration** > **Other Integrations**, then click the **High Availability** tab and choose **Resume Synchronization**.

Error	Description	Solution
Device Registration Status:Host <*string*> is not reachable	During the initial configuration of a threat defense, if the management center IP address and NAT ID are specified, the **Host** field can be left blank. However, in an HA environment with both the management centers behind a NAT, this error occurs when you add the threat defense on the secondary management center.	1. Delete the threat defense from primary management center. See *Delete a Device from the* Management Center in Cisco Secure Firewall Management Center Device Configuration Guide. 2. Remove managers from threat defense using the **configure manager delete** command. See Cisco Secure Firewall Threat Defense Command Reference. 3. Add threat defense to the management center with the IP address or name of the threat defense device in the **Host** field. See *Add a Device to the* Management Center in Cisco Secure Firewall Management Center Device Configuration Guide.
Device Registration Status:Host <*string*> is not reachable	The error occurs when adding threat defense device to the secondary management center center in a high-availability deployment where both the secondary management center and the threat defense device are behind NAT.	On the standby management center web interface, click **Integration** > **Other Integrations** > **High Availability**. Under the pending device registration table, click the IP address of the pending device, and then change the IP address to the public IP address of the threat defense. OR 1. Access the threat defense shell and use the `show managers` command to get the standby management center entry identifier value. 2. In the threat defense shell, edit the standby management center hostname to the public IP address. Execute the `configure manager edit <standby_uuid> hostname <standby_ip>` command using the entry identifier value and the host IP address. For more information, see Using CLI to Resolve Device Registration in Management Center High Availability, on page 17.

Requirements for Management Center High Availability

Model Support

See Hardware Requirements, on page 7.

Virtual Model Support

See Virtual Platform Requirements, on page 7.

Supported Domains

Global

User Roles

Admin

Hardware Requirements

- All management center hardware supports high availability. The peers must be the same model.
- The peers may be physically and geographically separated from each other in different data centers.
- Bandwidth requirement for high availability configuration depends on various factors such as the size of the network, the number of managed devices, the volume of events and logs, and the size and frequency of configuration updates.

  For a typical management center high availability deployment, in case of high latency networks of close to 100 ms, a minimum of 5 Mbps network bandwidth between the peers is recommended.

  You can enhance the high availability synchronization speed by reducing the number of configuration versions saved on your management center. For more information, see *Set the Number of Configuration Versions* in Cisco Secure Firewall Management Center Device Configuration Guide. Note that this option is not supported on Secure Firewall Management Center versions 7.3.0 and 7.4.0.
- Ensure that both management centers have unique UUIDs. To check the UUID, review this file:`/etc/sf/ims.conf`.
- Do not restore a backup of the primary peer to the secondary.
- See also License Requirements for Management Center High Availability Configurations, on page 8.

Virtual Platform Requirements

High availability is supported for the following public cloud platforms:

- Amazon Web Services (AWS)
- Oracle Cloud Infrastructure (OCI)

And these on-prem/private cloud platforms:

- Cisco HyperFlex
- Kernel-based virtual machine (KVM)
- VMware vSphere/VMware ESXi

The management centers must have the same device management capacity (not supported on FMCv2) and be identically licensed. You also need one threat defense entitlement for each managed device. For more information, see License Requirements for Management Center High Availability Configurations, on page 8.

Note If you are managing Version 7.0.x Classic devices only (NGIPSv or ASA FirePOWER), you do not need FMCv entitlements.

Software Requirements

Access the **Appliance Information** widget to verify the software version, the intrusion rule update version and the vulnerability database update. By default, the widget appears on the **Status** tab of the **Detailed Dashboard** and the **Summary Dashboard**. For more information, see The Appliance Information Widget

- The two management centers in a high availability configuration must have the same major (first number), minor (second number), and maintenance (third number) software version.
- The two management centers in a high availability configuration must have the same version of the intrusion rule update installed.
- The two management centers in a high availability configuration must have the same version of the vulnerability database update installed.
- The two management centers in a high availability configuration must have the same version of the LSP (Lightweight Security Package) installed.
- The two management centers in a high availability configuration must have port 8305 accessible between them for communication.

Warning If the software versions, intrusion rule update versions and vulnerability database update versions are not identical on both management centers, you cannot establish high availability.

License Requirements for Management Center High Availability Configurations

Each device requires the same licenses whether managed by a single management center or by management centers in a high availability pair (hardware or virtual).

Example: If you want to enable advanced malware protection for two devices managed by a management center pair, buy two Malware Defense licenses and two TM subscriptions, register the active management center with the Smart Software Manager, then assign the licenses to the two devices on the active management center.

Only the active management center is registered with the Smart Software Manager. When failover occurs, the system communicates with Smart Software Manager to release the license entitlements from the originally-active management center and assign them to the newly-active management center.

In Specific License Reservation deployments, only the primary management center requires a Specific License Reservation.

Hardware Management Center

No special license is required for hardware management centers in a high availability pair.

Management Center Virtual

You will need two identically licensed management center virtuals.

Example: For the management center virtual high availability pair managing 10 devices, you can use:

- Two (2) management center virtual 10 entitlements
- 10 device licenses

If you break the high availability pair, the management center virtual entitlements associated with the secondary management center virtual are released. (In the example, you would then have two standalone management center virtual 10s.)

Prerequisites for Management Center High Availability

Before establishing the management center high availability pair:

- Export required policies from the intended secondary management center to the intended primary management center. For more information, see Exporting Configurations.
- Make sure that the intended secondary management center does not have any devices added to it. Delete devices from the intended secondary management center and register these devices to the intended primary management center. For more information see *Delete a Device from the Management Center* and *Add a Device to the Management Center* in the Cisco Secure Firewall Management Center Device Configuration Guide.
- Import the policies into the intended primary management center. For more information, see Importing Configurations.
- On the intended primary management center, verify the imported policies, edit them as needed and deploy them to the appropriate device. For more information, see *Deploy Configuration Changes* in the Cisco Secure Firewall Management Center Device Configuration Guide.
- On the intended primary management center, associate the appropriate licenses to the newly added devices. For more information see Assign Licenses to a Single Device.

You can now proceed to establish high availability. For more information, see Establishing Management Center High Availability, on page 10.

Establishing Management Center High Availability

Establishing high availability can take a significant amount of time, even several hours, depending on the bandwidth between the peers and the number of policies. It also depends on the number of devices registered to the active management center, which need to be synced to the standby management center. You can view the High Availability page to check the status of the high availability peers.

Before you begin

- Confirm that both the management centers adhere to the high availability system requirements. For more information , see Requirements for Management Center High Availability, on page 7.
- Confirm that you completed the prerequisites for establishing high availability. For more information, see Prerequisites for Management Center High Availability, on page 9.
- In a multidomain deployment, you must be in the Global domain to perform this task.

Procedure

Step 1 Log into the management center that you want to designate as the secondary.

Step 2 Choose **Integration** > **Other Integrations**.

Step 3 Choose **High Availability**.

Step 4 Under Role for this management center, choose **Secondary**.

Step 5 Enter the hostname or IP address of the primary management center in the **Primary Firewall Management Center Host** text box.

You can leave this empty if the primary management center does not have an IP address reachable from the peer management center (which can be public or private IP address). In this case, use both the **Registration Key** and the **Unique NAT ID** fields. You need to specify the IP address of at least one management center to enable HA connection.

Step 6 Enter a one-time-use registration key in the **Registration Key** text box.

The registration key is any user-defined alphanumeric value up to 37 characters in length. This registration key will be used to register both -the secondary and the primary management centers.

Step 7 If you did not specify the primary IP address, or if you do not plan to specify the secondary IP address on the primary management center, then in the **Unique NAT ID** field, enter a unique alphanumeric ID. See NAT Environments for more information.

Step 8 Click **Register**.

Step 9 Using an account with Admin access, log into the management center that you want to designate as the primary.

Step 10 Choose **Integration** > **Other Integrations**.

Step 11 Choose **High Availability**.

Step 12 Under Role for this management center, choose **Primary**.

Step 13 Enter the hostname or IP address of the secondary management center in the **Secondary Firewall Management Center Host** text box.

You can leave this empty if the secondary management center does not have an IP address reachable from the peer management center (which can be public or private IP address). In this case, use both the **Registration Key** and the **Unique NAT ID** fields. You need to specify the IP address of at least one management center to enable HA connection.

Step 14 Enter the same one-time-use registration key in the **Registration Key** text box you used in step 6.

Step 15 If required, enter the same NAT ID that you used in step 7 in the **Unique NAT ID** text box.

Step 16 Click **Register**.

What to do next

After establishing the management center high availability pair, devices registered to the active management center are automatically registered to the standby management center.

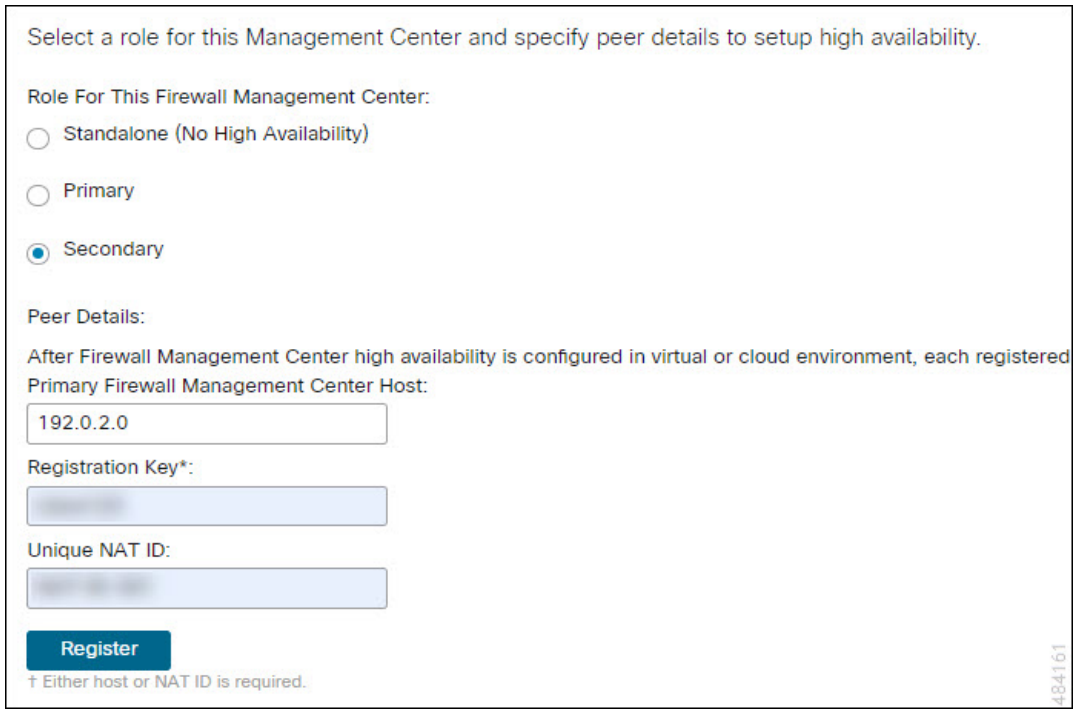
Note When a registered device has a NAT IP address, automatic device registration fails and the secondary management center High Availability page lists the device as local, pending. You can then assign a different NAT IP address to the device on the standby management center High Availability page. If automatic registration otherwise fails on the standby management center, but the device appears to be registered to the active Secure Firewall Management Center, see Using CLI to Resolve Device Registration in Management Center High Availability, on page 17.

High Availability for Management Centers Hosted on Public Cloud

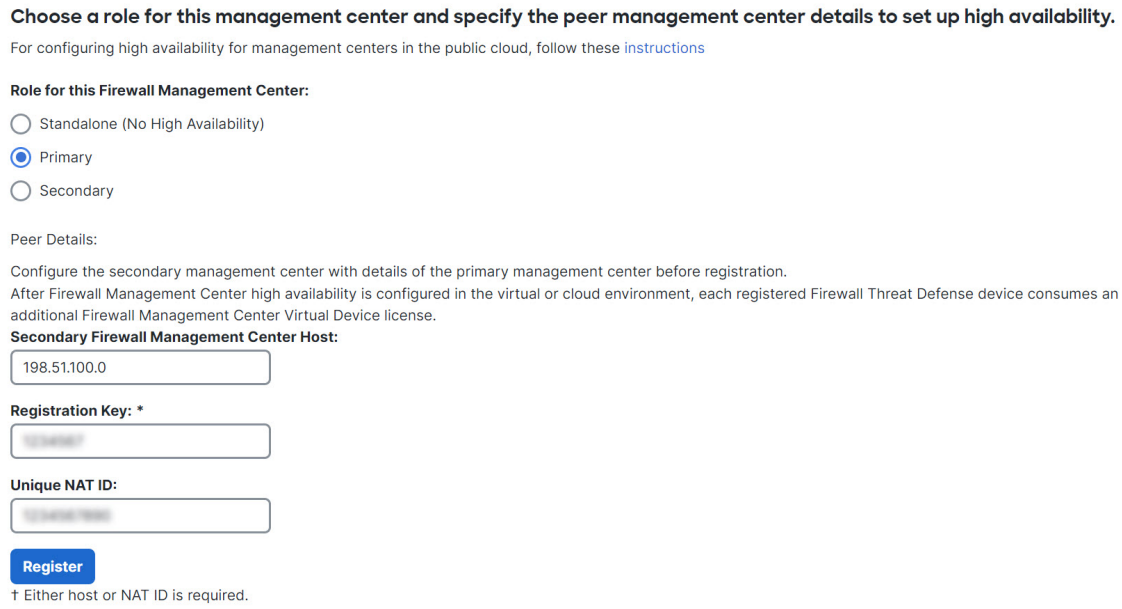
While establishing high availability between management centers hosted on public clouds, the combinations of IP addresses or hostnames for the primary and secondary management centers described below can successfully form high availability and get the devices registered on both the peers. In the **High Availability** page (**Integration** > **Other Integrations** > **High Availability**), perform one of the following configurations to successfully form high availability between management centers hosted in public cloud.

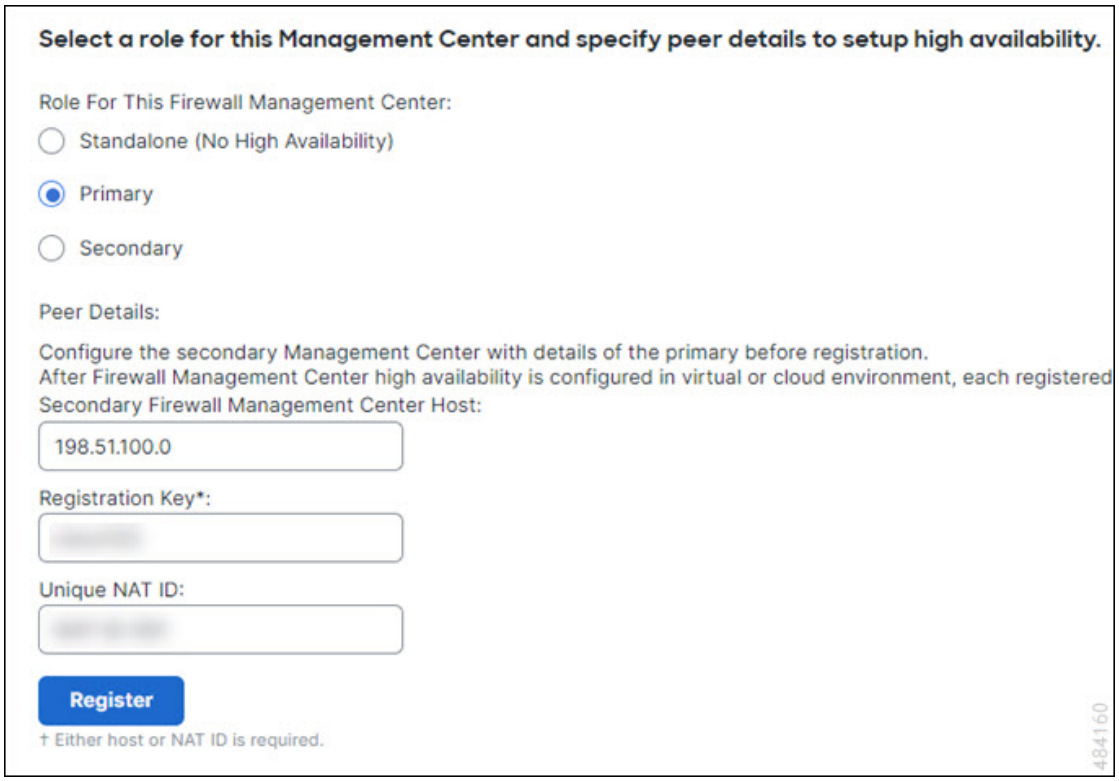
Using the Public IP Addresses or Hostnames for Both the Primary and Secondary Management Centers

1. On the secondary management center, do the following:
   a. Choose **Secondary** as the **Role for this Firewall Management Center**.
   b. Enter the public IP address or hostname for the secondary management center in the **Primary Firewall Management Center Host** field.
   c. Enter the registration key.
   d. Enter the same NAT ID that you used in the primary management center.



2. On the primary management center, do the following:
   a. Choose **Primary** as the **Role for this Firewall Management Center**.
   b. Enter the public IP address or hostname for the secondary management center in the **Secondary Firewall Management Center Host** field.
   c. Enter the registration key.
   d. Enter the unique NAT ID.





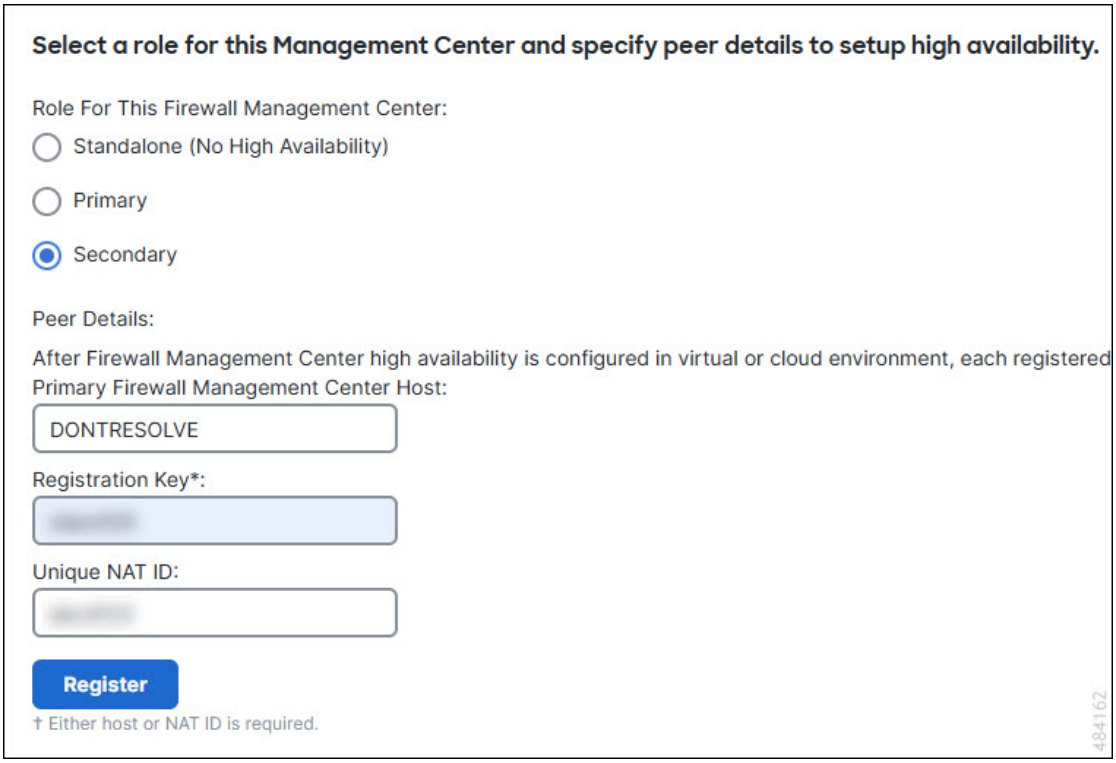
Using the Public IP Address or Hostname for the Secondary Management Center

1. On the secondary management center, do the following:
   a. Choose **Secondary** as the **Role for this Firewall Management Center**.

b. Enter **DONTRESOLVE** in the **Primary Firewall Management Center Host** field.

c. Enter the registration key.

d. Enter the same NAT ID that you used in the primary management center.



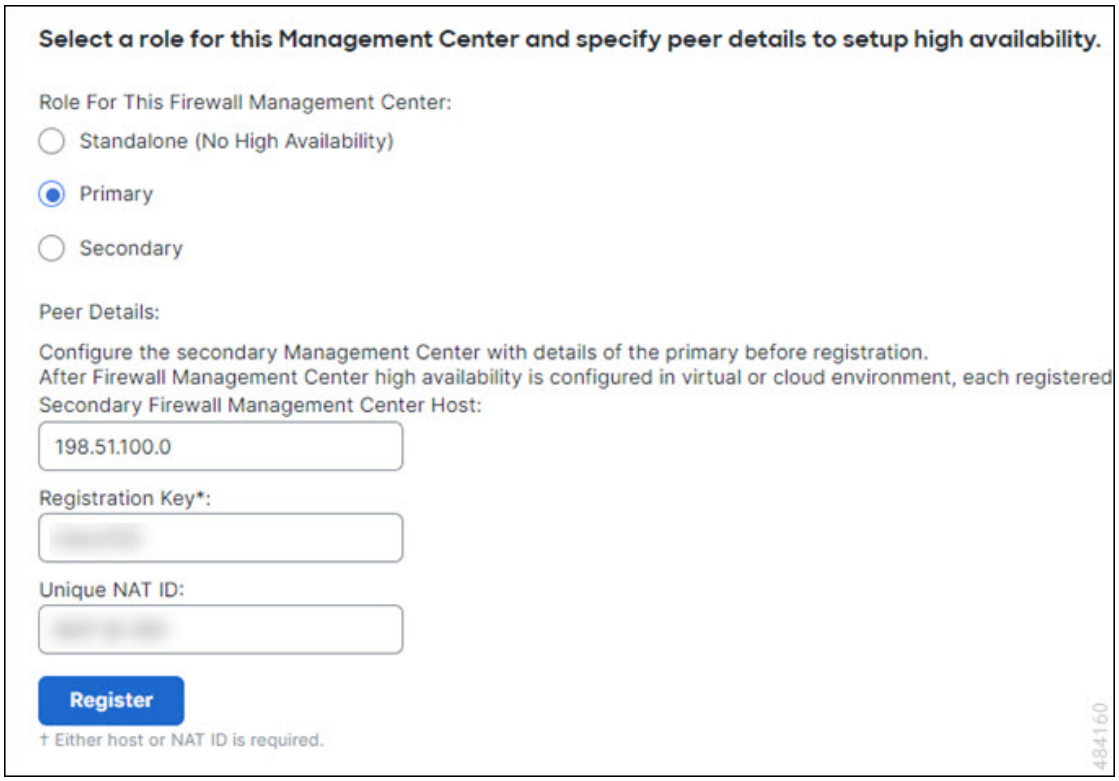
2. On the primary management center, do the following:

a. Choose **Primary** as the **Role for this Firewall Management Center**.

b. Enter the public IP address or hostname for the secondary management center in the **Secondary Firewall Management Center Host** field.

c. Enter the registration key.

d. Enter the unique NAT ID.



Viewing Management Center High Availability Status

After you identify your active and standby management centers, you can view information about the local management center and its peer.

Note In this context, Local Peer refers to the appliance where you are viewing the system status. Remote Peer refers to the other appliance, regardless of active or standby status.

Procedure

Step 1 Log into one of the management centers that you paired using high availability.

Step 2 Choose **Integration** > **Other Integrations**.

Step 3 Choose **High Availability**.

You can view:

Summary Information

- The health status of the high availability pair. The status of a correctly functioning system will oscillate between "Healthy" and "Synchronization task is in progress" as the standby unit receives configuration changes from the active unit.

- The current synchronization status of the high availability pair
- The IP address of the active peer and the last time it was synchronized
- The IP address of the standby peer and the last time it was synchronized

System Status

- The configured IP addresses for both peers
- The operating system for both peers
- The software version for both peers
- The appliance model of both peers

Note
You can view export control and compliance status only on the active management center.

Remote and Local Device Registration
You can view the list of devices that are pending or failed registration on management center.

Configurations Synced on Management Center High Availability Pairs

When you establish high availability between two management centers, the following configuration data is synced between them:

- License entitlements
- Access control policies
- Intrusion rules
- Malware and file policies
- DNS policies
- Identity policies
- SSL policies
- Prefilter policies
- Network discovery rules
- Application detectors
- Correlation policy rules
- Alerts
- Scanners
- Response groups

- Contextual cross-launch of external resources for investigating events
- Remediation settings, although you must install custom modules on both management centers. For more information on remediation settings, see Managing Remediation Modules.

Configuring External Access to the Management Center Database in a High Availability Pair

In a high availability setup, we recommend you to use only the active peer to configure the external access to the database. When you configure the standby peer for external database access, it leads to frequent disconnections. To restore the connectivity, you must pause and resume the synchronization of the standby peer. For information on how to enable external database access to management centers, see Enabling External Access to the Database .

Using CLI to Resolve Device Registration in Management Center High Availability

If automatic device registration fails on the standby management center, but appears to be registered to the active management center, complete the following steps:

Warning If you do an RMA of secondary management center or add a secondary management center, the managed devices are unregistered, and their configuration can get deleted as a result.

Procedure

Step 1 Delete the device from the active management center. See *Delete (Unregister) a Device from the management center* in Cisco Secure Firewall Management Center Device Configuration Guide.

Step 2 Complete the following steps to trigger automatic registration of the device on the standby management center:

a. Log in to the CLI for the affected device.

b. Run the CLI command: **configure manager delete**.

This command disables and removes the current management center.

c. Run the CLI command: **configure manager add**.

This command configures the device to initiate a connection to a management center.

Tip
Configure remote management on the device, only for the active management center. When you establish high availability, the devices are automatically registered to the standby management center.

d. Log in to the active management center and register the device.

Step 3 If the standby management center is behind NAT, complete the following steps to edit the hostname of the standby management center:

a. Access the threat defense shell and use the `show managers` command to get the standby management center entry identifier value.

b. In the threat defense shell, edit the standby management center hostname to the public IP address. Execute the `configure manager edit <standby_uuid> hostname <standby_ip>` command using the entry identifier value and the host IP address.

Switching Peers in the Management Center High Availability Pair

Because the system restricts some functionality to the active management center, if that appliance fails, you must promote the standby management center to active:

Procedure

Step 1 Log into one of the management centers that you paired using high availability.

Step 2 Choose **Integration** > **Other Integrations**.

Step 3 Choose **High Availability**.

Step 4 Choose **Switch Peer Roles** to change the local role from Active to Standby, or Standby to Active. With the Primary or Secondary designation unchanged, the roles are switched between the two peers.

Pausing Communication Between Paired Management Centers

If you want to temporarily disable high availability, you can disable the communications channel between the management centers. You can pause synchronization from an active or standby peer.

Procedure

Step 1 Log into one of the management centers that you paired using high availability.

Step 2 Choose **Integration** > **Other Integrations**.

Step 3 Choose **High Availability**.

Step 4 Choose **Pause Synchronization**.

Restarting Communication Between Paired Management Centers

If you temporarily disable high availability, you can restart high availability by enabling the communications channel between the management centers. You can resume synchronization from an active or standby peer.

Procedure

Step 1 Log into one of the management centers that you paired using high availability.

Step 2 Choose **Integration** > **Other Integrations**.

Step 3 Choose **High Availability**.

Step 4 Choose **Resume Synchronization**.

Change the IP Address of the Management Center in a High Availability Pair

If the IP address for one of the high availability peers is changed, this change will not be automatically updated on the other peer, even after performing a high availability synchronization. To ensure that the remote peer management center is also updated, you must manually change the IP address.

Procedure

Step 1 Log in to the peer management center where you want to manually modify the IP address of the other peer manager.

Step 2 Choose **Integration** > **Other Integrations**.

Step 3 Choose **High Availability**.

Step 4 Choose **Peer Manager**.

Step 5 Choose **Edit** ( ).

Step 6 Enter the display name of the appliance, which is used only within the context of the system.

Entering a different display name does not change the host name for the appliance.

Step 7 Enter the fully qualified domain name or the name that resolves through the local DNS to a valid IP address (that is, the host name), or the host IP address.

Step 8 Click **Save**.

Disabling Management Center High Availability

Procedure

Step 1 Log into one of the management centers in the high availability pair.

Step 2 Choose **Integration** > **Other Integrations**.

Step 3 Choose **High Availability**.

Step 4 Choose **Break High Availability**.

Step 5 Choose one of the following options for handling managed devices:

- To control all managed devices with this management center, choose **Manage registered devices from this console**. All devices will be unregistered from the peer.
- To control all managed devices with the other management center, choose **Manage registered devices from peer console**. All devices will be unregistered from this management center.
- To stop managing devices altogether, choose **Stop managing registered devices from both consoles**. All devices will be unregistered from both management centers.

Note
If you choose to manage the registered devices from the secondary management center, the devices will be unregistered from the primary management center. The devices are now registered to be managed by the secondary management center. However the licenses that were applied to these devices are deregistered on account of the high availability break operation. You must now proceed to re-register (enable) the licenses on the devices from the secondary management center. For more information see Assign Licenses to Devices.

Step 6 Click **OK**.

Replacing Management Centers in a High Availability Pair

If you need to replace a failed unit in the management center high availability pair, you must follow one of the procedures listed below. The table lists four possible failure scenarios and their corresponding replacement procedures.

Failure Status	Data Backup Status	Replacement Procedure
Primary management center failed	Data backup successful	Replace a Failed Primary Management Center (Successful Backup), on page 21
	Data backup not successful	Replace a Failed Primary Management Center (Unsuccessful Backup), on page 22

Failure Status	Data Backup Status	Replacement Procedure
Secondary management center failed	Data backup successful	Replace a Failed Secondary Management Center (Successful Backup), on page 23
	Data backup not successful	Replace a Failed Secondary Management Center (Unsuccessful Backup), on page 23

Replace a Failed Primary Management Center (Successful Backup)

Two management centers, *FMC1* and *FMC2*, are part of a high availability pair. *FMC1* is the primary and *FMC2* is the secondary. This task describes the steps to replace a failed primary management center, *FMC1*, when data backup from the primary is successful.

Before you begin

Verify that the data backup from the failed primary management center is successful.

Procedure

Step 1 Contact Support to request a replacement for a failed management center - *FMC1*.

Step 2 When the primary management center - *FMC1* fails, access the web interface of the secondary management center - *FMC2* and switch peers. For more information, see Switching Peers in the Management Center High Availability Pair, on page 18.

This promotes the secondary management center - *FMC2* to active.

You can use *FMC2* as the active management center until the primary management center - *FMC1* is replaced.

Caution
Do not break management center high availability from *FMC2*, since licenses that were synced to *FMC2* from *FMC1* (before failure), will be removed from *FMC2* and you will be unable to perform any deploy actions from *FMC2*.

Step 3 Reimage the replacement management center with the same software version as *FMC1*.

Step 4 Restore the data backup retrieved from *FMC1* to the new management center.

Step 5 Install required management center patches, geolocation database (GeoDB) updates, vulnerability database (VDB) updates and system software updates to match *FMC2*.

The new management center and *FMC2* will now both be active peers, resulting in a high availability split-brain.

Step 6 When the management center web interface prompts you to choose an active appliance, select *FMC2* as active.

This syncs the latest configuration from *FMC2* to the new management center - *FMC1*.

Step 7 When the configuration syncs successfully, access the web interface of the secondary management center - *FMC2* and switch roles to make the primary management center - *FMC1* active. For more information, see Switching Peers in the Management Center High Availability Pair, on page 18.

What to do next

High availability has now been re-established and the primary and the secondary management centers will now work as expected.

Replace a Failed Primary Management Center (Unsuccessful Backup)

Two management centers - *FMC1* and *FMC2* are part of a high availability pair. *FMC1* is the primary and *FMC2* is the secondary. This task describes the steps to replace a failed primary management center -*FMC1* when data backup from the primary is unsuccessful.

Procedure

Step 1 Contact Support to request a replacement for a failed management center - *FMC1*.

Step 2 When the primary management center - *FMC1* fails, access the web interface of the secondary management center - *FMC2* and switch peers. For more information, see Switching Peers in the Management Center High Availability Pair, on page 18.

This promotes the secondary management center - *FMC2* to active.

You can use *FMC2* as the active management center until the primary management center - *FMC1* is replaced.

Caution
Do not break management center High Availability from *FMC2*, since licenses that were synced to *FMC2* from *FMC1* (before failure), will be removed from *FMC2* and you will be unable to perform any deploy actions from *FMC2*.

Step 3 Reimage the replacement management center with the same software version as *FMC1*.

Step 4 Install required management center patches, geolocation database (GeoDB) updates, vulnerability database (VDB) updates and system software updates to match *FMC2*.

Step 5 Deregister one of the management centers - *FMC2* from the Cisco Smart Software Manager. For more information, see Deregister the Management Center.

Deregistering management center from the Cisco Smart Software Manager removes the Management Center from your virtual account. All license entitlements associated with the management center release back to your virtual account. After deregistration, the management center enters Enforcement mode where no update or changes on licensed features are allowed.

Step 6 Access the web interface of the secondary management center - *FMC2* and break management center high availability. For more information, see Disabling Management Center High Availability, on page 20. When prompted to select an option for handling managed devices, choose **Manage registered devices from this console**.

As a result, licenses that were synced to the secondary management center- *FMC2*, will be removed and you cannot perform deployment activities from *FMC2*.

Step 7 Re-establish management center high availability, by setting up the management center - *FMC2* as the primary and management center - *FMC1* as the secondary. For more information , see Establishing Management Center High Availability, on page 10.

Step 8 Register a Smart License to the primary management center - *FMC2*. For more information see Register the Management Center with the Smart Software Manager.

What to do next

High availability has now been re-established and the primary and the secondary management centers will now work as expected.

Replace a Failed Secondary Management Center (Successful Backup)

Two management centers - *FMC1* and *FMC2* are part of a high availability pair. *FMC1* is the primary and *FMC2* is the secondary. This task describes the steps to replace a failed secondary management center -*FMC2* when data backup from the secondary is successful.

Before you begin

Verify that the data backup from the failed secondary management center is successful.

Procedure

Step 1 Contact Support to request a replacement for a failed management center - *FMC2*.

Step 2 Continue to use the primary management center - *FMC1* as the active management center.

Step 3 Reimage the replacement management center with the same software version as *FMC2*.

Step 4 Restore the data backup from *FMC2* to the new management center.

Step 5 Install required management center patches, geolocation database (GeoDB) updates, vulnerability database (VDB) updates and system software updates to match *FMC1*.

Step 6 Resume data synchronization (if paused) from the web interface of the new management center - *FMC2*, to synchronize the latest configuration from the primary management center - *FMC1*. For more information, see Restarting Communication Between Paired Management Centers, on page 19.

Classic and Smart Licenses work seamlessly.

What to do next

High availability has now been re-established and the primary and the secondary management centers will now work as expected.

Replace a Failed Secondary Management Center (Unsuccessful Backup)

Two management centers - *FMC1* and *FMC2* are part of a high availability pair. *FMC1* is the primary and *FMC2* is the secondary. This task describes the steps to replace a failed secondary management center -*FMC2* when data backup from the secondary is unsuccessful.

Procedure

Step 1 Contact Support to request a replacement for a failed management center - *FMC2*.

Step 2 Continue to use the primary management center - *FMC1* as the active management center.

Step 3 Reimage the replacement management center with the same software version as *FMC2*.

Step 4 Install required management center patches, geolocation database (GeoDB) updates, vulnerability database (VDB) updates and system software updates to match *FMC1*.

Step 5 Access the web interface of the primary management center - *FMC1* and break management center high availability. For more information, see Disabling Management Center High Availability, on page 20. When prompted to select an option for handling managed devices, choose **Manage registered devices from this console**.

Step 6 Re-establish management center high availability, by setting up the management center - *FMC1* as the primary and management center - *FMC2* as the secondary. For more information , see Establishing Management Center High Availability, on page 10.

- When high availability is successfully established, the latest configuration from the primary management center - *FMC1* is synchronized to the secondary management center - *FMC2*.
- Classic and Smart Licenses work seamlessly.

What to do next

High availability has now been re-established and the primary and the secondary management centers will now work as expected.

Management Center High Availability Disaster Recovery

In case of a disaster recovery situation, a manual switchover must be performed. When the primary management center - FMC1 fails, access the web interface of the secondary management center - FMC2 and switch peers. This is applicable conversely also in case the secondary (FMC2) fails. For more information, see Switching Peers in the Management Center High Availability Pair, on page 18.

For restoring a failed management center, refer to Replacing Management Centers in a High Availability Pair, on page 20.

Restoring Management Center in a High Availability Pair (No Hardware Failure)

To restore a management center high availability pair when there is no hardware failure, follow these procedures:

- Restore Backup on the Primary Management Center , on page 25
- Restore Backup on the Secondary Management Center, on page 25

Restore Backup on the Primary Management Center

Before you begin

- There is no hardware failure and replacement of the management center.
- You are familiar with the backup and restore process. See Backup/Restore.

Procedure

Step 1 Verify if backup of the primary management center is available—either a local storage in /var/sf/backup/, or a remote network volume.

Step 2 Pause synchronization on the primary management center. Choose **Integration** > **Other Integrations**, and then go to the **High Availability** tab to pause synchronization.

Step 3 Restore the backup on the primary management center. The management center reboots when the restoration is complete.

Step 4 Once the primary management center is active and its user interface is reachable, resume synchronization on the secondary management center. Choose **Integration** > **Other Integrations**, and then go to the **High Availability** tab to resume synchronization.

Restore Backup on the Secondary Management Center

Before you begin

- There is no hardware failure and replacement of the management center.
- You are familiar with the backup and restore process. See Backup/Restore.

Procedure

Step 1 Verify if backup of the secondary management center is available—either a local storage in /var/sf/backup/, or a remote network volume.

Step 2 Pause synchronization on the primary management center. Choose **Integration** > **Other Integrations**, and then go to the **High Availability** tab to pause synchronization.

Step 3 Restore the backup on the secondary management center. The management center reboots when the restoration is complete.

Step 4 Once the secondary management center is active and its user interface is reachable, resume synchronization on the primary management center. Choose **Integration** > **Other Integrations**, and then go to the **High Availability** tab to resume synchronization.

Unified Backup of Management Centers in High Availability

You can perform a unified backup on an active management center, where a single backup file is created for both the active and standby management centers. The unified backup is applicable only for configuration-only backup. If eventing or TID backup is required, you must take separate backup for active and standby management centers. When you select configuration-only backup, by default, unified backup is applied. In a unified backup, if the active management center is unable to get a backup tar file from the standby management center, the normal backup file is generated for the active unit that can be used for restoration. There are several benefits of unified backup over the normal backup:

- Unified backup does not require you to take separate backups on active and standby management centers.
- Redundant data in backups and storage constraints are removed in a unified backup.
- In a normal backup, when the primary unit fails, and if a secondary unit backup is not available, you had to break the high availability pairing for the secondary RMA. This situation is eradicated in a unified backup.
- Typically, the backup of a standby unit cannot be scheduled. In an unified backup that is scheduled, both active and standby units' backup are taken.
- While executing unified backup, you do not have to pause the HA synchronization to perform backup on the standby unit.

You can use the unified backup to recover a new RMA device if an unanticipated incident occurs. You can identify the unified backup file by its name. A prefix "Unified" is added to the unified backup file name. You can select the management center to restore and also select its State (Active/Standby).

Ensure that you select the appropriate state of the restored management center to prevent Split-Brain conflict.

Restore Management Center from Unified Backup

Use this procedure to restore management center from the unified backup(configuration-only).

Procedure

Step 1 Log into the management center you want to restore.

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

The Backup Management page lists all locally and remotely stored backup files including the unified backup file (configuration-only).

If the unified 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.

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

Step 4 In the **Restore Backup** page, select which unit you want to restore. Because the unified backup stores the backup configuration of both primary and secondary management centers, you need to choose which unit you want to restore.

Step 5 To select the state of the restored management center, click the **Active** or **Standby** radio button. You must verify the role and state of your working management center to avoid having both peers with same role and

state configuration. Choosing the incorrect role and state for your management center when restoring can cause HA failure.

Step 6 Click **Restore**, and then **Confirm Restore** to begin the restoration.

History for Management Center High Availability

Feature	Minimum Management Center	Minimum Threat Defense	Details
Single backup file for high availability management centers.	7.4.1 7.2.6	Any	When performing a configuration-only backup of the active management center in a high availability pair, the system now creates a single backup file which you can use to restore either unit. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.
Support for high availability on KVM.	7.3.0	Any	We now support high availability on management center virtual for KVM.
Support for high availability on AWS and OCI.	7.1.0	Any	We now support high availability on management center virtual for AWS and OCI.
Support for high availability on HyperFlex.	7.0.0	Any	We now support high availability on management center virtual for HyperFlex.
Support for high availability on VMware.	6.7.0	Any	We now support high availability on management center virtual for VMware.
Single sign-on.	6.7.0	Any	When configuring one or both members of a high availability pair for single sign-on, you must take into account special considerations.