

テンプレートを使用したAzure MarketplaceからのFDM VMの配置

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[Azureポータル上のテンプレートからのFDMの配置](#)

[VMの設定の確認](#)

[AzureにデプロイされたVMの確認](#)

[FDMの基本設定](#)

はじめに

このドキュメントでは、Azure Marketplaceとテンプレートを使用して仮想マシンにCisco Secure Firewall Threat Defense(FDM)仮想マシンを導入する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall Management Center(FMC)
- Cisco Secure Firewall Threat Defense(FTD)
- Azureアカウント/アクセス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Secure Firewall Threat Defense仮想バージョン : 7.4.1、7.3.1、7.2.7、7.1.0、7.0.6、および6.4.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

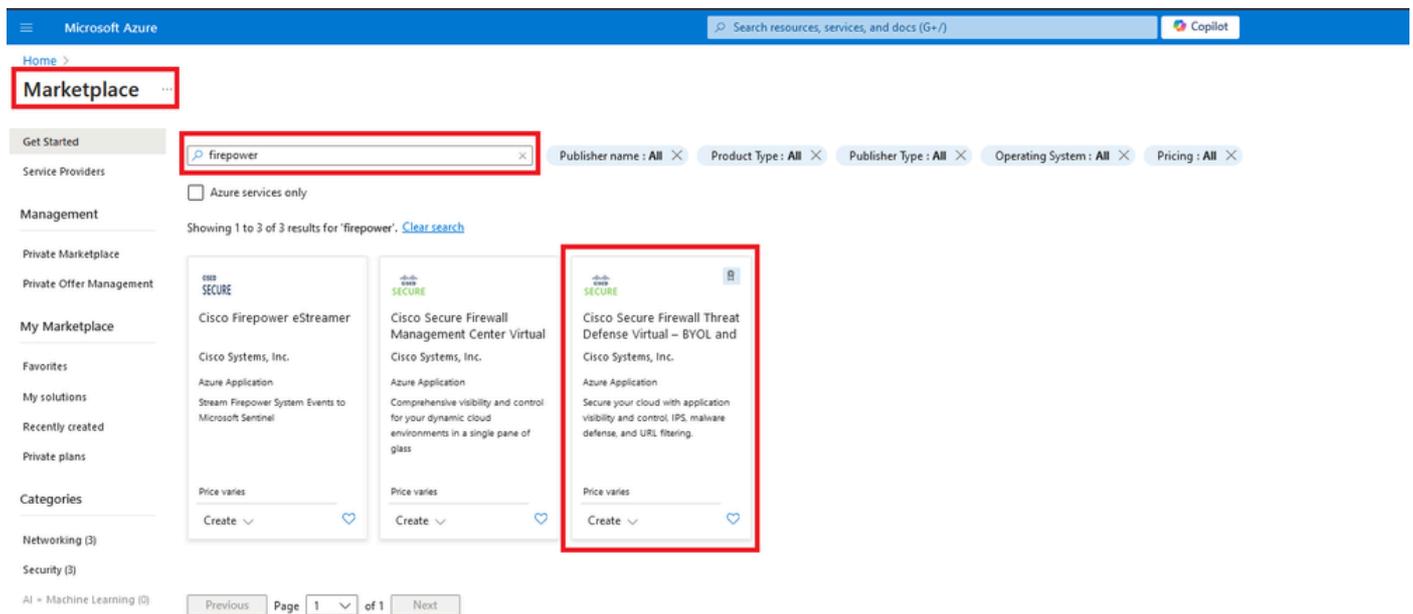
設定

お客様がAzureから仮想マシンにFirepower Device Manager (FDM)をデプロイしようとするとき、特にAzure Marketplaceとテンプレートを使用するときには問題が発生します。

Azureポータル上のテンプレートからのFDMの配置

AzureポータルからFDMを配置するには、次の手順を使用します：

1. Azure Portalに移動し、Azure Services内でMarketplaceを見つけます。Cisco Secure Firewall Threat Defense Virtual - BYOL and PAYGを検索して選択します。



Firepowerを検索し、Cisco Secure Firewall Threat Defense Virtuaを選択する – BOYL

2. Createをクリックして、FTDの設定プロセスを開始します。

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>
--	--	---	--

AzureポータルからのVMの作成

3. 基本設定ページで、デバイスのリソースグループを作成し、リージョンを選択し、VMの名前を選択します。

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

新しいリソースグループの作成

4. 使用可能なオプションから、VM導入に必要なバージョンを選択します。

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

Azure Marketで展開できるバージョン

5. プライマリアカウントのユーザ名を設定し、認証タイプとしてPasswordを選択し、VMアクセスのパスワードと管理者パスワードを設定します。

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 * ⓘ	fw-azure
Resource group * ⓘ	(New) FDM

[Create new](#)

Instance details

Region * ⓘ	East US
Virtual Machine name * ⓘ	fdm
Licensing ⓘ	BYOL : Bring-your-own-license
Software Version ⓘ	7.4.1-172
Availability Option * ⓘ	<input checked="" type="radio"/> None <input type="radio"/> Availability Zone

Username for primary account (not the FTDv admin user account) * ⓘ	<input type="password"/>
Authentication type * ⓘ	<input checked="" type="radio"/> Password <input type="radio"/> SSH Public Key
Password * ⓘ	<input type="password"/>
Confirm password *	<input type="password"/>
Admin Password * ⓘ	<input type="password"/>
Confirm Admin Password * ⓘ	<input type="password"/>
FTDv Management * ⓘ	FDM : Firepower Device Management

ユーザ名と管理者パスワード。

6. 管理タイプについては、このドキュメントの目的に合わせてFDMを選択します。

FTDv Management * ⓘ

Enter FMC registration information * ⓘ

FMC : Firepower Management Center

FDM : Firepower Device Management

FMC : Firepower Management Center

管理デバイス。

7. Cisco FTDv Settingsタブで、基本設定が完了した後にデフォルトで作成されるVMサイズ、ストレージアカウント、パブリックIPアドレス、およびDNSラベルを確認します。

仮想ネットワーク、管理サブネット、およびその他のイーサネット設定が正しいことを確認します。

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の設定

8. [選択したポートの許可]を選択して、VMへのHTTPSアクセスに対してポートSSH(22)、SFTunnel(8305)、およびHTTPS(443)を有効にし、デバイスをFMCに移行するためにSFTunnelポートを有効にします。

Virtual network ⓘ (New) vnet01 FDM

[Edit virtual network](#)

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

[Edit subnet](#)

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

[Edit subnet](#)

GigabitEthernet 0/1 subnet * ⓘ (New) subnet3 172.18.2.0 - 172.18.2.255 (256 addresses)

[Edit subnet](#)

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.

Cisco FTDvで許可されるポート

VMの設定の確認

9. Review + Createタブで設定を確認し、VMを作成します。

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

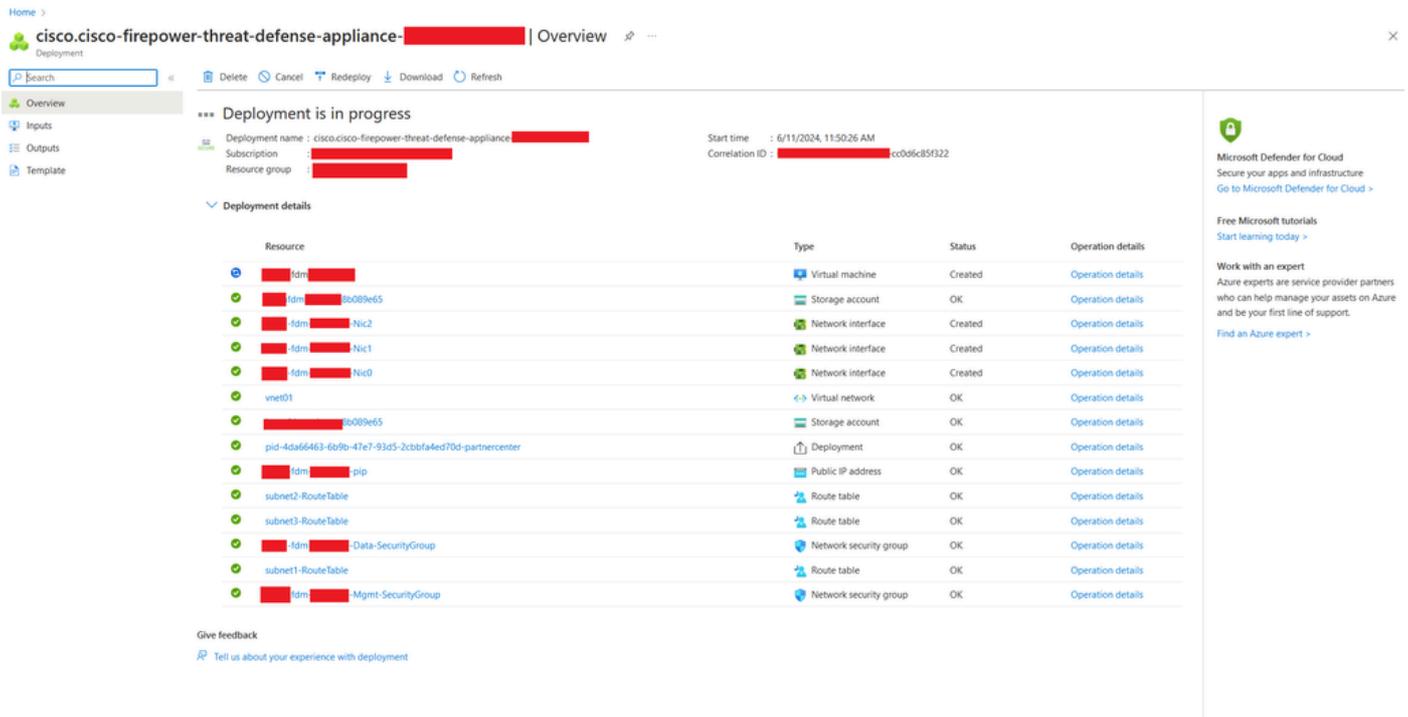
Virtual machine size	Standard_D3_v2
Storage account	<input type="text" value="8b089e65"/>
Public IP address	<input type="text" value="fdm- -pip"/>
Domain name label	<input type="text" value="-fdm- -c352e65c"/>
Attach diagnostic interface	No

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)

レビューと作成

この時点で、VMの作成を送信できます。

10. デプロイの進行状況を「概要」タブで監視します。このタブには、デプロイが進行中であることを示すメッセージが表示されます。



Deployment name: cisco.cisco-firepower-threat-defense-appliance- [redacted] | Overview

Deployment is in progress

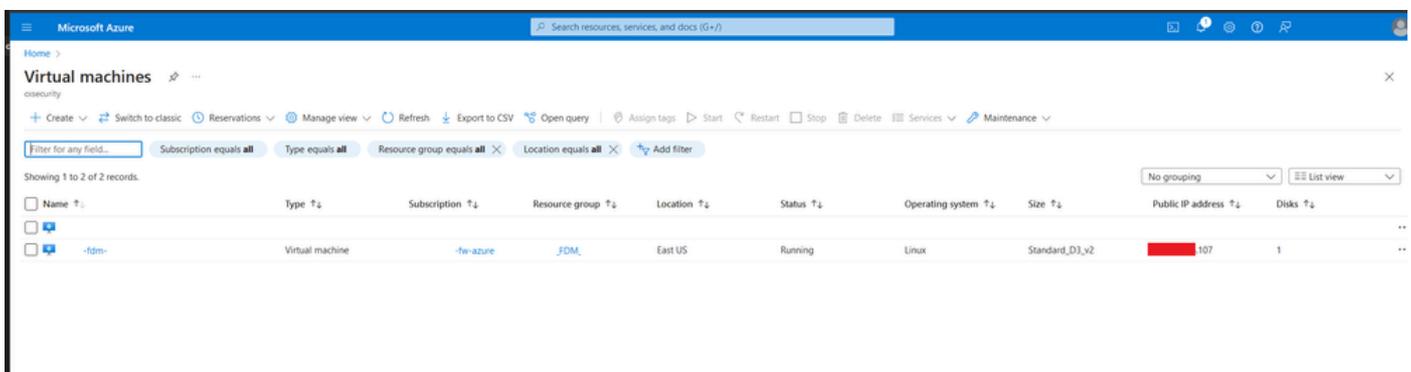
Start time: 6/11/2024, 11:50:26 AM
Correlation ID: [redacted] cc0d6c85f322

Resource	Type	Status	Operation details
[redacted] fdm	Virtual machine	Created	Operation details
[redacted] fdm [redacted] 3a089e65	Storage account	OK	Operation details
[redacted] fdm Nic2	Network interface	Created	Operation details
[redacted] fdm Nic1	Network interface	Created	Operation details
[redacted] fdm Nic0	Network interface	Created	Operation details
vnet01	Virtual network	OK	Operation details
[redacted] 3a089e65	Storage account	OK	Operation details
pid-4da66463-6b9b-47e7-93d5-2cbbfa4ed70d-partnercenter	Deployment	OK	Operation details
[redacted] fdm pip	Public IP address	OK	Operation details
subnet2-RouteTable	Route table	OK	Operation details
subnet3-RouteTable	Route table	OK	Operation details
[redacted] fdm Data-SecurityGroup	Network security group	OK	Operation details
subnet1-RouteTable	Route table	OK	Operation details
[redacted] fdm Mgmt-SecurityGroup	Network security group	OK	Operation details

展開中です。

AzureにデプロイされたVMの確認

11. VMが作成されたら、Virtual MachinesセクションでそのVMを見つけて、その特性と割り当てられているパブリックIPアドレスを確認します。



Microsoft Azure

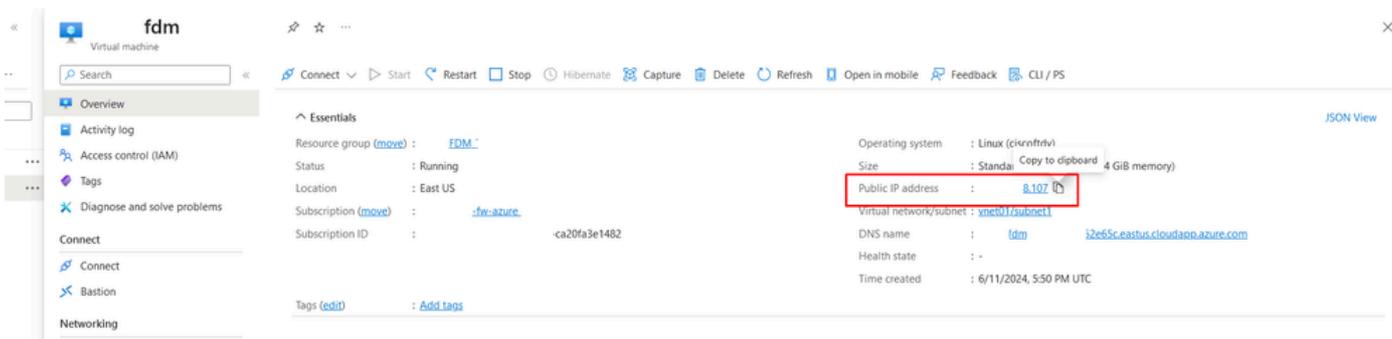
Virtual machines

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

仮想マシンの場所

12. ブラウザを使用してデバイスの割り当てられたIPアドレスに移動し、FDMの初期設定を開始

します。



FDMのパブリックIP

FDMの基本設定

13. 割り当てられた範囲内のIPを選択し、NTPを設定し、デバイスをライセンスに登録して、基本設定を行います。

ここでは、[FDM初期設定](#)に関するドキュメントを参照できます。

Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

Rule 1	Default Action
Trust Outbound Traffic This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	Block all other traffic The default action blocks all other traffic.

Outside Interface Address

Connect GigabitEthernet0/0 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4
Manually input

IPv4 Address
.1.15

Network Mask
255.255.255.0

Gateway
.1.1

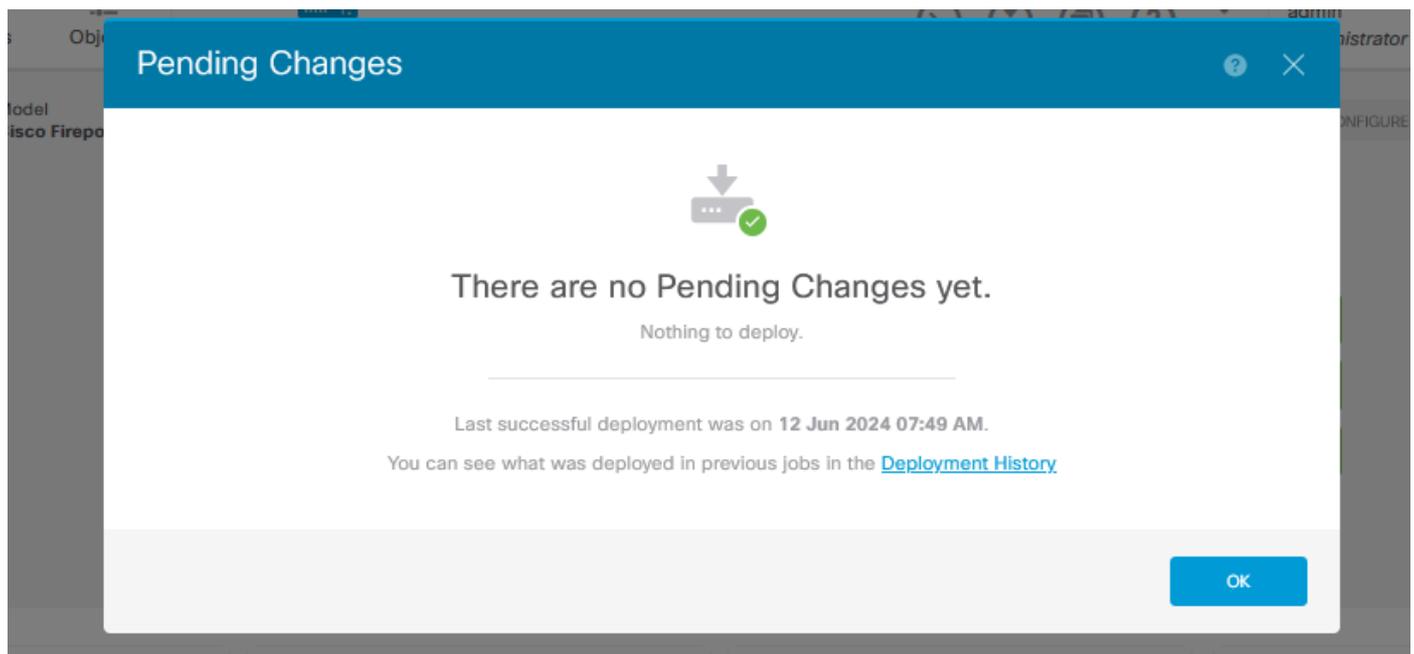
Configure IPv6
Off

IPv6 Address
Disabled

Prefix Length
Disabled

FDMの基本設定

14. デバイスを登録した後、保留中の展開が残っていないことを確認します。



翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。