

# Implementar la máquina virtual de FDM desde Azure Marketplace mediante plantilla

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Implementar FDM desde una plantilla en Azure Portal](#)

[Verificar configuración para VM](#)

[Comprobar VM implementada en Azure](#)

[Configuración básica de FDM](#)

---

## Introducción

Este documento describe la implementación de Cisco Secure Firewall Threat Defence Virtual (FDM) en una máquina virtual mediante Azure Marketplace y plantillas.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defence (FTD)
- Cuenta/acceso de Azure

## Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Secure Firewall Threat Defence Versiones virtuales: 7.4.1, 7.3.1, 7.2.7, 7.1.0, 7.0.6 y 6.4.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

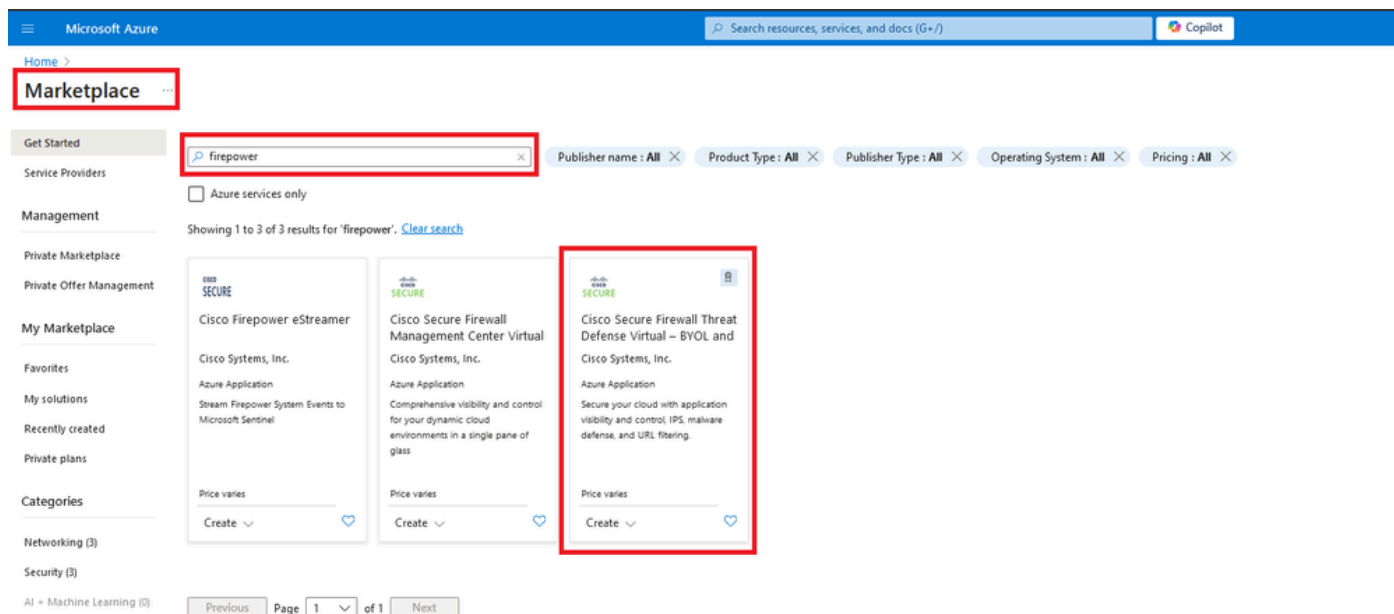
## Configurar

Los clientes han encontrado problemas al intentar implementar Firepower Device Manager (FDM) en una máquina virtual desde Azure, específicamente al usar Azure Marketplace y las plantillas.

## Implementar FDM desde una plantilla en Azure Portal

Para implementar FDM desde el portal de Azure, utilice este procedimiento:

1. Navegue hasta el portal de Azure y localice el Marketplace dentro de los Servicios de Azure. Busque y seleccione Cisco Secure Firewall Threat Defence Virtual - BYOL y PAYG.



Busque Firepower y seleccione Cisco Secure Firewall Threat Defence Virtual - BOYL

2. Pulse Crear para iniciar el proceso de configuración del 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](http://www.cisco.com/go/firewallTEI)

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

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

Crear VM desde Azure Portal

3. En la página de configuración básica, cree un grupo de recursos para el dispositivo, elija la región y seleccione un nombre para la máquina virtual.

# 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

Crear un nuevo grupo de recursos

4. Elija la versión que desee para la implementación de VM entre las opciones disponibles.

Software Version ⓘ

Availability Option \* ⓘ

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

Authentication type \* ⓘ

7.4.1-172

7.4.1-172

7.3.1-19

7.2.7-500

7.1.0-92

7.0.6-236

6.4.0-110

Versiones disponibles para implementar en el mercado de Azure

5. Configure un nombre de usuario para la cuenta principal, elija Contraseña como tipo de autenticación y establezca la contraseña para el acceso a VM y la contraseña de administrador.

# 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 \* ⓘ

Nombre de usuario y contraseñas de administrador.

6. Para el tipo de gestión, seleccione FDM a efectos de este documento.

FTDv Management \* ⓘ

Enter FMC registration information \* ⓘ

FMC : Firepower Management Center

FDM : Firepower Device Management

FMC : Firepower Management Center

Dispositivo de administración.

7. En la pestaña Cisco FTDv Settings, revise el tamaño de la máquina virtual, la cuenta de almacenamiento, la dirección IP pública y la etiqueta DNS, que se crean de forma predeterminada después de completar la configuración básica.

Asegúrese de que la red virtual, la subred de administración y otros parámetros de Ethernet sean correctos.

# 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.

Configuración de Cisco FTDv.

8. Seleccione Allow selected Port para habilitar los puertos SSH (22), SFTunnel (8305) y HTTPS (443) para el acceso HTTPS a la VM y al puerto SFTunnel para migrar el dispositivo a 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.

Puertos permitidos en Cisco FTDv

## Verificar configuración para VM

9. Revise la configuración en la pestaña Revisar + Crear y cree la máquina virtual.



# 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)

Revisar y crear.

En este momento podemos enviar la creación de la VM.

10. Supervise el progreso de la implementación en la ficha Descripción general, donde un mensaje indica que la implementación está en curso.

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

Deployment name: cisco.cisco-firepower-threat-defense-appliance [redacted] Start time: 6/11/2024, 11:50:26 AM  
Correlation ID: [redacted] cc0d6c85f322

Deployment details

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

Implementación en curso.

## Comprobar VM implementada en Azure

11. Cuando se cree la máquina virtual, búsquela en la sección Máquinas virtuales para encontrar sus características y la dirección IP pública asignada.

Virtual machines

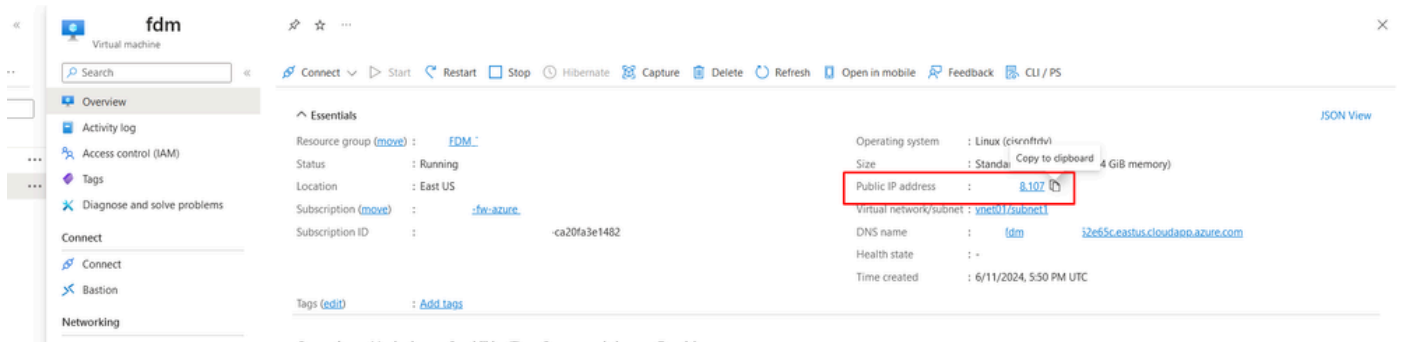
Showing 1 to 2 of 2 records.

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

Ubicación de máquinas virtuales

12. Utilice un navegador para navegar hasta la dirección IP asignada del dispositivo e iniciar la

## configuración inicial de FDM.

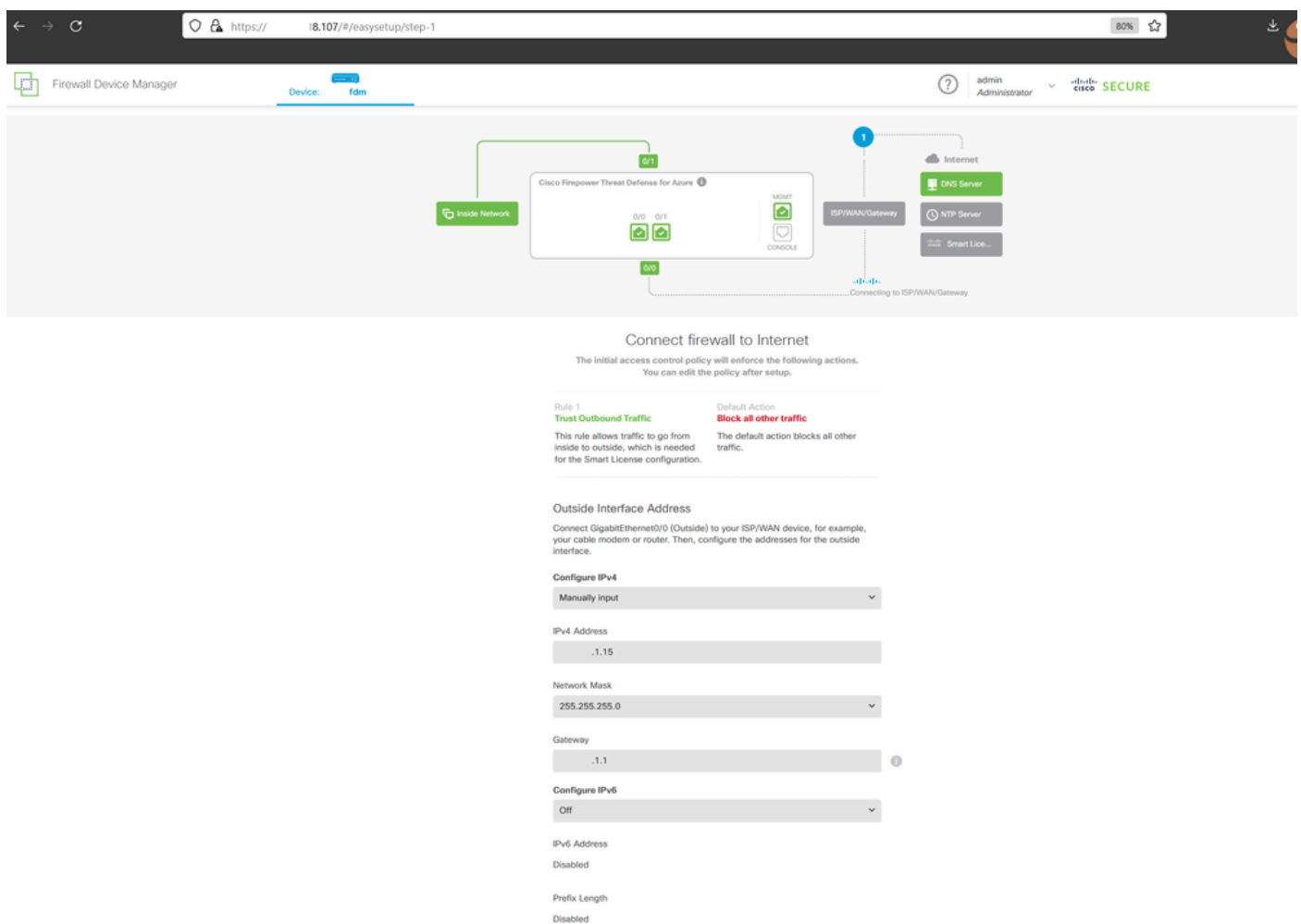


IP pública para FDM

## Configuración básica de FDM

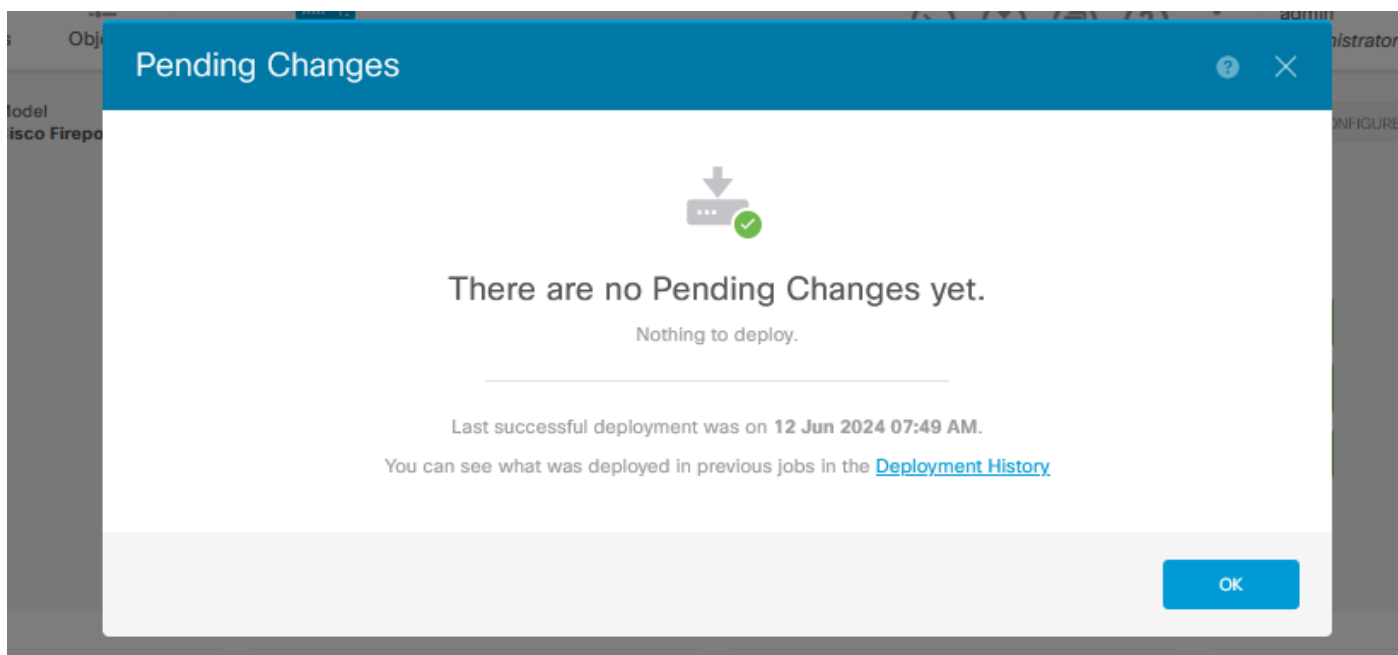
13. Configure los parámetros básicos seleccionando una IP dentro del rango asignado, configurando NTP y registrando el dispositivo con la licencia.

Aquí puede encontrar la documentación de la [configuración inicial de FDM](#).



Configuración básica en FDM

14. Después de registrar el dispositivo, asegúrese de que no quedan implementaciones pendientes.



## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).