High Availability

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

About FMC High Availability

To ensure the continuity of operations, the high availability feature allows you to designate redundant FMCs to manage devices. The FMCs 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 FMC to take over the functionality of a primary FMC if the primary fails. When the primary FMC fails, you must promote the secondary FMC to become the active unit.

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

Note that FMCs 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 FMC, if that appliance fails, you must promote the standby FMC to active.

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

Similarly, when FMC HA synchronization is in degraded state, triggering a switchover or changing roles could make FMC 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 FMCs in a High Availability Pair, on page 18 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 FMC High Availability

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

Roles v. Status in FMC High Availability

Primary/Secondary Roles

When setting up Firepower Management Centers in a high availability pair, you configure one Firepower 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 Firepower Management Center becomes the active peer, while the secondary Firepower 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 Firepower Management Centers in a high availability pair are related to which peer is active and which peer is standby. The active Firepower Management Center remains fully

functional, where you can manage devices and policies. On the standby Firepower Management Center, functionality is hidden; you cannot make any configuration changes.

Event Processing on FMC High Availability Pairs

Since both FMCs 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 FMC fails.

AMP Cloud Connections and Malware Information

Although they share file policies and related configurations, FMCs 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 FMCs, both primary and secondary FMCs must have access to the AMP cloud.

URL Filtering and Security Intelligence

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

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

User Data Processing During FMC Failover

If the primary FMC fails, the Secondary FMC 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 FMC High Availability Pairs

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

If the active FMC 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.

FMC High Availability Disaster Recovery

In case of a disaster recovery situation, a manual switchover must be performed. When the primary FMC - FMC1 fails, access the web interface of the secondary FMC - FMC2 and switch peers. This is applicable conversely also in case the secondary (FMC2) fails. For more information, see Switching Peers in the FMC High Availability Pair, on page 16.

For restoring a failed FMC, refer to Replacing FMCs in a High Availability Pair, on page 18.

Single Sign-On and High Availability Pairs

FMCs 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 FMCs 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 FMC configured for SSO.
- In a high availability pair of FMCs where both are configured to support SSO, before a user can use SSO to access the secondary FMC for the first time, that user must first use SSO to log into the primary FMC at least once.
- When configuring SSO for FMCs in a high availability pair:
  - If you configure SSO on the primary FMC, you are not required to configure SSO on the secondary FMC.
  - If you configure SSO on the secondary FMC, you are required to configure SSO on the primary FMC as well. (This is because SSO users must log in to the primary FMC at least once before logging into the secondary FMC.)

Related Topics

Configure SAML Single Sign-On

FMC High Availability Behavior During a Backup

When you perform a Backup on a FMC high availability pair, the Backup operation pauses synchronization between the peers. During this operation, you may continue using the active FMC, 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.

FMC High Availability Split-Brain

If the active FMC in a high-availability pair goes down (due to power issues, network/connectivity issues), you can promote the standby FMC 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 FMC goes down (or disconnects due to a network failure), you may either break high availability or switch roles. The standby FMC 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 FMC 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 FMC before re-establishing high availability. You may then register the managed devices and import the policies to the intended active FMC.

Troubleshooting FMC High Availability

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

Error	Description	Solution
You must reset your password on the active FMC before you can log in to the standby.	You attempted to log into the standby FMC when a force password reset is enabled for your account.	As the database is read-only for a standby FMC, reset the password on the login page of the active FMC.
500 Internal	May appear when attempting to access the web interface while performing critical FMC 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 FMC reboots (manually or while recovering from a power down) during a high availability or data synchronization operation.	1. Access the FMC shell and use the `manage_hadc.pl` command to access the FMC high availability configuration utility. **Note** Run the utility as a root user, using `sudo`. 2. Pause mirroring operations by using option 5. Reload the FMC web interface. 3. Use the web interface to resume synchronization. Choose **System** (⚙) > **Integration**, 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 FTD, if the FMC IP address and NAT ID are specified, the **Host** field can be left blank. However, in an HA environment with both the FMCs behind a NAT, this error occurs when you add the FTD on the secondary FMC.	1. Delete the FTD from primary FMC. See *Delete a Device from the* FMC in Cisco Firepower Management Center Device Configuration Guide. 2. Remove managers from FTD using the **configure manager delete** command. See Cisco Secure Firewall Threat Defense Command Reference. 3. Add FTD to the FMC with the IP address or name of the FTD device in the **Host** field. See *Add a Device to the* FMC in Cisco Firepower Management Center Device Configuration Guide.
Device Registration Status:Host <*string*> is not reachable	The error occurs when adding FTD device to the secondary FMC center in a high-availability deployment where both the secondary FMC and the FTD device are behind NAT.	On the standby FMC 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 FTD. OR 1. Access the FTD shell and use the `show managers` command to get the standby FMC entry identifier value. 2. In the FTD shell, edit the standby FMC 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 FMC High Availability, on page 15.

Requirements for FMC 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 FMC 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 FMC 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.
- Ensure that both FMCs 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 FMC 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
- VMware vSphere/VMware ESXi

The FMCs must have the same device management capacity (not supported on FMCv2) and be identically licensed. You also need one FTD entitlement for each managed device. For more information, see License Requirements for FMC 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 FMCs in a high availability configuration must have the same major (first number), minor (second number), and maintenance (third number) software version.
- The two FMCs in a high availability configuration must have the same version of the intrusion rule update installed.
- The two FMCs in a high availability configuration must have the same version of the vulnerability database update installed.
- The two FMCs 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 FMCs, you cannot establish high availability.

License Requirements for FMC High Availability Configurations

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

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

Only the active FMC 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 FMC and assign them to the newly-active FMC.

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

Hardware FMC

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

FMCv

You will need two identically licensed FMCvs.

Example: For the FMCv high availability pair managing 10 devices, you can use:

- Two (2) FMCv 10 entitlements
- 10 device licenses

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

Prerequisites for FMC High Availability

Before establishing the FMC high availability pair:

- Export required policies from the intended secondary FMC to the intended primary FMC. For more information, see Export Configurations.
- Make sure that the intended secondary FMC does not have any devices added to it. Delete devices from the intended secondary FMC and register these devices to the intended primary FMC. For more information see *Delete a Device from the FMC* and *Add a Device to the FMC* in the Firepower Management Center Device Configuration Guide.
- Import the policies into the intended primary FMC. For more information, see Import Configurations.
- On the intended primary FMC, verify the imported policies, edit them as needed and deploy them to the appropriate device. For more information, see *Deploy Configuration Changes* in the Firepower Management Center Device Configuration Guide.
- On the intended primary FMC, 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 FMC High Availability, on page 9.

Establishing FMC 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 FMC, which need to be synced to the standby FMC. You can view the High Availability page to check the status of the high availability peers.

Before you begin

- Confirm that both the FMCs adhere to the high availability system requirements. For more information , see Requirements for FMC High Availability, on page 6.
- Confirm that you completed the prerequisites for establishing high availability. For more information, see Prerequisites for FMC 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 FMC that you want to designate as the secondary.

Step 2 Choose **System** (⚙) > **Integration**, and then choose **High Availability**.

Step 3 Under Role for this FMC, choose **Secondary**.

Step 4 Enter the hostname or IP address of the primary FMC in the **Primary Firepower Management Center Host** text box.

You can leave this empty if the primary FMC does not have an IP address reachable from the peer FMC (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 FMC to enable HA connection.

Step 5 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 FMCs.

Step 6 If you did not specify the primary IP address, or if you do not plan to specify the secondary IP address on the primary FMC, then in the **Unique NAT ID** field, enter a unique alphanumeric ID. See NAT Environments for more information.

Step 7 Click **Register**.

Step 8 Using an account with Admin access, log into the FMC that you want to designate as the primary.

Step 9 Choose **System** (⚙) > **Integration**, and then choose **High Availability**.

Step 10 Under Role for this FMC, choose **Primary**.

Step 11 Enter the hostname or IP address of the secondary FMC in the **Secondary Firepower Management Center Host** text box.

You can leave this empty if the secondary FMC does not have an IP address reachable from the peer FMC (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 FMC to enable HA connection.

Step 12 Enter the same one-time-use registration key in the **Registration Key** text box you used in step 6.

Step 13 If required, enter the same NAT ID that you used in step 7 in the **Unique NAT ID** text box.

Step 14 Click **Register**.

What to do next

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

Note When a registered device has a NAT IP address, automatic device registration fails and the secondary FMC High Availability page lists the device as local, pending. You can then assign a different NAT IP address to the device on the standby FMC High Availability page. If automatic registration otherwise fails on the standby FMC, but the device appears to be registered to the active Firepower Management Center, see Using CLI to Resolve Device Registration in FMC High Availability, on page 15.

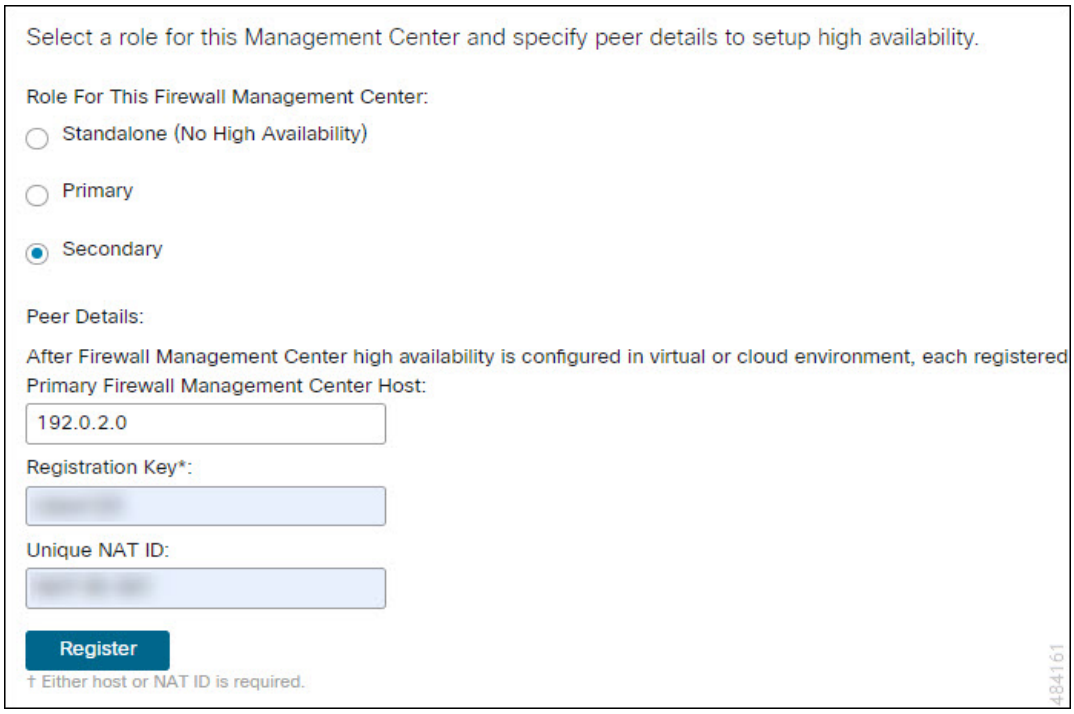
High Availability for FMCs Hosted on Public Cloud

While establishing high availability between FMCs hosted on public clouds, the combinations of IP addresses or hostnames for the primary and secondary FMCs described below can successfully form high availability and get the devices registered on both the peers. In the **High Availability** page (**Integration** > **Other**

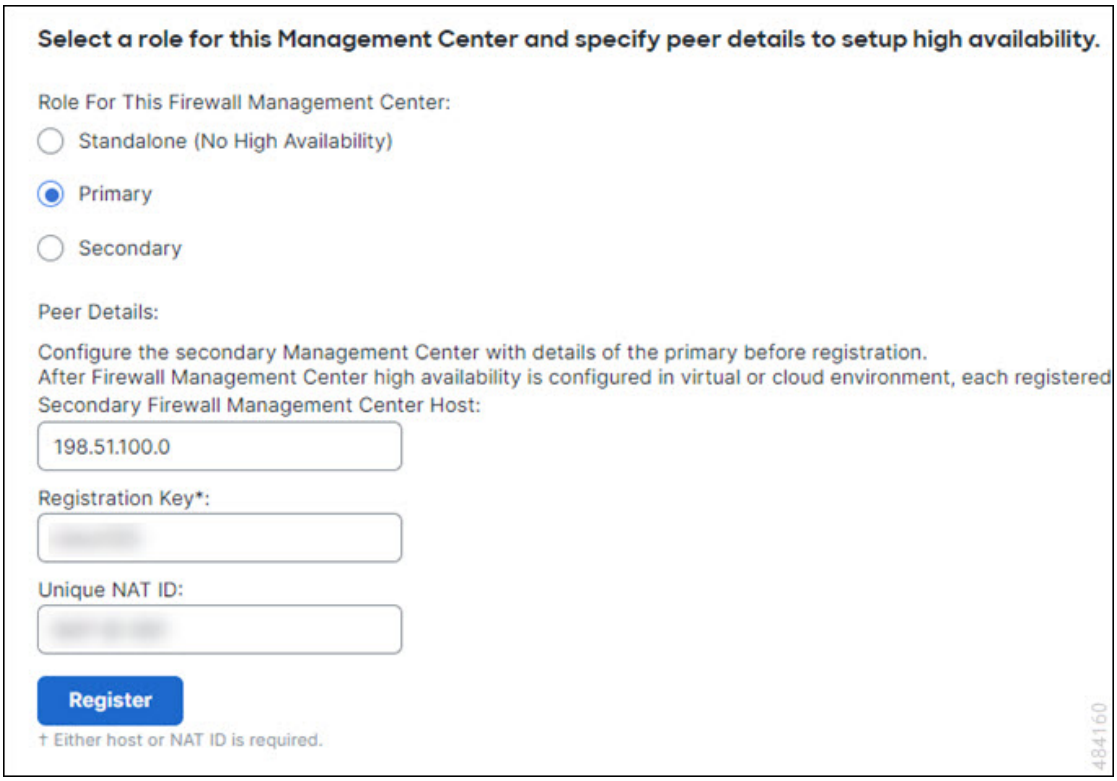
Integrations > **High Availability**), perform one of the following configurations to successfully form high availability between FMCs hosted in public cloud.

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

1. On the secondary FMC, 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 FMC 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 FMC.

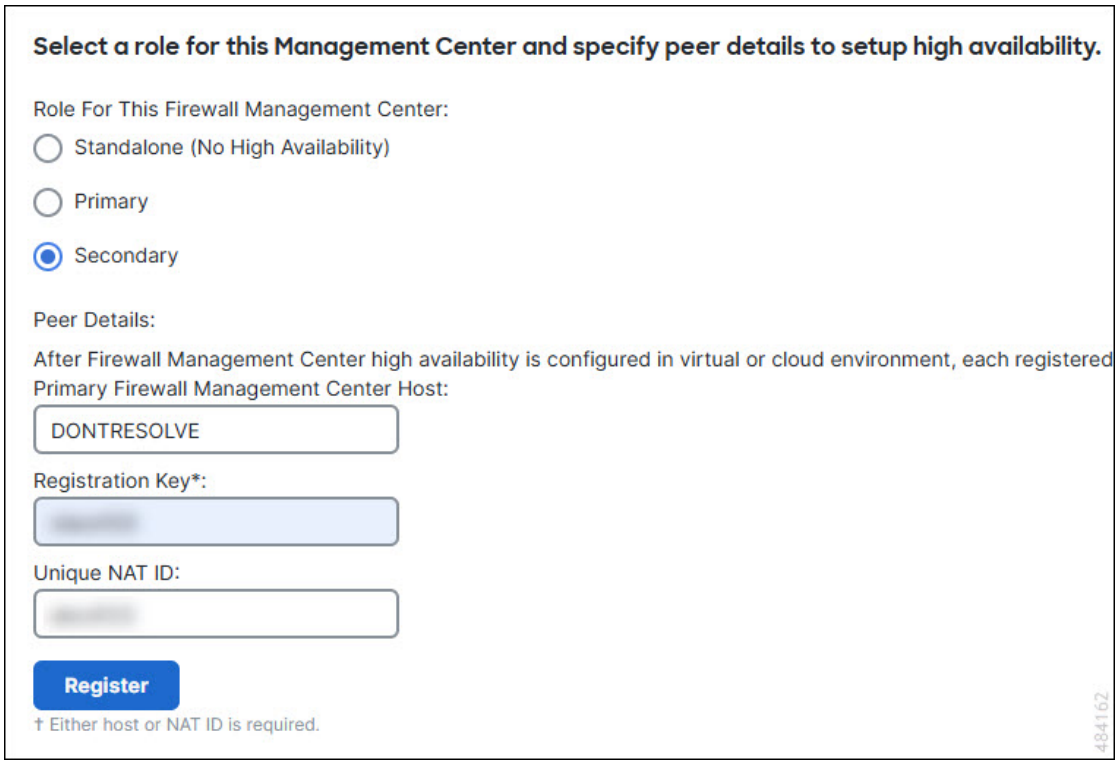


2. On the primary FMC, do the following:
   a. Choose **Primary** as the **Role for this Firewall Management Center**.
   b. Enter the public IP address or hostname for the secondary FMC in the **Secondary Firewall Management Center Host** field.
   c. Enter the registration key.
   d. Enter the unique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

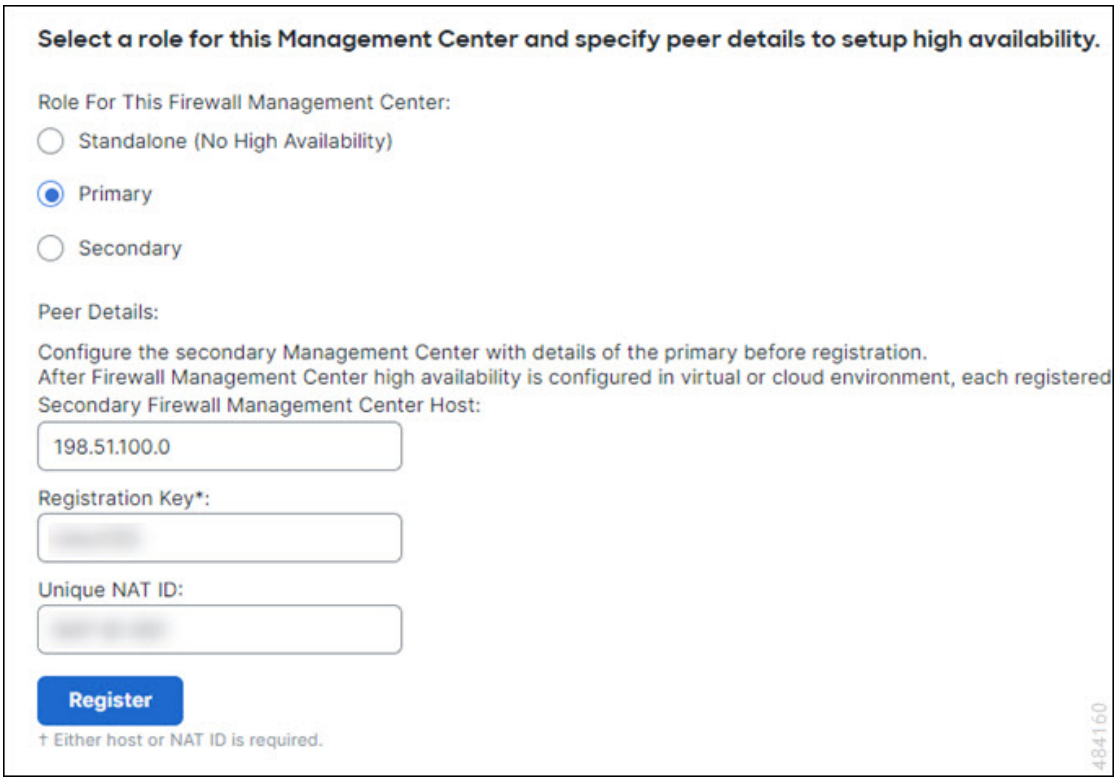


Using the Public IP Address or Hostname for the Secondary FMC

1. On the secondary FMC, 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 FMC.



2. On the primary FMC, 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 FMC in the **Secondary Firewall Management Center Host** field.
   c. Enter the registration key.
   d. Enter the unique NAT ID.



Viewing FMC High Availability Status

After you identify your active and standby FMCs, you can view information about the local FMC 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 FMCs that you paired using high availability.

Step 2 Choose **System** (⚙) > **Integration**, and then choose **High Availability** .

Configurations Synced on FMC High Availability Pairs

When you establish high availability between two FMCs, 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 FMCs. For more information on remediation settings, see Managing Remediation Modules.

Configuring External Access to the FMC 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 FMCs, see Enabling External Access to the Database .

Using CLI to Resolve Device Registration in FMC High Availability

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

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

Procedure

Step 1 Delete the device from the active FMC. See *Delete (Unregister) a Device from the FMC* 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 FMC:

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 FMC.

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

This command configures the device to initiate a connection to a FMC.

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

d. Log in to the active FMC and register the device.

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

a. Access the FTD shell and use the `show managers` command to get the standby FMC entry identifier value.

b. In the FTD shell, edit the standby FMC 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 FMC High Availability Pair

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

Procedure

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

Step 2 Choose **System** (⚙) > **Integration**, and then choose **High Availability**.

Step 3 Choose **Switch Peer Roles** to change the local role from Active to Standby, or Standby to Active. This switches the active and standby roles between the two peers, while the Primary and Secondary designations remain unchanged. Note that *role* here refers to the active or standby status of the management center in the HA deployment, not the primary or secondary designation assigned during HA setup.

Pausing Communication Between Paired FMCs

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

Procedure

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

Step 2 Choose **System** (⚙) > **Integration**, and then choose **High Availability**.

Step 3 Choose **Pause Synchronization**.

Restarting Communication Between Paired FMCs

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

Procedure

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

Step 2 Choose **System** (⚙) > **Integration**, and then choose **High Availability**.

Step 3 Choose **Resume Synchronization**.

Change the IP Address of the FMC 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 FMC is also updated, you must manually change the IP address.

Procedure

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

Step 2 Choose **System** (⚙) > **Integration**.

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 FMC High Availability

Procedure

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

Step 2 Choose **System** (⚙) > **Integration**, and then choose **High Availability**.

Step 3 Choose **Break High Availability**.

Step 4 Choose one of the following options for handling managed devices:

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

Note

- If you choose to manage the registered devices from the secondary FMC, the devices will be unregistered from the primary FMC. The devices are now registered to be managed by the secondary FMC. 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 FMC. For more information see Assign Licenses to Devices.
- The standby management center retains the access control policies after the HA break is complete.

Step 5 Click **OK**.

Replacing FMCs in a High Availability Pair

If you need to replace a failed unit in the FMC 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 FMC failed	Data backup successful	Replace a Failed Primary FMC (Successful Backup), on page 19
	Data backup not successful	Replace a Failed Primary FMC (Unsuccessful Backup), on page 20
Secondary FMC failed	Data backup successful	Replace a Failed Secondary FMC (Successful Backup), on page 21
	Data backup not successful	Replace a Failed Secondary FMC (Unsuccessful Backup), on page 21

Replace a Failed Primary FMC (Successful Backup)

Two FMCs, *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 FMC, *FMC1*, when data backup from the primary is successful.

Before you begin

Verify that the data backup from the failed primary FMC is successful.

Procedure

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

Step 2 When the primary FMC - *FMC1* fails, access the web interface of the secondary FMC - *FMC2* and switch peers. For more information, see Switching Peers in the FMC High Availability Pair, on page 16.

This promotes the secondary FMC - *FMC2* to active.

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

Caution
Do not break FMC 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 FMC with the same software version as *FMC1*.

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

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

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

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

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

Step 7 When the configuration syncs successfully, access the web interface of the secondary FMC - *FMC2* and switch roles to make the primary FMC - *FMC1* active. For more information, see Switching Peers in the FMC High Availability Pair, on page 16.

What to do next

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

Replace a Failed Primary FMC (Unsuccessful Backup)

Two FMCs - *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 FMC -*FMC1* when data backup from the primary is unsuccessful.

Procedure

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

Step 2 When the primary FMC - *FMC1* fails, access the web interface of the secondary FMC - *FMC2* and switch peers. For more information, see Switching Peers in the FMC High Availability Pair, on page 16.

This promotes the secondary FMC - *FMC2* to active.

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

Caution
Do not break FMC 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 FMC with the same software version as *FMC1*.

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

Step 5 Deregister one of the FMCs - *FMC2* from the Cisco Smart Software Manager. For more information, see Deregister the FMC.

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

Step 6 Access the web interface of the secondary FMC - *FMC2* and break FMC high availability. For more information, see Disabling FMC High Availability, on page 18. 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 FMC- *FMC2*, will be removed and you cannot perform deployment activities from *FMC2*.

Step 7 Re-establish FMC high availability, by setting up the FMC - *FMC2* as the primary and FMC - *FMC1* as the secondary. For more information , see Establishing FMC High Availability, on page 9.

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

What to do next

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

Replace a Failed Secondary FMC (Successful Backup)

Two FMCs - *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 FMC -*FMC2* when data backup from the secondary is successful.

Before you begin

Verify that the data backup from the failed secondary FMC is successful.

Procedure

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

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

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

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

Step 5 Install required FMC 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 FMC - *FMC2*, to synchronize the latest configuration from the primary FMC - *FMC1*. For more information, see Restarting Communication Between Paired FMCs, on page 17.

Classic and Smart Licenses work seamlessly.

What to do next

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

Replace a Failed Secondary FMC (Unsuccessful Backup)

Two FMCs - *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 FMC -*FMC2* when data backup from the secondary is unsuccessful.

Procedure

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

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

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

Step 4 Install required FMC 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 FMC - *FMC1* and break FMC high availability. For more information, see Disabling FMC High Availability, on page 18. When prompted to select an option for handling managed devices, choose **Manage registered devices from this console**.

Step 6 Re-establish FMC high availability, by setting up the FMC - *FMC1* as the primary and FMC - *FMC2* as the secondary. For more information , see Establishing FMC High Availability, on page 9.

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

What to do next

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

FMC High Availability Disaster Recovery

In case of a disaster recovery situation, a manual switchover must be performed. When the primary FMC - FMC1 fails, access the web interface of the secondary FMC - FMC2 and switch peers. This is applicable conversely also in case the secondary (FMC2) fails. For more information, see Switching Peers in the FMC High Availability Pair, on page 16.

For restoring a failed FMC, refer to Replacing FMCs in a High Availability Pair, on page 18.

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

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

- Restore Backup on the Primary Management Center , on page 23
- Restore Backup on the Secondary Management Center, on page 23

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 FMC is available—either a local storage in /var/sf/backup/, or a remote network volume.

Step 2 Pause synchronization on the primary FMC. Choose **System** (⚙) > **Integration**, and then choose **High Availability** tab to pause synchronization.

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

Step 4 Once the primary FMC is active and its user interface is reachable, resume synchronization on the secondary FMC. Choose **System** (⚙) > **Integration**, and then choose **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 FMC is available—either a local storage in /var/sf/backup/, or a remote network volume.

Step 2 Pause synchronization on the primary FMC. Choose **System** (⚙) > **Integration**, and then choose**High Availability** tab to pause synchronization.

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

Step 4 Once the secondary FMC is active and its user interface is reachable, resume synchronization on the primary FMC. Choose **System** (⚙) > **Integration**, and then choose **High Availability** tab to resume synchronization.

History for FMC High Availability

Feature	Minimum FMC	Minimum FTD	Details
Support for high availability on AWS and OCI.	7.1.0	Any	We now support high availability on FMCv for AWS and OCI.
Support for high availability on HyperFlex.	7.0.0	Any	We now support high availability on FMCv for HyperFlex.
Support for high availability on VMware.	6.7.0	Any	We now support high availability on FMCv 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.