

Déployer la machine virtuelle FDM depuis Azure Marketplace à l'aide du modèle

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Déployer FDM à partir d'un modèle sur Azure Portal](#)

[Vérifier la configuration de la VM](#)

[Vérifier la VM déployée sur Azure](#)

[Configuration de base pour FDM](#)

Introduction

Ce document décrit le déploiement de Cisco Secure Firewall Threat Defense Virtual (FDM) sur une machine virtuelle à l'aide d'Azure Marketplace et de modèles.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)
- Compte/accès Azure

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Versions virtuelles de Cisco Secure Firewall Threat Defense : 7.4.1, 7.3.1, 7.2.7, 7.1.0, 7.0.6 et 6.4.0

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.

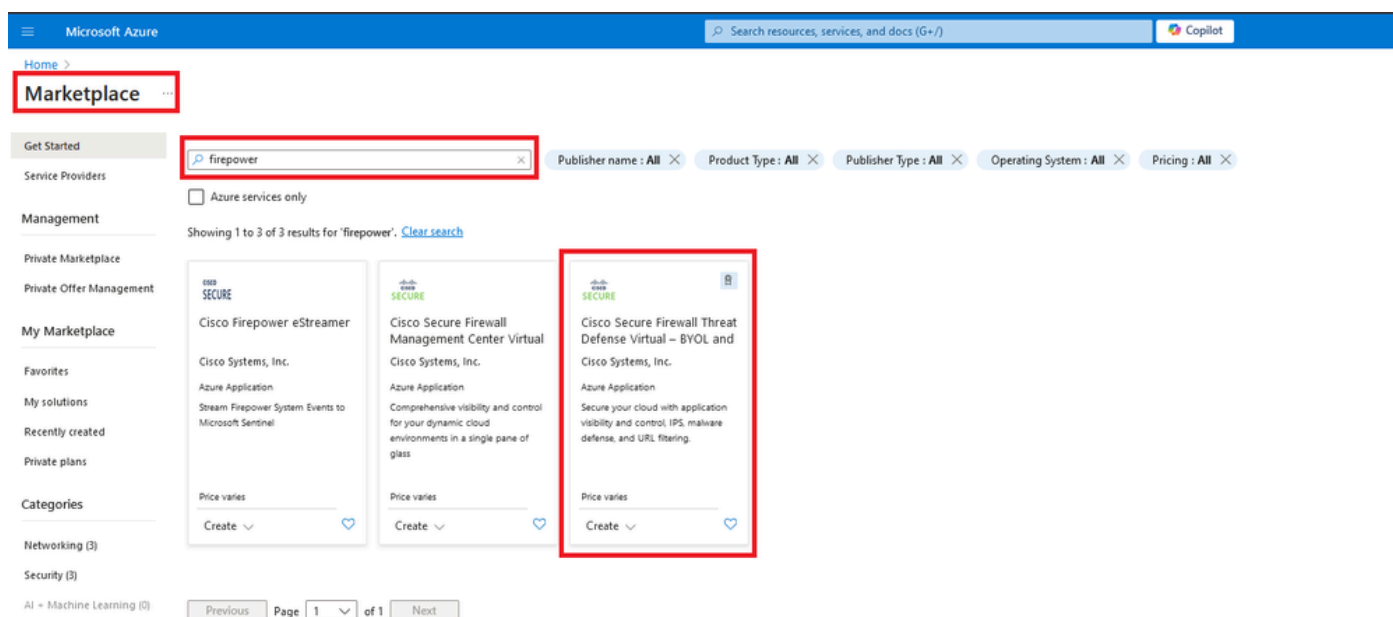
Configurer

Les clients ont rencontré des problèmes lors de la tentative de déploiement d'un Firepower Device Manager (FDM) sur une machine virtuelle à partir d'Azure, en particulier lors de l'utilisation d'Azure Marketplace et des modèles.

Déployer FDM à partir d'un modèle sur Azure Portal

Pour déployer le FDM à partir du portail Azure, procédez comme suit :

1. Accédez au portail Azure et localisez le Marketplace dans Azure Services. Recherchez et sélectionnez Cisco Secure Firewall Threat Defense Virtual - BYOL et PAYG.



Recherchez Firepower et sélectionnez Cisco Secure Firewall Threat Defense Virtual - BOYL

2. Cliquez sur Créer pour démarrer le processus de configuration du FTD.

Home > Marketplace >

Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG 🔗 ⋮

Cisco Systems, Inc.



Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG ♥ Add to Favorites

Cisco Systems, Inc. | Azure Application

★ 4.0 (2 ratings)

Microsoft preferred solution

Plan

Cisco Secure Firewall Threat Defense...

Create

- Leverage Azure Traffic Manager for highly scalable remote access VPN
- Integrate with Azure Transit VNet for scalable inter-VNet traffic

Cisco Talos® Threat Intelligence is included, protecting against known and unknown threats from one of the world's largest commercial threat intelligence teams.

[Learn more](#)

*Forrester Total Economic Impact of Cisco Secure Firewall, 2022. www.cisco.com/go/firewallTEI

More products from Cisco Systems, Inc. [See All](#)

<p>Cisco Meraki vMX</p> <p>Cisco Systems, Inc.</p> <p>Azure Application</p> <p>A Cisco Meraki Virtual MX to connect your Meraki network to your Azure deployments</p> <p>Starts at Free</p> <p>Create ♥</p>	<p>Cisco Catalyst 8000V Edge Software (PAYG)</p> <p>Cisco Systems, Inc.</p> <p>Virtual Machine</p> <p>Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud.</p> <p>Starts at \$2.53/hour</p> <p>Create ♥</p>	<p>Cisco Catalyst 8000V Edge Software - Solution</p> <p>Cisco Systems, Inc.</p> <p>Azure Application</p> <p>Deploy and manage enterprise-class networking services and VPN technologies for the Azure cloud.</p> <p>Price varies</p> <p>Create ♥</p>	<p>Cisco Nexus Dashboard</p> <p>Cisco Systems, Inc.</p> <p>Azure Application</p> <p>Simplified, centralized data center dashboard makes it easier to manage your hybrid cloud network</p> <p>Price varies</p> <p>Create ♥</p>
--	--	--	---

Créer une machine virtuelle à partir du portail Azure

3. Dans la page de configuration de base, créez un groupe de ressources pour le périphérique, choisissez la région et sélectionnez un nom pour la machine virtuelle.

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG ...

Basics Cisco FTDv settings Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ

Instance details

Region * ⓘ

Virtual Machine name * ⓘ

Licensing ⓘ

Software Version ⓘ

A resource group is a container that holds related resources for an Azure solution.

Name *

Créer un nouveau groupe de ressources

4. Choisissez la version souhaitée pour le déploiement de la VM dans les options disponibles.

Software Version ⓘ

Availability Option * ⓘ

Username for primary account (not the FTDv admin user account) * ⓘ

Authentication type * ⓘ

- 7.4.1-172
- 7.3.1-19
- 7.2.7-500
- 7.1.0-92
- 7.0.6-236
- 6.4.0-110

Versions disponibles pour un déploiement sur Azure Market

5. Configurez un nom d'utilisateur pour le compte principal, choisissez Mot de passe comme type d'authentification, et définissez le Mot de passe pour l'accès à la VM et le Mot de passe Admin.

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

Basics Cisco FTDv settings Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Region * ⓘ

Virtual Machine name * ⓘ

Licensing ⓘ

Software Version ⓘ

Availability Option * ⓘ None Availability Zone

Username for primary account (not the FTDv admin user account) * ⓘ

Authentication type * ⓘ Password SSH Public Key

Password * ⓘ

Confirm password *

Admin Password * ⓘ

Confirm Admin Password * ⓘ

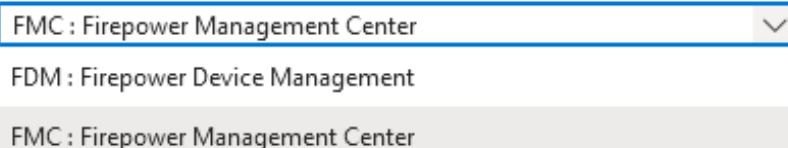
FTDv Management * ⓘ

Nom d'utilisateur et mots de passe Admin.

6. Pour le type de gestion, sélectionnez FDM pour l'objectif de ce document.

FTDv Management * ⓘ

Enter FMC registration information * ⓘ



A dropdown menu with a blue border and a downward arrow on the right. The menu is open, showing three options: 'FMC : Firepower Management Center' (highlighted in light gray), 'FDM : Firepower Device Management', and 'FMC : Firepower Management Center'.

Périphérique de gestion

7. Dans l'onglet Paramètres FTDv de Cisco, vérifiez la taille de la VM, le compte de stockage, l'adresse IP publique et l'étiquette DNS, qui sont créés par défaut après avoir terminé la configuration de base.

Vérifiez que les paramètres Virtual Network, Management subnet et autres paramètres Ethernet sont corrects.

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG ...

Basics Cisco FTDv settings Review + create

Virtual machine size * ⓘ

1x Standard D3 v2
4 vcpus, 14 GB memory
[Change size](#)

Storage account * ⓘ

(new) [redacted]8b089e65
[Create New](#)

Public IP address ⓘ

(new) [redacted]-pip
[Create new](#)

DNS label ⓘ

[redacted]:352e65c ✓

.eastus.cloudapp.azure.com

Attach diagnostic interface * ⓘ

No
 Yes

Virtual network ⓘ

(New) vnet01 [redacted]FDM [redacted]
[Edit virtual network](#)

Management subnet * ⓘ

(New) subnet1
[Edit subnet](#) 172.18.0.0 - 172.18.0.255 (256 addresses)

GigabitEthernet 0/0 subnet * ⓘ

(New) subnet2
[Edit subnet](#) 172.18.1.0 - 172.18.1.255 (256 addresses)

GigabitEthernet 0/1 subnet * ⓘ

(New) subnet3
[Edit subnet](#) 172.18.2.0 - 172.18.2.255 (256 addresses)

Public inbound ports (mgmt. interface) * ⓘ

None
 Allow selected ports

i All traffic from the Internet will be blocked by default. You will be able to change inbound port rules in the VM Networking page later.

Paramètres FTDv de Cisco.

8. Sélectionnez Allow selected Port pour activer les ports SSH (22), SFTunnel (8305) et HTTPS (443) pour l'accès HTTPS à la machine virtuelle et le port SFTunnel pour la migration du périphérique vers FMC.

Virtual network ⓘ (New) vnet01 [redacted] FDM [redacted] ⌵
[Edit virtual network](#)

Management subnet * ⓘ (New) subnet1 ⌵
[Edit subnet](#) 172.18.0.0 - 172.18.0.255 (256 addresses)

GigabitEthernet 0/0 subnet * ⓘ (New) subnet2 ⌵
[Edit subnet](#) 172.18.1.0 - 172.18.1.255 (256 addresses)

GigabitEthernet 0/1 subnet * ⓘ (New) subnet3 ⌵
[Edit subnet](#) 172.18.2.0 - 172.18.2.255 (256 addresses)


Public inbound ports (mgmt. interface) * ⓘ None
 Allow selected ports

Select Inbound Ports (mgmt. interface) * ⓘ 3 selected ⌵

SSH (22)
SSH: ssh connectivity to the VM.

SFTunnel (8305)
SFTunnel: [FMC Management]: default tcp port 8305: management center and managed device(s) communication.

HTTPS (443)
HTTPS: [FDM Management]: FDM UI accessibility.

 Selected ports will be open for access from the Internet. See the Networking page later.

Ports à autoriser sur Cisco FTDv

Vérifier la configuration de la VM

9. Vérifiez la configuration dans l'onglet Vérifier + Créer et créez la VM.

Create Cisco Secure Firewall Threat Defense Virtual – BYOL and PAYG

by Cisco Systems, Inc.
[Terms of use](#) | [Privacy policy](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name	<input type="text"/>
Preferred e-mail address	<input type="text" value="@cisco.com"/>
Preferred phone number	<input type="text"/>

Basics

Subscription	<input type="text" value="fw-azure"/>
Resource group	<input type="text" value="FDM"/>
Region	East US
Virtual Machine name	<input type="text" value="fdm"/>
Licensing	BYOL : Bring-your-own-license
Software Version	7.4.1-172
Availability Option	None
Username for primary account (not the ...)	<input type="text"/>
Password	*****
Admin Password	*****
FTDv Management	FDM : Firepower Device Management

Cisco FTDv settings

Virtual machine size	Standard_D3_v2
Storage account	<input type="text" value="8b089e65"/>
Public IP address	<input type="text" value="fdm- -pip"/>
Domain name label	<input type="text" value="-fdm- -c352e65c"/>
Attach diagnostic interface	No

Virtual network	vnet01
Management subnet	subnet1
Address prefix (Management subnet)	172.18.0.0/24
GigabitEthernet 0/0 subnet	subnet2
Address prefix (GigabitEthernet 0/0 su...)	172.18.1.0/24
GigabitEthernet 0/1 subnet	subnet3
Address prefix (GigabitEthernet 0/1 su...)	172.18.2.0/24
Public inbound ports (mgmt. interface)	Allow selected ports
Select Inbound Ports (mgmt. interface)	SSH (22), SFTunnel (8305), HTTPS (443)

Vérifier et créer.

À ce stade, nous pouvons envoyer la création de VM.

10. Surveillez la progression du déploiement dans l'onglet Présentation, où un message indique que le déploiement est en cours.

The screenshot shows the Azure portal interface for a deployment. The deployment name is 'cisco.cisco-firepower-threat-defense-appliance'. The status is 'Deployment is in progress'. The start time is '6/11/2024, 11:50:26 AM' and the correlation ID is 'cc0d6c85f322'. The deployment details table is as follows:

Resource	Type	Status	Operation details
fdm	Virtual machine	Created	Operation details
fdm-3b089e65	Storage account	OK	Operation details
fdm-Nic2	Network interface	Created	Operation details
fdm-Nic1	Network interface	Created	Operation details
fdm-Nic0	Network interface	Created	Operation details
vnet01	Virtual network	OK	Operation details
3b089e65	Storage account	OK	Operation details
pid-4da66463-6b9b-47e7-93d5-2cbbfa4ed70d-partnercenter	Deployment	OK	Operation details
fdm-pip	Public IP address	OK	Operation details
subnet2-RouteTable	Route table	OK	Operation details
subnet3-RouteTable	Route table	OK	Operation details
fdm-Data-SecurityGroup	Network security group	OK	Operation details
subnet1-RouteTable	Route table	OK	Operation details
fdm-Mgmt-SecurityGroup	Network security group	OK	Operation details

Déploiement en cours.

Vérifier la VM déployée sur Azure

11. Lorsque la machine virtuelle est créée, localisez-la dans la section Machines virtuelles pour trouver ses caractéristiques et l'adresse IP publique attribuée.

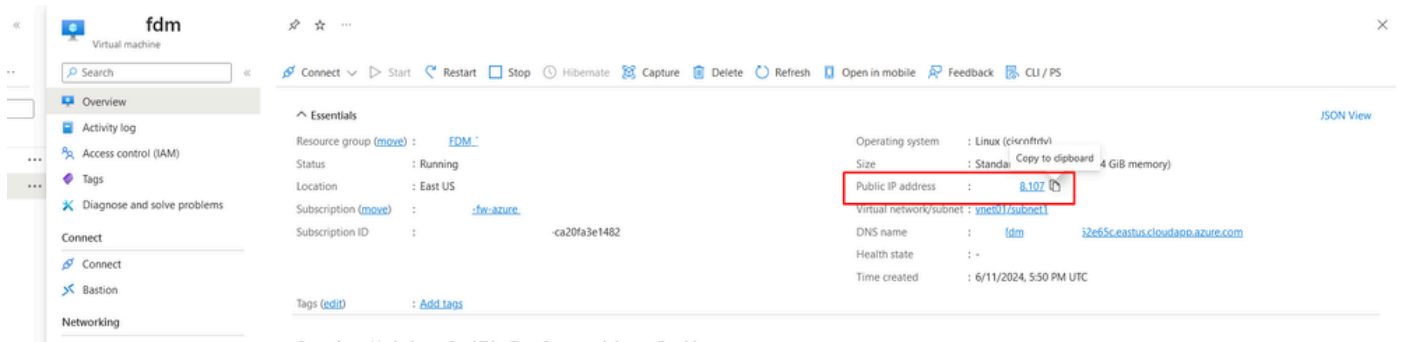
The screenshot shows the 'Virtual machines' section in the Azure portal. The table displays the following information:

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
fdm	Virtual machine	-fw-azure	_FDM_	East US	Running	Linux	Standard_D3_v2	107	1

Emplacement des machines virtuelles

12. Utilisez un navigateur pour accéder à l'adresse IP attribuée au périphérique et commencer la

configuration initiale de FDM.

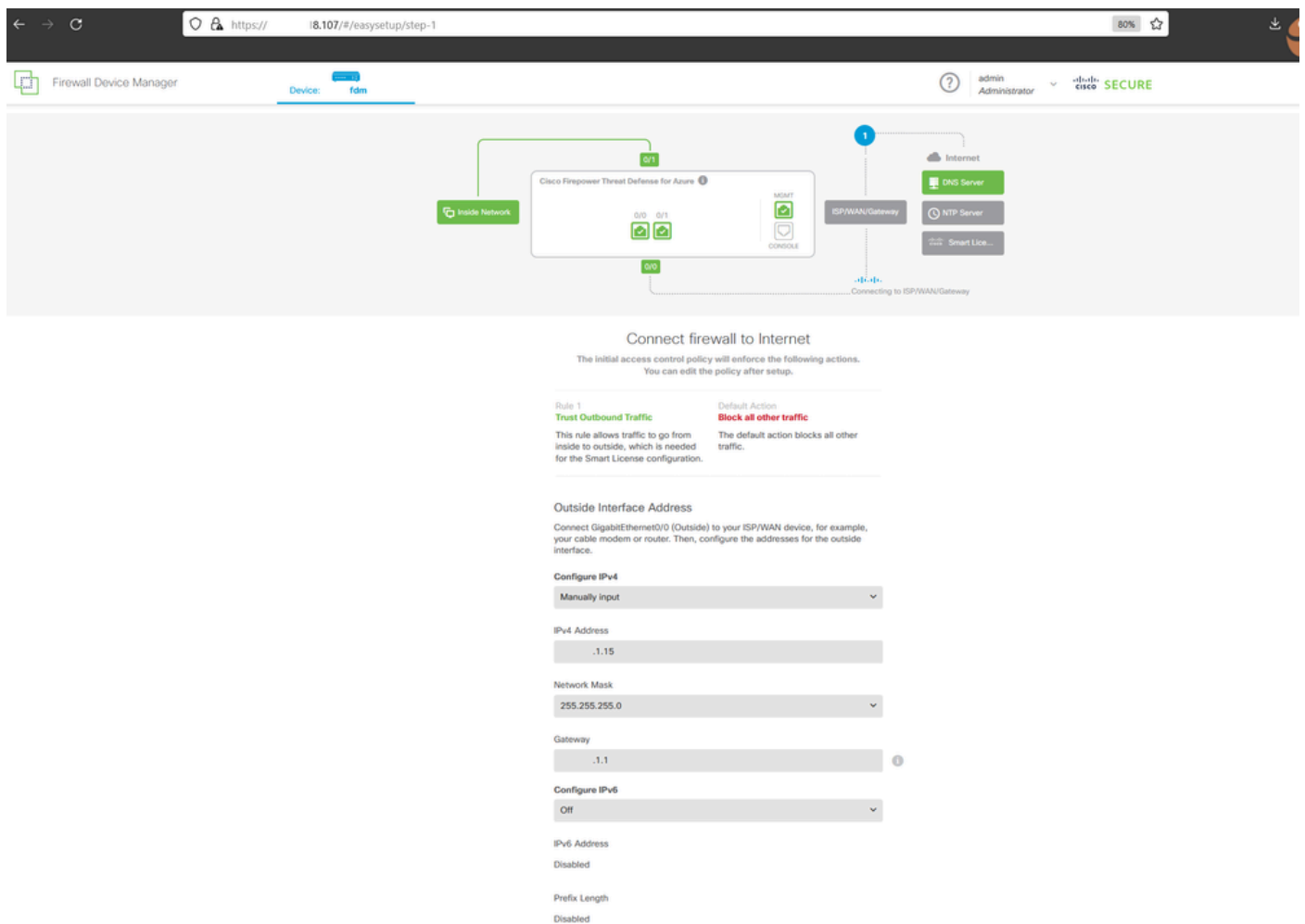


IP publique pour FDM

Configuration de base pour FDM

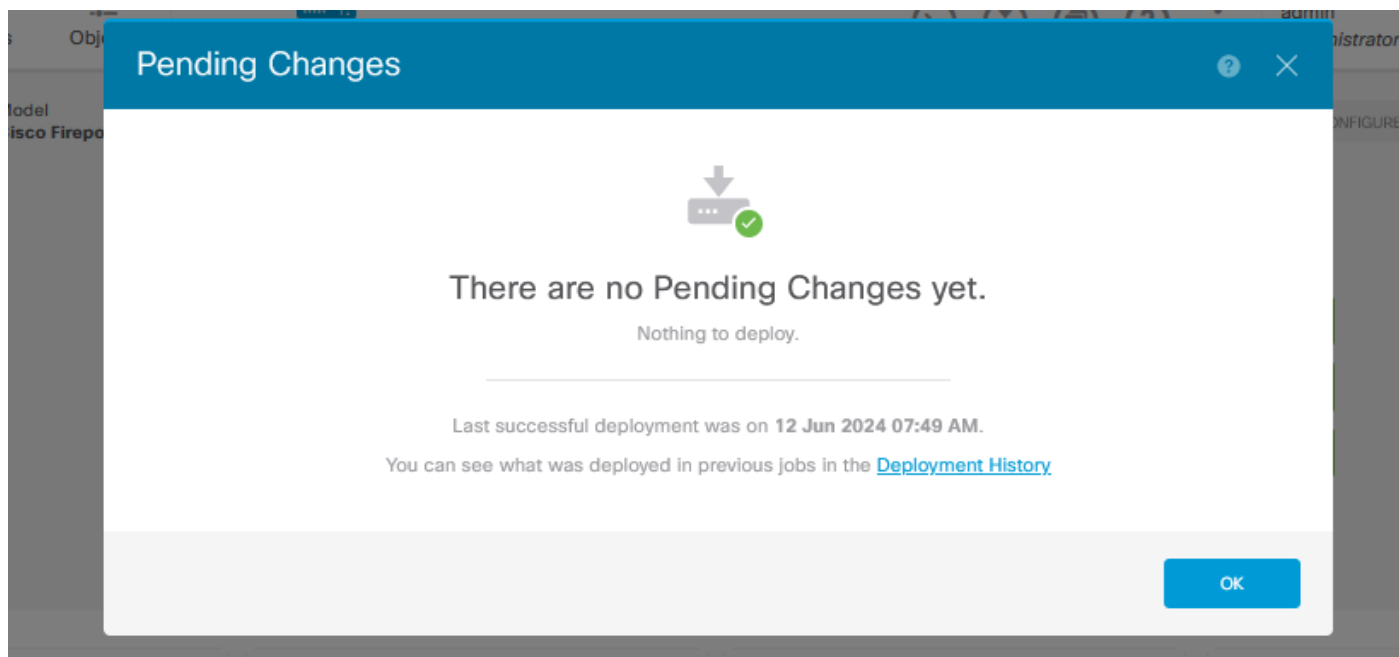
13. Configurez les paramètres de base en sélectionnant une adresse IP dans la plage attribuée, en configurant le protocole NTP et en enregistrant le périphérique avec la licence.

Vous trouverez ici la documentation de la [configuration initiale FDM](#) .



Configuration de base sur FDM

14. Une fois le périphérique enregistré, assurez-vous qu'aucun déploiement en attente ne reste.



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.