

Bereitstellen der virtuellen FDM-Maschine aus Azure Marketplace mithilfe der Vorlage

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Bereitstellung von FDM aus Vorlage im Azure-Portal](#)

[Konfiguration für VM überprüfen](#)

[VM auf Azure prüfen](#)

[Basiskonfiguration für FDM](#)

Einleitung

In diesem Dokument wird die Bereitstellung von Cisco Secure Firewall Threat Defense Virtual (FDM) auf einem virtuellen System mithilfe von Azure Marketplace und Vorlagen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)
- Azure-Konto/Zugriff

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Virtuelle Versionen von Cisco Secure Firewall Threat Defense: 7.4.1, 7.3.1, 7.2.7, 7.1.0, 7.0.6 und 6.4.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

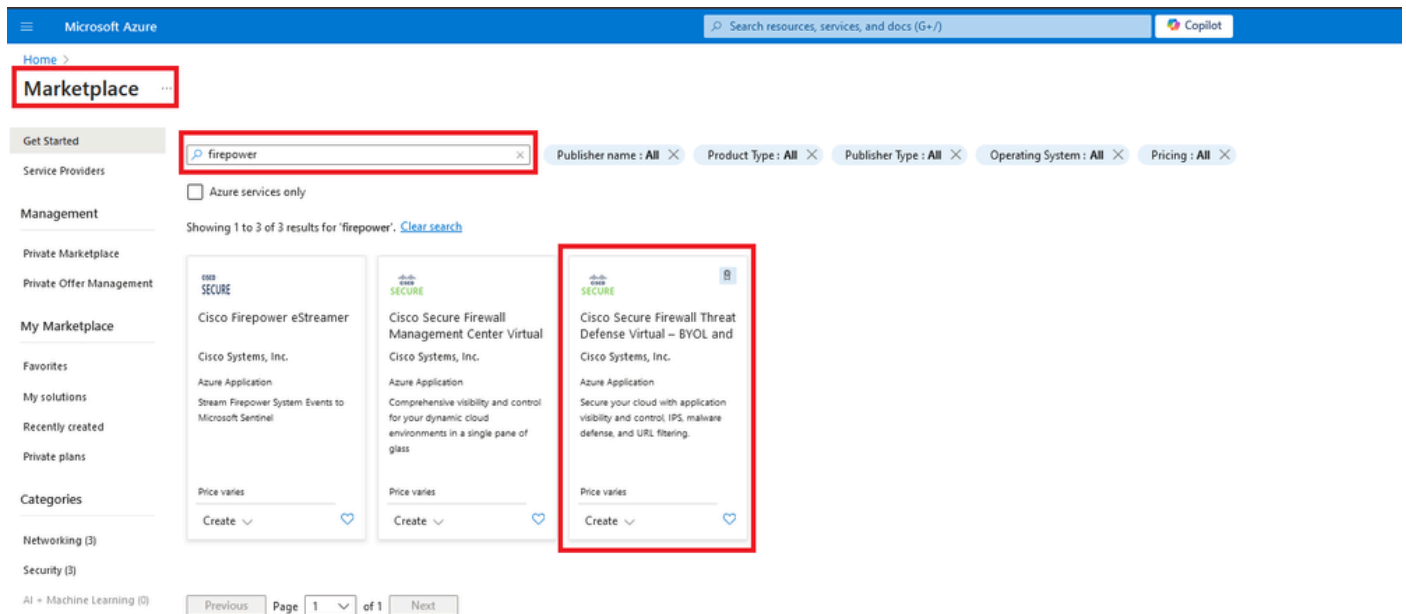
Konfigurieren

Bei der Bereitstellung eines FirePOWER-Gerätemanagers (FDM) auf einem virtuellen System von Azure sind Probleme aufgetreten, insbesondere bei der Verwendung von Azure Marketplace und Vorlagen.

Bereitstellung von FDM aus Vorlage im Azure-Portal

Gehen Sie folgendermaßen vor, um den FDM über das Azure-Portal bereitzustellen:

1. Navigieren Sie zum Azure-Portal, und suchen Sie den Marketplace in Azure Services. Suchen Sie nach Cisco Secure Firewall Threat Defense Virtual - BYOL and PAYG, und wählen Sie diese Option aus.



Suchen Sie nach Firepower und wählen Sie Cisco Secure Firewall Threat Defense Virtual - BOYL

2. Klicken Sie auf Erstellen, um den Konfigurationsprozess für FTD zu starten.

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...

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

VM aus Azure-Portal erstellen

3. Erstellen Sie auf der Seite für die Basiskonfiguration eine Ressourcengruppe für das Gerät, wählen Sie die Region aus, und wählen Sie einen Namen für die VM aus.

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 *

OK Cancel

Neue Ressourcengruppe erstellen

4. Wählen Sie aus den verfügbaren Optionen die gewünschte Version für die VM-Bereitstellung aus.

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

Verfügbare Versionen für die Bereitstellung auf Azure Market

5. Richten Sie einen Benutzernamen für das primäre Konto ein, wählen Sie Kennwort als Authentifizierungstyp aus, und legen Sie das Kennwort für den VM-Zugriff und das Admin-Kennwort fest.

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 * ⓘ

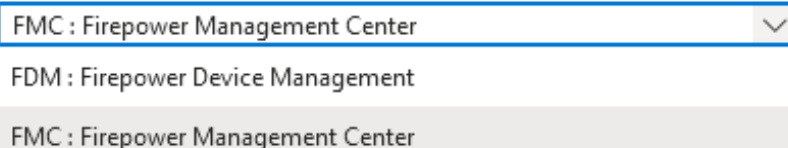
FTDv Management * ⓘ

Benutzername und Administratorkennwörter.

6. Wählen Sie für den Verwaltungstyp FDM für dieses Dokument aus.

FTDv Management * ⓘ

Enter FMC registration information * ⓘ



A dropdown menu is open, showing three options. The top option is 'FMC : Firepower Management Center' and is highlighted with a blue border. The middle option is 'FDM : Firepower Device Management'. The bottom option is 'FMC : Firepower Management Center' and is highlighted with a grey background. A small downward arrow is visible in the top right corner of the dropdown box.

Verwaltungsgerät.

7. Überprüfen Sie auf der Registerkarte Cisco FTDv Settings (Cisco FTDv-Einstellungen) die Größe des virtuellen Systems, das Speicherkonto, die öffentliche IP-Adresse und das DNS-Label, die standardmäßig nach Abschluss der Basiskonfiguration erstellt werden.

Stellen Sie sicher, dass die Einstellungen für Virtual Network, Management-Subnetz und andere Ethernet-Komponenten richtig sind.

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.

Cisco FTDv-Einstellungen.

8. Wählen Sie Ausgewählten Port zulassen, um die Ports SSH (22), SFTunnel (8305) und HTTPS (443) für den HTTPS-Zugriff auf den VM- und SFTunnel-Port für die Migration des Geräts zu FMC zu aktivieren.

Virtual network ⓘ (New) vnet01 FDM

Management subnet * ⓘ (New) subnet1
172.18.0.0 - 172.18.0.255 (256 addresses)


GigabitEthernet 0/0 subnet * ⓘ (New) subnet2
172.18.1.0 - 172.18.1.255 (256 addresses)

GigabitEthernet 0/1 subnet * ⓘ (New) subnet3
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.

Zulässige Ports für Cisco FTDv

Konfiguration für VM überprüfen

9. Überprüfen Sie die Konfiguration auf der Registerkarte Prüfen + Erstellen, und erstellen Sie die 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)

Prüfen und erstellen.

An dieser Stelle können wir die Erstellung der VM einreichen.

10. Überwachen Sie den Bereitstellungsstatus auf der Registerkarte Overview (Übersicht), auf der eine Meldung angezeigt wird, dass die Bereitstellung ausgeführt wird.

Resource	Type	Status	Operation details
fdm-...	Virtual machine	Created	Operation details
fdm-3a089e65	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
3a089e65	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

Bereitstellung wird ausgeführt.

VM auf Azure prüfen

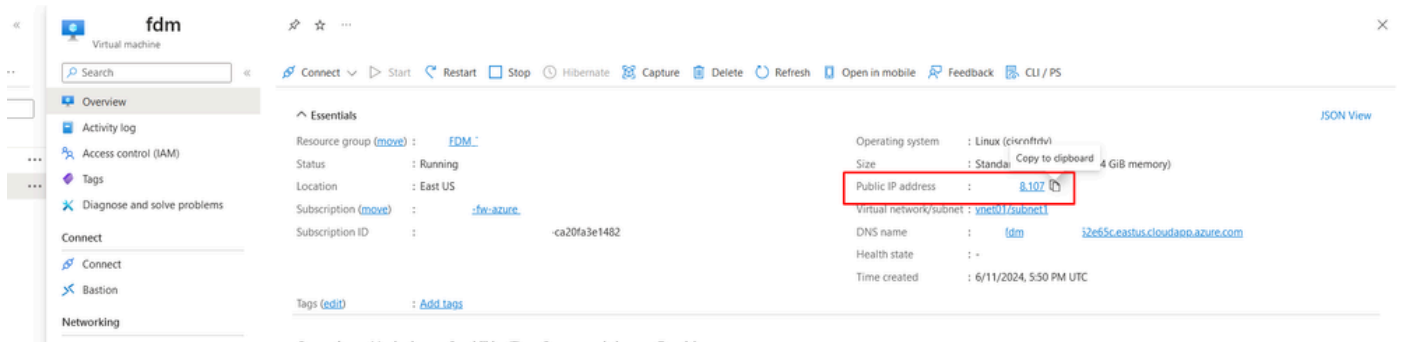
11. Wenn die VM erstellt wird, suchen Sie sie im Abschnitt Virtuelle Maschinen, um ihre Merkmale und die zugewiesene öffentliche IP-Adresse zu ermitteln.

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

Standort virtueller Systeme

12. Navigieren Sie in einem Browser zur zugewiesenen IP-Adresse des Geräts, und beginnen Sie

mit der Erstkonfiguration von FDM.

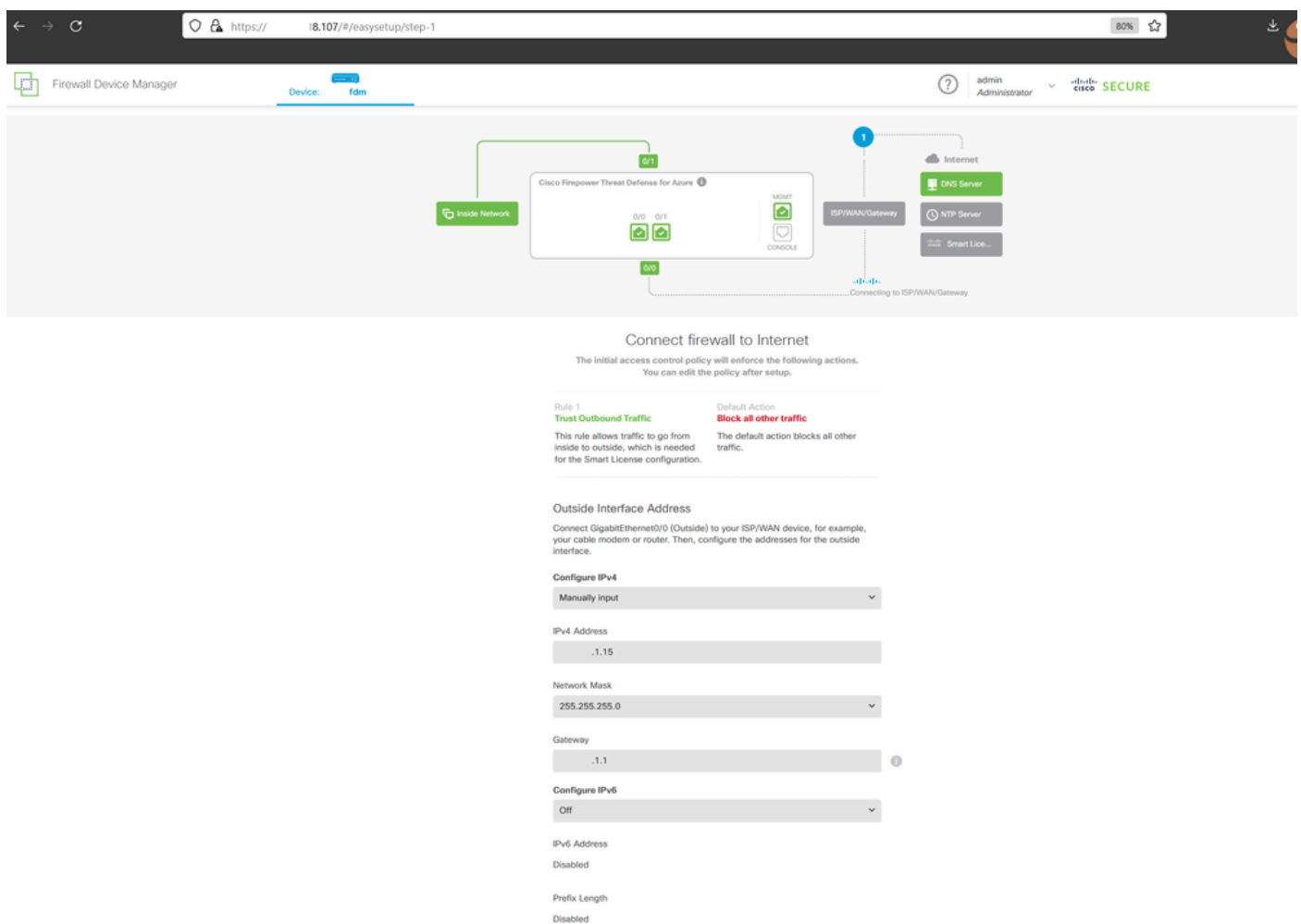


Öffentliche IP für FDM

Basiskonfiguration für FDM

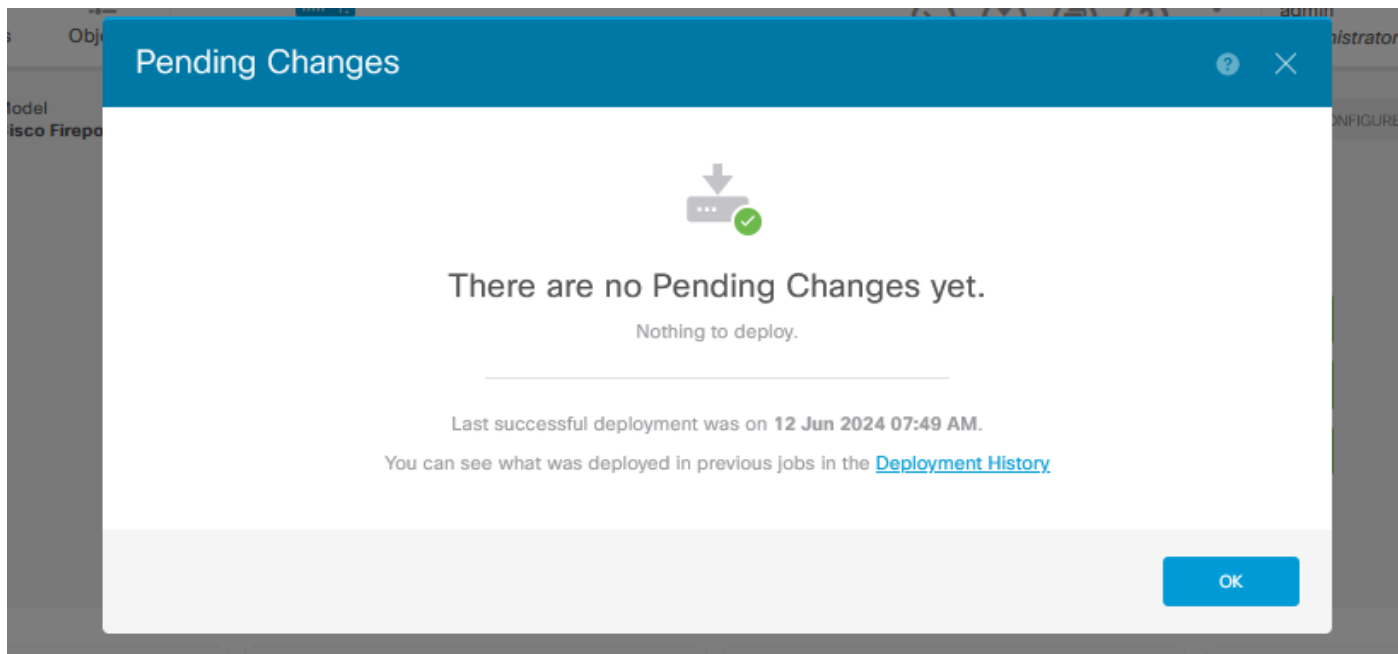
13. Konfigurieren Sie die Grundeinstellungen, indem Sie eine IP innerhalb des zugewiesenen Bereichs auswählen, NTP einrichten und das Gerät mit der Lizenz registrieren.

Hier finden Sie die Dokumentation zur [Erstkonfiguration](#) des [FDM](#) .



Basiskonfiguration auf FDM

14. Stellen Sie nach der Registrierung des Geräts sicher, dass keine ausstehenden Bereitstellungen bestehen bleiben.



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.