

Implementazione di un CFC (Cloud-Delivered FMC) in Cisco Defense Orchestrator (CDO)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Distribuire un Firepower Management Center distribuito tramite cloud su CDO.](#)

[Integrazione di un FTD su un FMC fornito tramite cloud](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il processo di installazione e onboard di un CCP fornito tramite cloud sulla piattaforma CDO.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CdFMC (Cloud-Delivery Firepower Management Center)
- Cisco Defense Orchestrator (CDO)
- Firepower Threat Defense Virtual (FTDv)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- cdFMC 7.2.0
- FTDv 7.2.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco Defense Orchestrator (CDO) è la piattaforma per il centro di gestione dei firewall (cdFMC) distribuito nel cloud. Il centro di gestione dei firewall distribuito tramite cloud è un prodotto SaaS (Software-as-a-Service) che gestisce i dispositivi Secure Firewall Threat Defense. Offre molte delle stesse funzioni di una difesa contro le minacce Secure Firewall on-premises. Ha lo stesso aspetto e comportamento di un Centro di gestione Secure Firewall locale e utilizza la stessa API (Application Programming Interface) di FMC.

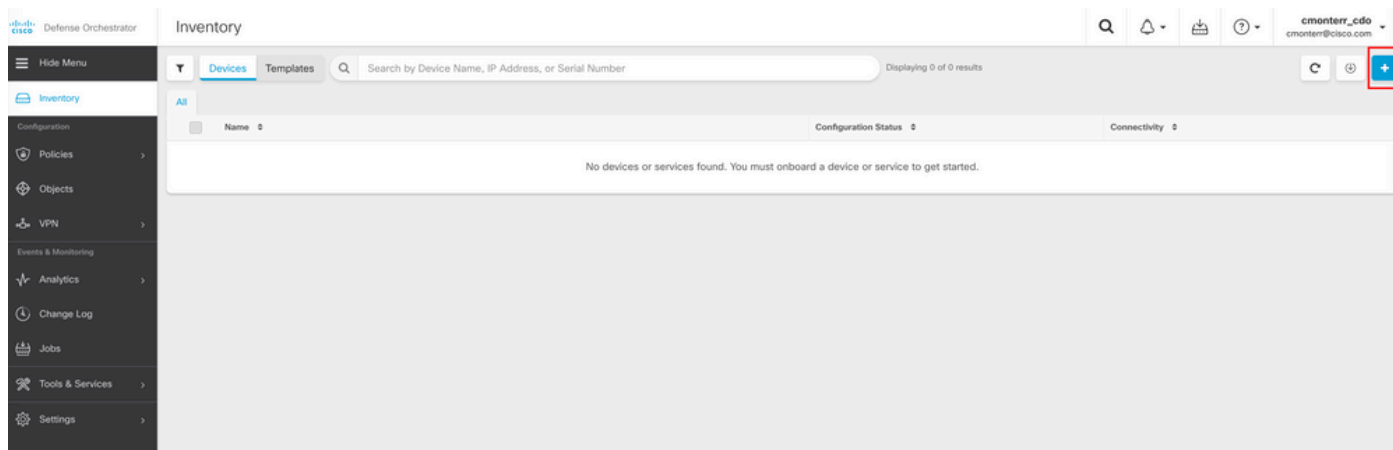
Questo prodotto è progettato per la migrazione dai Secure Firewall Management Center locali alla versione SaaS di Secure Firewall Management Center.

Configurazione

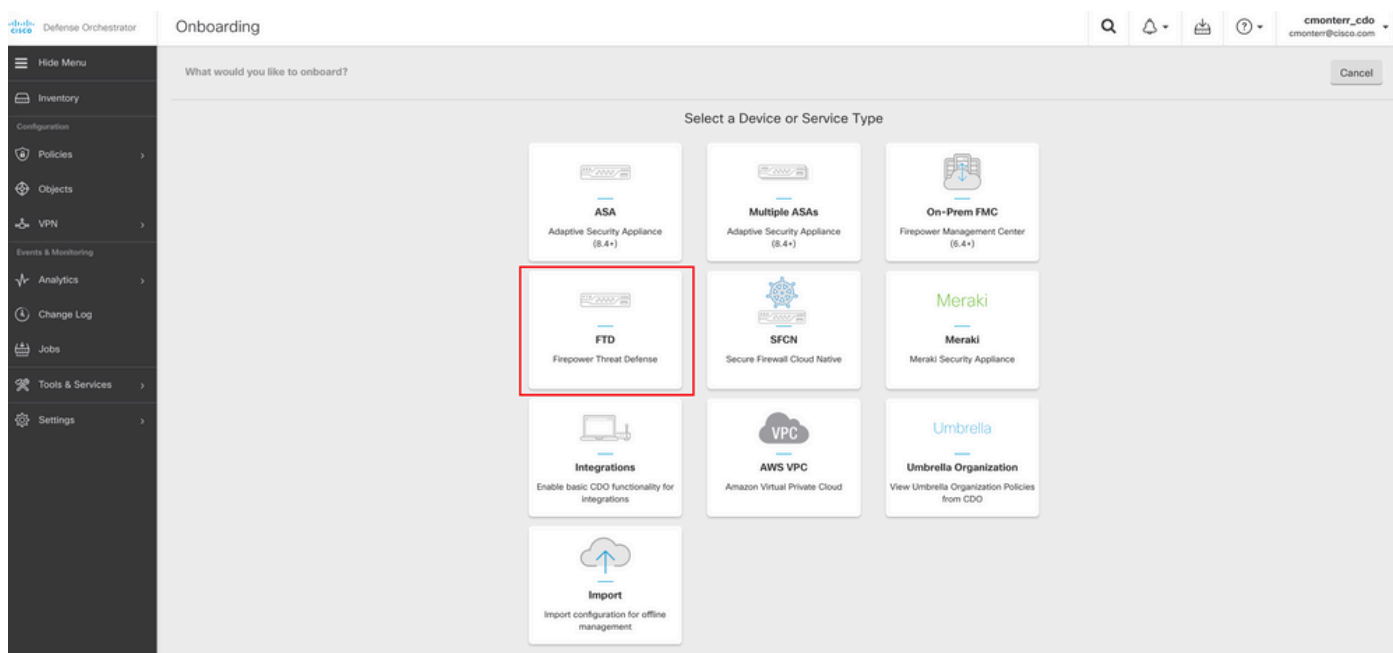
Distribuire un Firepower Management Center distribuito tramite cloud su CDO.

Queste immagini mostrano il processo di configurazione iniziale necessario per installare un FMC distribuito tramite cloud su CDO.

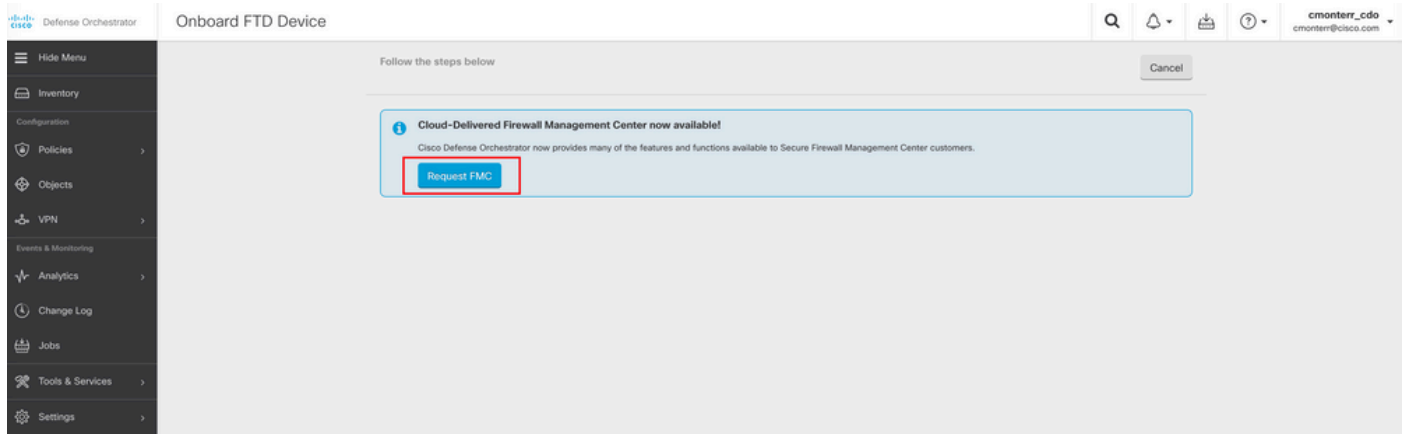
Innanzitutto, passare a **Menu > Inventory** per aggiungere una nuova periferica.



Seleziona Firepower Threat Defense (FTD).

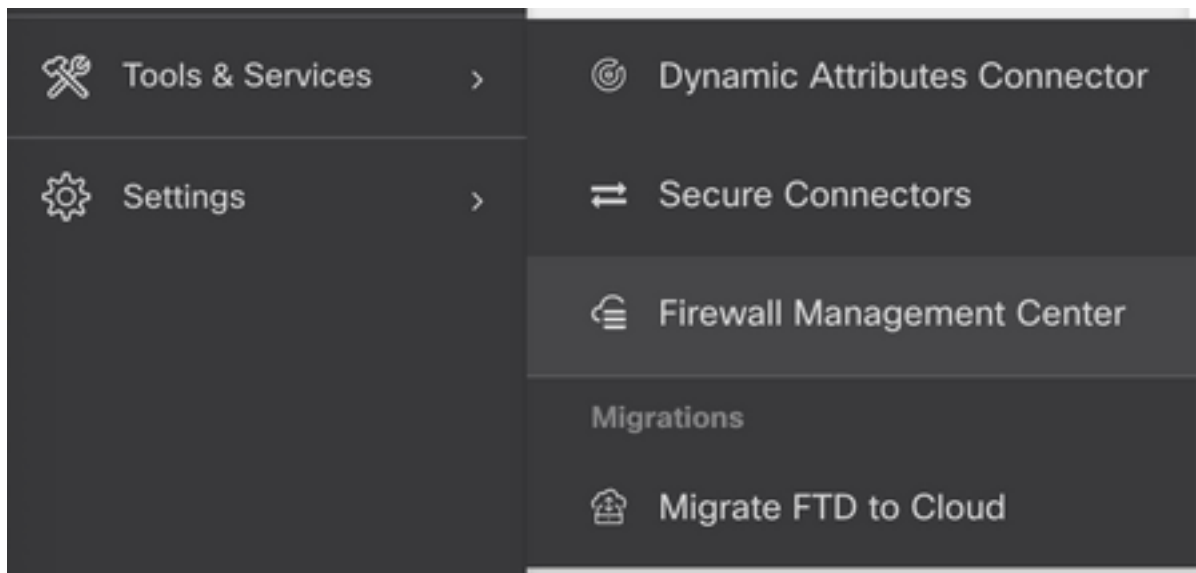


Seleziona **Request FMC** per richiedere il Cloud-Delivered Firepower Management Center.

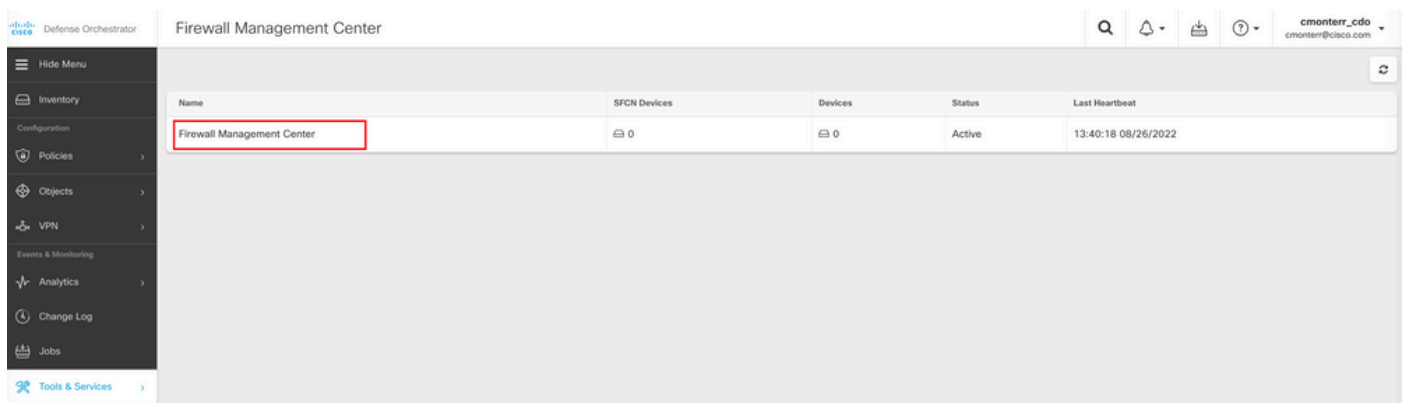


Nota: l'opzione "Request FMC" (Richiedi FMC) viene visualizzata solo se nel tenant non è presente alcun cdFMC.

Passa a **Menu > Tools & Services > Firewall Management Center** quando il cdFMC è pronto per l'uso.



Selezionare il cdFMC desiderato per visualizzare le informazioni sul cdFMC.



Per accedere all'interfaccia grafica dell'utente (GUI) di cdFMC, selezionare una delle opzioni disponibili sul lato destro.

Firewall Management Center

Name	SFCN Devices	Devices	Status	Last Heartbeat
Firewall Management Center	0	0	Active	13:40:18 08/26/2022

Firewall Management Center
 Hostname: cmonterr-cdo.app.us.cdo.cisco.com
 Software Version: 7.2.0-build 10364

Actions

- Deployment
- Updates
- Workflows
- API Explorer

Management

- Policies
- Objects
- NAT

Settings

- Configuration
- Smart Licenses
- AMP Management
- Device Health
- Audit
- Cisco Cloud Events

Ora è possibile vedere l'interfaccia utente di cdFMC.

Defense Orchestrator
 FMC / System / Health / Monitor

Analysis Policies Devices Objects Integration

Return Home Deploy

Monitoring

Home

Devices (1)

- FTDv

Health Status

1 total 0 critical 0 warnings 1 normal 0 disabled

Filter using device name ...

Device	Version	Model
FTDv	7.2.0	Cisco Firepower Threat Defense for Azure

Integrazione di un FTD su un FMC fornito tramite cloud

Nelle immagini viene mostrato come integrare un FTD per la registrazione su un CdFMC con una chiave di registrazione CLI (Command Line Interface).

Selezionare innanzitutto **onboard an FTD** nella home page CDO.

Defense Orchestrator

No devices or services have been onboarded

Click Here to Get Started

FTD Management **New**

- Manage FTD Policies
Create, edit, or manage FTD Policies
- Onboard an FTD**
Onboard an FTD Device
- Migrate FTD to Cloud
Migrate FTD Manager from Firewall Management Center to Cloud-Delivered FMC via CDO
- Dynamic Attributes Connector
Configure Dynamic Attributes

Take a tour of Cisco Defense Orchestrator

- Onboarding Devices and Services
Get started by onboarding all your devices to CDO.
- Object Management and Issue Detection
CDO provides easy object management and analytics.
- ASA Image Upgrades
ASA and ASDM upgrades made simple.
- ASA Command Line Interface
For expert users, CDO provides a command line interface for ASA devices.
- VPN Management
Visualize VPN configurations across all your devices to detect and resolve issues.
- Change Log and Change Requests
CDO provides easy logging of changes made across your devices.
- Read More
Visit our documentation for a full view of what CDO offers.

What's New in Defense Orchestrator

- August 4th, 2022
CDO Support for FDM-Managed Devices, Version 7.2
CDO now supports Secure Firewall Threat Defense version 7.2 for FDM-managed devices. You can now onboard an FDM-managed device running version 7.2 and upgrade an existing FDM-managed device to version 7.2.
- June 30th, 2022
Cisco Secure Firewall Migration Tool Supports Migrations to Cisco Secure Firewall Threat Defense
The Secure Firewall Migration Tool Version 3.0, allows you to migrate a Secure Firewall ASA to a Cisco Secure Firewall Threat Defense managed by either an on-prem or virtual Secure Firewall Management Center, or by our new cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
- June 9th, 2022
Cloud-Delivered Firewall Management Center
Cisco Defense Orchestrator (CDO) is now the platform for the cloud-delivered Firewall Management Center. The cloud-delivered Firewall Management Center is a software-as-a-service (SaaS) product that manages Secure Firewall Threat Defense devices. It offers many of the same functions as an on-premises Secure Firewall Management Center, it has the same appearance and behavior as an on-premises Secure Firewall Management Center, and uses the same FMC API. This product is designed for Secure Firewall Management Center customers who want to move from an on-premises version of the Secure Firewall Management Center to a SaaS version, or to new implementations of existing Firewall infra with its stability.

Quindi, selezionare **Use CLI Registration Key** opzione.

Onboard FTD Device

Follow the steps below

Cancel

Important: After onboarding your FTD, it will be managed by Firewall Management Center in CDO. Note that use of the firewall device manager will not be available after onboarding, and all existing policy configurations will be reset. You will need to reconfigure policies from CDO after onboarding. [Learn more](#)

Firepower Threat Defense
90-day Evaluation License:
89 days left
[Manage Smart License](#)

Use CLI Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using the Command Line Interface. (FTD 7.0.3+ & 7.2+)

Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number. (FTD 7.2+)

Procedere per immettere le informazioni FTDv richieste e desiderate.

1 Device Name **FTDv** [Edit](#)

2 Policy Assignment **Access Control Policy: Default Access Control Policy** [Edit](#)

3 Subscription License

Please indicate if this FTD is physical or virtual:

Physical FTD Device

Virtual FTD Device

Performance Tier (FTDv 7.0 and above only)

FTDv100 - Tiered (16 core / 32 GB)

License Type	Includes
<input checked="" type="checkbox"/> Base License	Base Firewall Capabilities
<input type="checkbox"/> Threat	Intrusion Policy
<input type="checkbox"/> Malware	File Policy
<input type="checkbox"/> URL License	URL Reputation
<input type="checkbox"/> RA VPN VPNOnly	RA VPN

[Next](#)

Info: Enable subscription licenses. CDO will attempt to enable the selected licenses when the device is connected to CDO and registered with the supplied Smart License. [Learn more about Cisco Smart Accounts.](#)

Note: All virtual FTDs require performance tier license. Make sure your subscription licensing account contains the available licenses you need. Its important to choose the tier that matches the license you have in your account. Until you choose a tier, your FTDv defaults to FTDv50 selection.

Infine, il CdFMC crea un CLI key Chiave CLI per il dispositivo.

4 CLI Registration Key

1 Ensure the device's initial configuration is complete before trying to apply the registration key. [Learn more](#)

2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cmonterr-cdo.app.us.cdo.cisco.com
NaRZpWdiG4waNYJMqVAXdKqsukd2nDTn 6qDJQJAYKn53d0TnEifT0XF5nseZ43pd cmonterr-
cdo.app.us.cdo.cisco.com
```

[Next](#)

Copiare CLI key nella CLI del dispositivo gestito.

```
> configure manager add cmonterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAXdK
qsukd2nDTn 6qDJQJAYKn53d0TnEifT0XF5nseZ43pd cmonterr-cdo.app.us.cdo.cisco.com
File HA_STATE is not found.

Manager cmonterr-cdo.app.us.cdo.cisco.com successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
> show managers
Type                : Manager
Host                : cmonterr-cdo.app.us.cdo.cisco.com
Display name       : cmonterr-cdo.app.us.cdo.cisco.com
Identifier         : 6qDJQJAYKn53d0TnEifT0XF5nseZ43pd
Registration       : Pending
```

CdFMC avvia un'attività di registrazione.

The screenshot shows the Cisco Defense Orchestrator (CDO) interface. The main view is the 'Inventory' page, which displays a table of devices. A single device, 'FTDv', is listed with a status of 'Onboarding'. The 'Onboarding' status is highlighted with a red box. To the right of the table, the 'Device Details' for 'FTDv' are shown, including fields for Location, Model, Serial, Version, Onboarding Method, and Registration Key. A 'Registration Pending' status is also highlighted with a red box, accompanied by instructions to complete the onboarding process by executing a registration command on the device. The command shown is 'configure manager add cmonterr-cdo.a...'. Below the details, there are sections for 'Device Actions', 'Monitoring', 'Device Management', 'Policies', 'Objects', and 'Label Groups and Labels'.

Nota: per completare il processo di registrazione, verificare che il dispositivo FTD in uso abbia la comunicazione sulle porte 8305 (sftunnel) e 443 al tenant CDO. Consultare i [requisiti di rete](#) completi.

Nota: se non è possibile connettersi all'host, è possibile rettificare la configurazione DNS nell'FTD-CLI con questo comando: **configure network dns <indirizzo>**.

Per monitorare il processo di registrazione, passare a **Device Actions > Workflows..**

The screenshot shows the 'Workflows' page in the Cisco Defense Orchestrator (CDO) interface. The page displays a table of workflow tasks for the device 'FTDv (FTD)'. The table has columns for Name, Priority, Condition, Current State, Last Active, and Time. Two tasks are listed: 'fmceRegisterFtdStateMachine' and 'ftdcOnboardingStateMachine'. Both tasks have a priority of 'On Demand', a condition of 'Done', and a current state of 'Done'. The last active times are 8/30/2022, 3:35:50 PM and 8/30/2022, 3:32:50 PM, respectively. The time column shows the start and end times of the workflow execution.

Espandere la **Active** per avere ulteriori informazioni, queste immagini mostrano come l'FTDv è stato registrato correttamente.

Workflows

Return to Inventory

FTDv (FTD)

Name	Priority	Condition	Current State	Last Active	Time
ACTION	TIME	START STATE	END STATE	RESULT	
PollingDelayedCheckAction	15:34:46.812 / 15:34:46.819	POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	● INITIATE_GET_TASK_STATUS	● SUCCESS	
FmcRequestGetAction	15:35:17.324 / 15:35:17.724	INITIATE_GET_TASK_STATUS	● WAIT_FOR_GET_TASK_STATUS	● SUCCESS	
FmcQueryTaskStatusResponseHandler	15:35:18.223 / 15:35:18.244	AWAIT_RESPONSE_FROM_executeFmcRequests	● POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	JOB_IN_PROGRESS	
PollingDelayedCheckAction	15:35:18.288 / 15:35:18.299	POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	● INITIATE_GET_TASK_STATUS	● SUCCESS	
FmcRequestGetAction	15:35:48.708 / 15:35:49.173	INITIATE_GET_TASK_STATUS	● WAIT_FOR_GET_TASK_STATUS	● SUCCESS	
FmcQueryTaskStatusResponseHandler	15:35:49.639 / 15:35:49.652	AWAIT_RESPONSE_FROM_executeFmcRequests	● INITIATE_GET_DEVICE_RECORDS_REGISTER_FTD	JOB_SUCCEEDED	
FmcRequestDeviceRecordsAction	15:35:49.674 / 15:35:50.084	INITIATE_GET_DEVICE_RECORDS_REGISTER_FTD	● WAIT_FOR_DEVICE_RECORDS_REGISTER_FTD	● SUCCESS	
FmcFilterDeviceResponseHandler	15:35:50.496 / 15:35:50.510	AWAIT_RESPONSE_FROM_executeFmcRequests	● DONE	● SUCCESS	
HOOK	TYPE	TIME	RESULT		
SaveInitialConnectivityStateBeforeHook	Before	15:33:11.229 / 15:33:11.231	Saved Connectivity State to context		
UpdateSMContextWithDeviceVersionHook	Before	15:33:11.231 / 15:33:11.234	setDeviceVersionInSMContext		
DeviceStateMachineClearErrorBeforeHook	Before	15:33:11.234 / 15:33:11.236	noErrorOccurred		
FmcRegisterFtdcStatusPreHook	Before	15:33:11.236 / 15:33:11.289	Executed pre hook successfully for FTD device: FTDv		
FmcRegisterFtdcStatusHook	After	15:35:50.517 / 15:35:50.519	Executed hook successfully		
NotifyOnConnectivityStateChangeAfterHook	After	15:35:50.519 / 15:35:50.521	Notification skipped for this event		
UpdateSMContextWithDeviceAsaNgPolicyFlagHook	After	15:35:50.521 / 15:35:50.523	notAsaDevice		
AddDeviceNameToStateMachineDebugAfterHook	After	15:35:50.523 / 15:35:50.528	Added device name to debug record		
DeviceStateMachineSetEmpirAfterHook	After	15:35:50.528 / 15:35:50.530	noErrorOccurred		
ftdcOnboardingStateMachine	● On Demand	● Done	● Done	8/30/2022, 3:32:50 PM	8/30/2022, 3:32:50 PM / 8/30/2022, 3:32:50 PM

Inventory

Devices Templates

Search by Device Name, IP Address, or Serial Number

Displaying 1 of 1 results

FTDv

Name	Configuration Status	Connectivity
FTDv FTD	○ Synced	● Online

Device Details

Location: n/a
Model: Cisco Firepower Threat Defense for Azure
Serial: 9AGTAFW24C6
Version: 7.2.0
Onboarding Method: Registration Key
Smart Version: 3.1.21.1-126

Synced
Your device's configuration is up-to-date.

Device Actions

- Check for Changes
- Manage Licenses
- Workflows
- Remove

Monitoring

- Health

Device Management

- Device Overview
- Routing
- Interfaces
- Inline Sets
- DHCP
- VTEP
- High Availability

Infine, passare a **Device Management > Device Overview** per accedere a cdFMC e rivedere lo stato della panoramica FTDv.

FTDv

Cisco Firepower Threat Defense for Azure

Device Routing Interfaces Inline Sets DHCP VTEP

<p>General</p> <p>Name: FTDv</p> <p>Transfer Packets: No</p> <p>Mode: Routed</p> <p>Compliance Mode: None</p> <p>TLS Crypto Acceleration: Disabled</p> <p>Device Configuration: Import Export Download</p>	<p>License</p> <p>Performance Tier: FTDv100 - Tiered (Core 16 / 32 GB)</p> <p>Base: Yes</p> <p>Export-Controlled Features: No</p> <p>Malware: No</p> <p>Threat: No</p> <p>URL Filtering: No</p> <p>AnyConnect Apex: No</p> <p>AnyConnect Plus: No</p> <p>AnyConnect VPN Only: No</p>	<p>System</p> <p>Model: Cisco Firepower Threat Defense for Azure</p> <p>Serial: 9AGTAFW2406</p> <p>Time: 2022-08-30 21:04:27</p> <p>Time Zone: UTC (UTC+0:00)</p> <p>Version: 7.2.0</p> <p>Time Zone setting for Time based Rules: UTC (UTC+0:00)</p>
<p>Inspection Engine</p> <p>Inspection Engine: Snort 3</p> <p>Revert to Snort 2</p>	<p>Health</p> <p>Status: ●</p> <p>Policy: Initial_Health_Policy 2022-06-04 01:25:03</p> <p>Excluded: None</p>	<p>Management</p> <p>Host: NO-IP</p> <p>Status: ●</p> <p>Manager Access Interface: Management Interface</p>

Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)
- [Gestione dei dispositivi Cisco Secure Firewall Threat Defense con Cloud Management Center](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).