

# Configurer la haute disponibilité sur FMC

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Avant de commencer](#)

[Configurer](#)

[Configuration du FMC secondaire](#)

[Configuration du FMC principal](#)

[Vérification](#)

---

## Introduction

Ce document décrit un exemple de configuration de haute disponibilité (HA) sur un centre de gestion des pare-feu (FMC).

## Conditions préalables

### Exigences

Aucune exigence spécifique n'est associée à ce document.

### Composants utilisés

Les informations contenues dans ce document sont basées sur Secure FMC pour VMware v7.2.5.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales

Les exigences spécifiques de ce document sont les suivantes :

- Les deux homologues FMC doivent être sur la même version logicielle, la même mise à jour de règle d'intrusion, la même base de données de vulnérabilité et le même package de sécurité léger
- Les deux homologues FMC doivent avoir la même capacité ou la même version matérielle
- Les deux FMC nécessitent une licence distincte

Pour connaître l'ensemble des conditions requises, vous pouvez consulter le [Guide d'administration](#).

---



Avertissement : En cas de non-correspondance dans les exigences répertoriées, vous ne pouvez pas configurer la haute disponibilité.

---

Cette procédure est prise en charge sur toutes les appliances matérielles.

## Avant de commencer

- Garantir un accès administrateur aux deux FMC
- Assurer la connectivité entre les interfaces de gestion
- Prenez le temps de vérifier les versions logicielles et assurez-vous que toutes les mises à niveau nécessaires sont effectuées

## Configurer

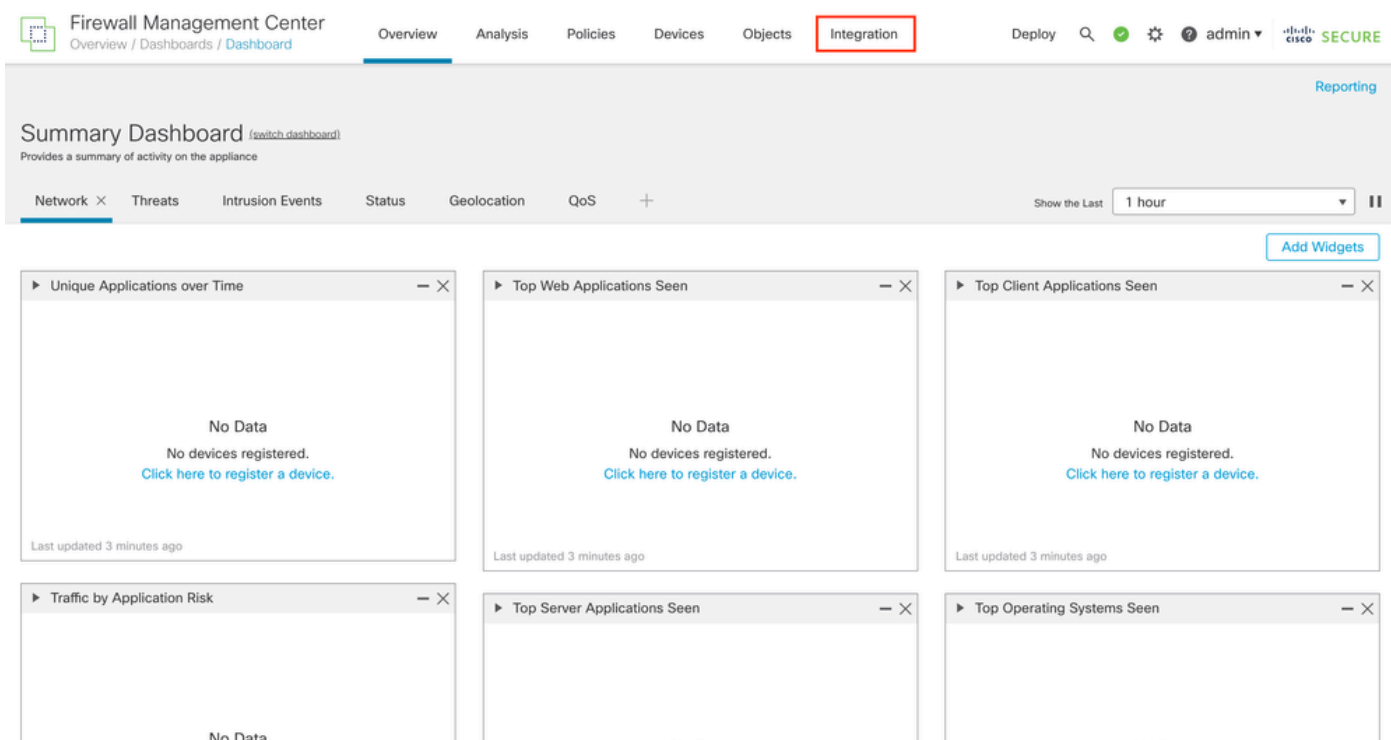
## Configuration du FMC secondaire

Étape 1. Connectez-vous à l'interface utilisateur graphique (GUI) du périphérique du FMC qui va jouer le rôle de secondaire/veille.



Se connecter à FMC

Étape 2. Accédez à l'onglet Intégration.



Accéder à l'intégration

Étape 3. Cliquez sur Autres intégrations.

## SecureX

## Security Analytics &amp; Logging

## Other Integrations

## AMP

## AMP Management

## Dynamic Analysis Connections

## Intelligence

## Incidents

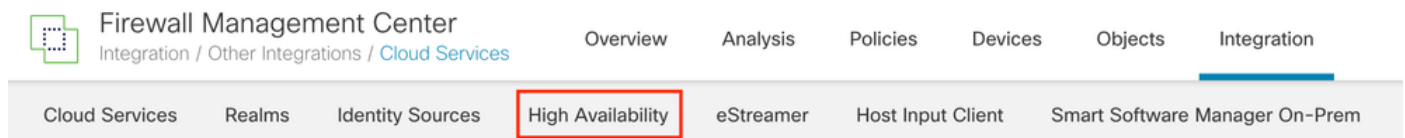
## Sources

## Elements

## Settings

Accédez à Autre intégration

#### Étape 4. Accédez à l'onglet Haute disponibilité.



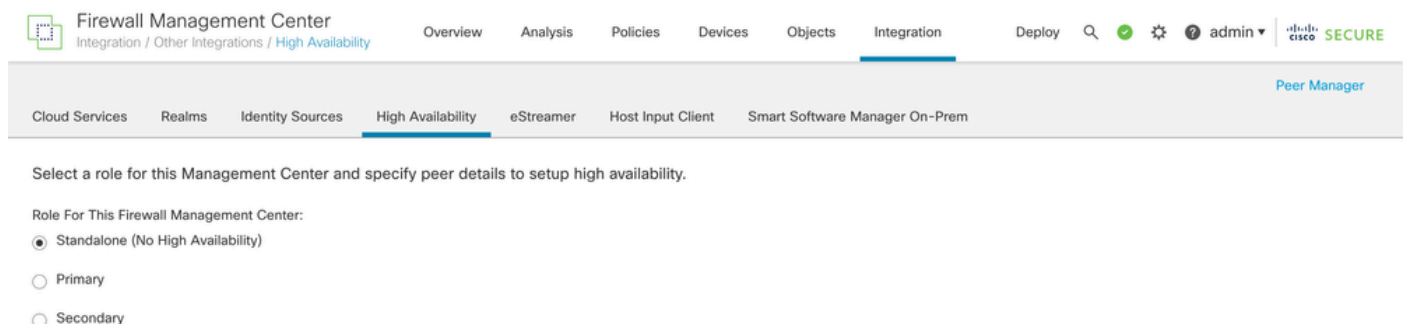
Firewall Management Center  
Integration / Other Integrations / Cloud Services

Overview Analysis Policies Devices Objects Integration

Cloud Services Realms Identity Sources **High Availability** eStreamer Host Input Client Smart Software Manager On-Prem

Accédez à Haute disponibilité

#### Étape 5. Cliquez sur Secondaire.



Firewall Management Center  
Integration / Other Integrations / High Availability

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ✔️ ⚙️ ❓ admin ▼ cisco SECURE

Cloud Services Realms Identity Sources **High Availability** eStreamer Host Input Client Smart Software Manager On-Prem Peer Manager

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Entrez les informations et sélectionnez le rôle souhaité pour le FMC actuel.

#### Étape 6. Entrez les informations relatives à l'homologue principal/actif et cliquez sur Register.

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

- Standalone (No High Availability)
- Primary
- Secondary

Peer Details:

After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Primary Firewall Management Center Host:

Registration Key\*:

Unique NAT ID:

**Register**

† Either host or NAT ID is required.

Remarque : Prenez note de la clé d'enregistrement, car elle sera utilisée sur le FMC actif.

Étape 7. Cet avertissement vous demande de confirmer, cliquez sur **Yes**.

## Warning

This operation may affect critical processes running in the background. Do you want to continue?

No

Yes



Remarque : Assurez-vous qu'aucune autre tâche n'est en cours d'exécution car pendant la création de HA, l'interface utilisateur redémarre.

---

Étape 8. Confirmez que vous souhaitez enregistrer l'homologue principal.

## Warning

---

Do you want to register primary peer:  
10.18.19.31?

No

Yes







Avertissement : Toutes les informations sur les périphériques/la stratégie/la configuration vont être supprimées du FMC secondaire une fois que la haute disponibilité aura été créée.

Étape 9. Vérifiez que l'état du contrôleur FMC secondaire est en attente.

Firewall Management Center  
Integration / Other Integrations / Peer Manager

Overview Analysis Policies Devices Objects Integration Deploy 🔍 🟢 ⚙️ 👤 admin ▾ 🔒 cisco SECURE

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Host	Last Modified	Status	State	
10.18.19.31	2023-09-28 13:53:56	Pending Registration	<input checked="" type="checkbox"/>	 

## Configuration du FMC principal

Répétez les étapes 1 à 4 sur le FMC principal/actif.

## Étape 5. Cliquez sur Principal.

Firewall Management Center  
Integration / Other Integrations / High Availability

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ⓘ admin ▾ Cisco SECURE

Peer Manager

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

Standalone (No High Availability)

Primary

Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.  
After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Secondary Firewall Management Center Host:

Registration Key\*:

Unique NAT ID:

Register

† Either host or NAT ID is required.

## Étape 6. Entrez les informations relatives à Secondary FMC et cliquez sur Register.

Peer Manager

Cloud Services Realms Identity Sources High Availability eStreamer Host Input Client Smart Software Manager On-Prem

Select a role for this Management Center and specify peer details to setup high availability.

Role For This Firewall Management Center:

Standalone (No High Availability)

Primary

Secondary

Peer Details:

Configure the secondary Management Center with details of the primary before registration.  
After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license.

Secondary Firewall Management Center Host:

Registration Key\*:

Unique NAT ID:

Register

† Either host or NAT ID is required.



Remarque : Utilisez la même clé d'enregistrement que le contrôleur FMC secondaire.

---

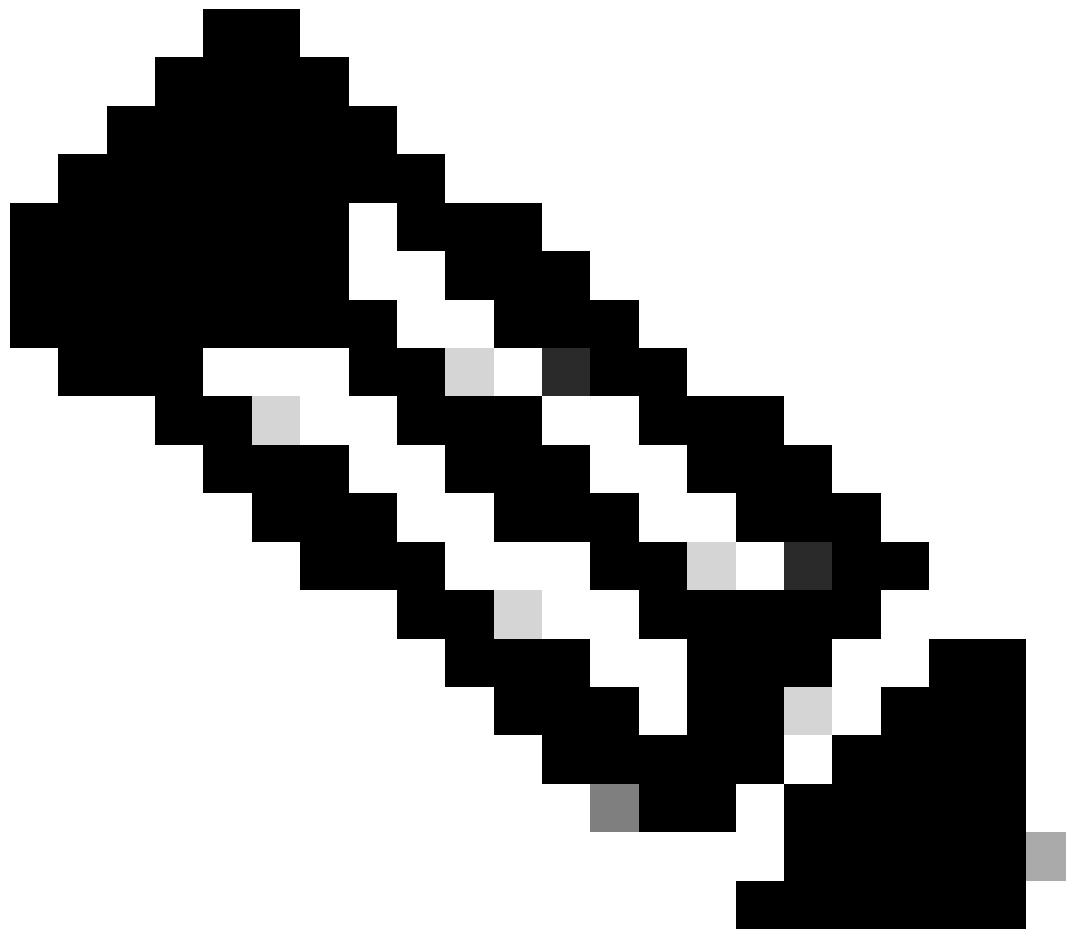
Étape 7. Cet avertissement vous demande de confirmer, cliquez sur **Yes**.

## Warning

This operation may affect critical processes running in the background. Do you want to continue?

No

Yes



---

Remarque : Vérifiez qu'aucune autre tâche n'est en cours d'exécution.

---

Étape 8. Confirmez que vous souhaitez vous inscrire au FMC secondaire.

## Warning

Secondary peer configuration and policies will be removed. After Firewall Management Center high availability is configured in virtual or cloud environment, each registered Firewall Threat Defense consumes an additional Firepower MCv Device license. Do you want to register secondary peer:  
10.18.19.32?

No

Yes



Remarque : Assurez-vous qu'il n'y a aucune information critique sur le FMC secondaire, car accepter cette invite supprime toutes les configurations du FMC.

---

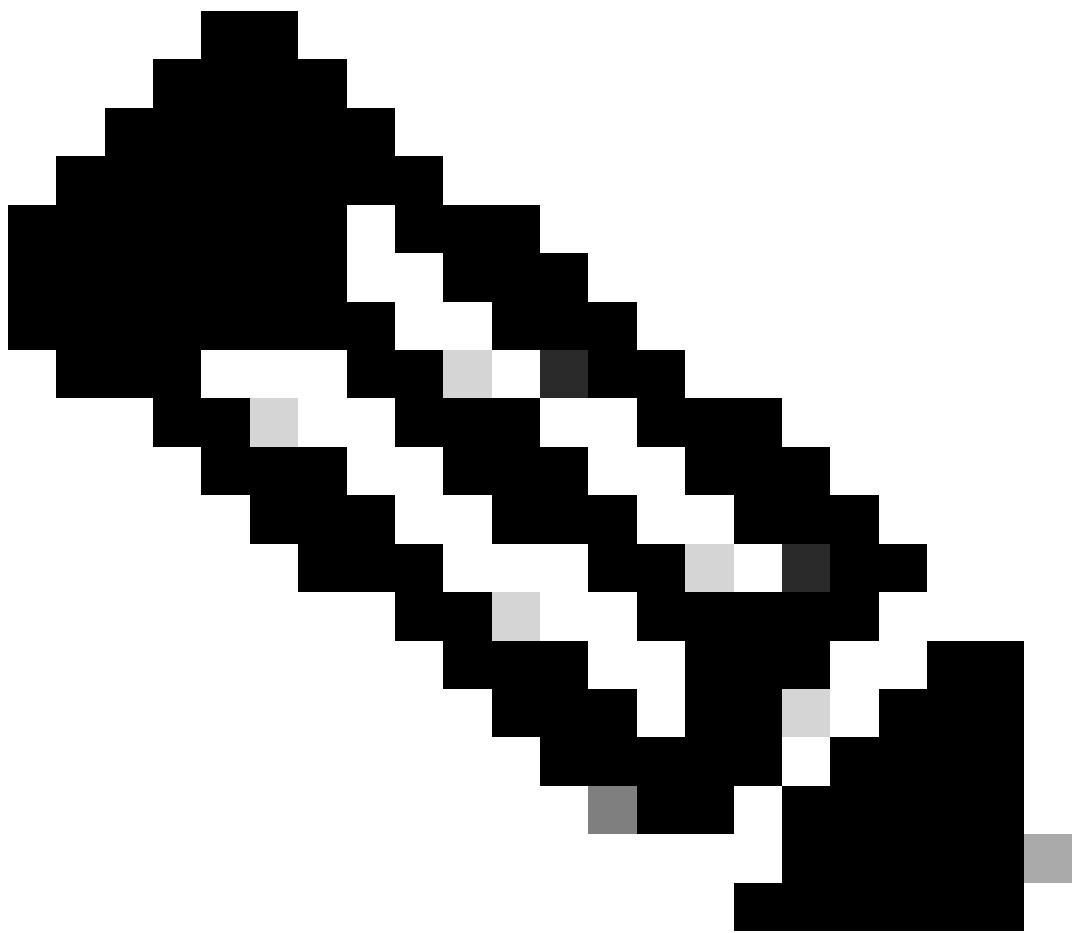
La synchronisation entre le principal et le secondaire commence ; la durée dépend de la configuration et des périphériques. Ce processus peut être surveillé à partir des deux unités.

[Switch Peer Roles](#) [Break HA](#) [Pause Synchronization](#)

High availability operations are in progress. The status messages and alerts on this page are temporary. Please check after high availability operations are complete. These operations include file copy which may take time to complete. Database files synchronization: 100% of 379MB transferred

Summary	
Status	▲ Temporarily degraded- high availability operations are in progress.
Synchronization	▲ Failed
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	<b>Active - Primary</b> (10.18.19.31)	<b>Standby - Secondary</b> (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware



Remarque : Pendant la synchronisation, attendez-vous à voir l'état Failed et Temporary degraded. Cet état s'affiche jusqu'à ce que le processus soit terminé.

# Vérification

Une fois la synchronisation terminée, le résultat attendu est Status Healthy et Synchronization OK.

Firewall Management Center  
Integration / Other Integrations / High Availability

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ⓘ admin | cisco SECURE

Cloud Services Realms Identity Sources **High Availability** eStreamer Host Input Client Smart Software Manager On-Prem Peer Manager

Switch Peer Roles Break HA Pause Synchronization

Summary	
Status	Healthy
Synchronization	OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	<b>Active - Primary</b> (10.18.19.31)	<b>Standby - Secondary</b> (10.18.19.32)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Le principal et le secondaire continuent de se synchroniser ; this is normal.

Firewall Management Center  
Integration / Other Integrations / High Availability

Devices Integration 🔍 ⚙️ ⓘ admin | cisco SECURE

Cloud Services **High Availability** eStreamer Host Input Client Peer Manager

Switch Peer Roles Break HA Pause Synchronization

Summary	
Status	Synchronization task is in progress
Synchronization	OK
Active System	10.18.19.31
Standby System	10.18.19.32

System Status		
	Local	Remote
	<b>Standby - Secondary</b> (10.18.19.32)	<b>Active - Primary</b> (10.18.19.31)
Operating System	7.2.5	7.2.5
Software Version	7.2.5-208	7.2.5-208
Model	Secure Firewall Management Center for VMware	Secure Firewall Management Center for VMware

Prenez quelques instants pour vérifier que vos périphériques s'affichent correctement sur le principal et le secondaire.



À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.