

# Boordgebaseerde FDM naar Defense Orchestrator

## Inhoud

---

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

---

## Inleiding

Dit document beschrijft hoe u met behulp van een registratiesleutel aan boord van een apparaat dat wordt beheerd door Firepower Device Manager (FDM) naar Cisco Defense Orchestrator (CDO).

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Device Manager (FDM)
- Cisco Defense Orchestrator (CDO)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Device Manager (FDM) Azure met versie 7.4.1

Zie de [Secure Firewall Threat Defence Compatibility](#) Guide voor meer informatie voor een uitgebreide lijst met compatibele versies en producten.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

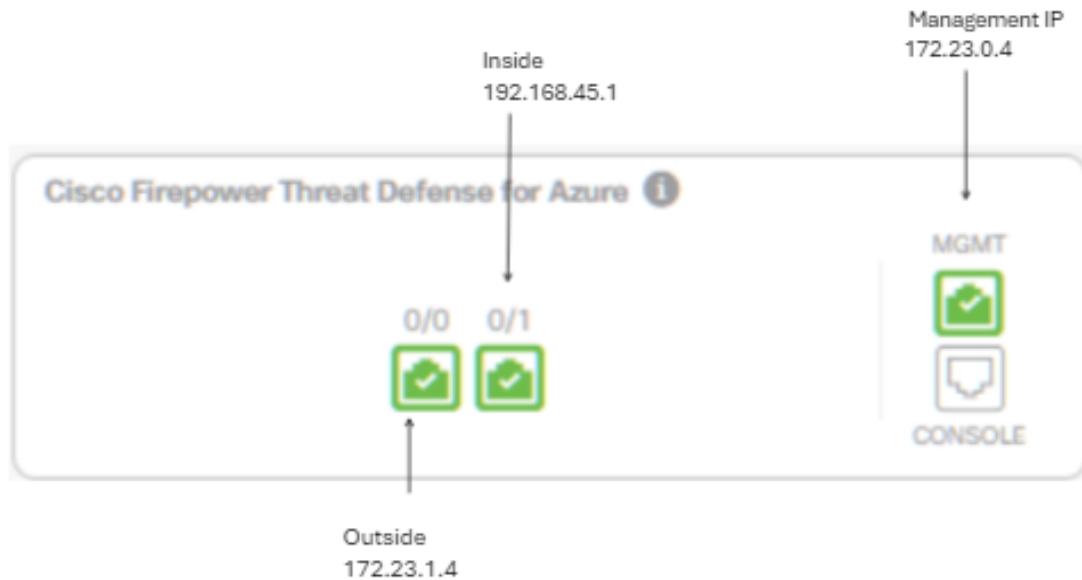
Zorg ervoor dat u aan deze voorwaarden voldoet voordat u met het onboardingsproces van een FDM-beheerd apparaat naar Cisco Defense Orchestrator (CDO) begint met behulp van een registratiesleutel:

1. Compatibele versie: Uw apparaat moet versie 6.6 of hoger uitvoeren.
2. Netwerkvereisten: [Sluit Cisco Defense Orchestrator aan op uw beheerde apparaten](#)
3. Beheerssoftware: het apparaat moet worden beheerd via Secure Firewall Device Manager (FDM).
4. Licentie: Uw apparaat kan gebruikmaken van een evaluatielicentie van 90 dagen of van een slimme licentie.
5. Bestaande registraties: Zorg ervoor dat het apparaat niet al is geregistreerd bij Cisco Cloud Services om conflicten tijdens het onboardingsproces te voorkomen.
6. Hangende veranderingen: Controleer dat er geen hangende veranderingen op het apparaat zijn.
7. DNS-configuratie: DNS-instellingen moeten correct worden geconfigureerd op uw FDM-beheerde apparaat.
8. Tijdservices: Tijdservices op het apparaat kunnen nauwkeurig worden geconfigureerd om synchronisatie met netwerktimeprotocollen te garanderen.
9. Vereiste voor activering van FDM-ondersteuning. Ondersteuning voor Firewall Device Manager (FDM) en de functionaliteit ervan wordt exclusief verleend op verzoek. Gebruikers zonder FDM-ondersteuning die op hun huurder is ingeschakeld, zijn niet in staat om configuraties te beheren of te implementeren op FDM-beheerde apparaten. Om dit platform te activeren, moeten gebruikers [een verzoek sturen naar het ondersteuningsteam](#) voor FDM ondersteuning enablement.

## Configureren

### Netwerkdigram

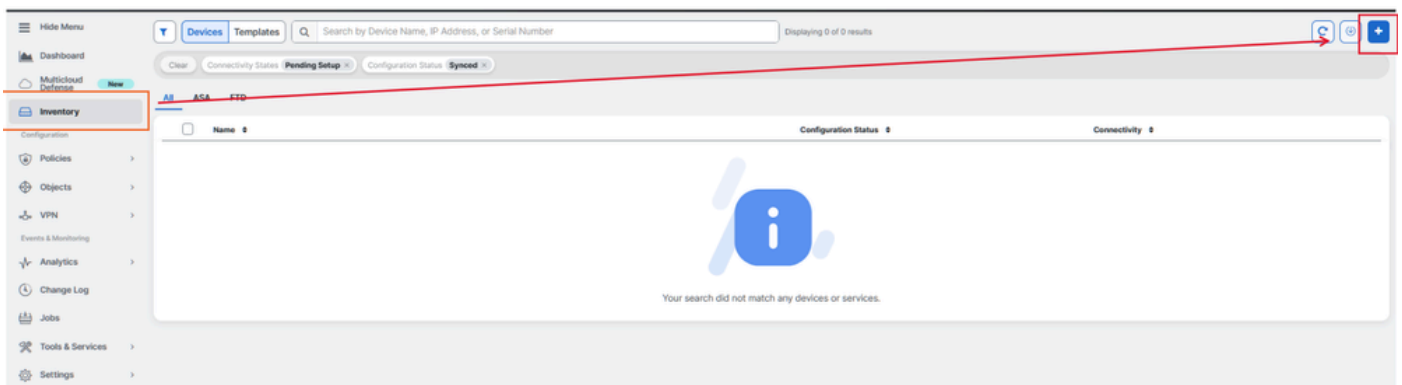
Dit artikel richt zich op een FDM (Firepower Device Manager) apparaat, dat wordt bestuurd via zijn beheerinterface. Deze interface heeft internettoegang die essentieel is voor de registratie van het apparaat met Cisco Defense Orchestrator (CDO).



## Configuraties

Stap 1. Log in op [Cisco Defense Orchestrator](#) (CDO).

Stap 2. Navigeer naar het Inventarisvenster en selecteer de blauwe knop plus om aan boord van een apparaat te gaan.












Stap 3. Kies de FTD-optie.

What would you like to onboard?

Select a Device or Service Type

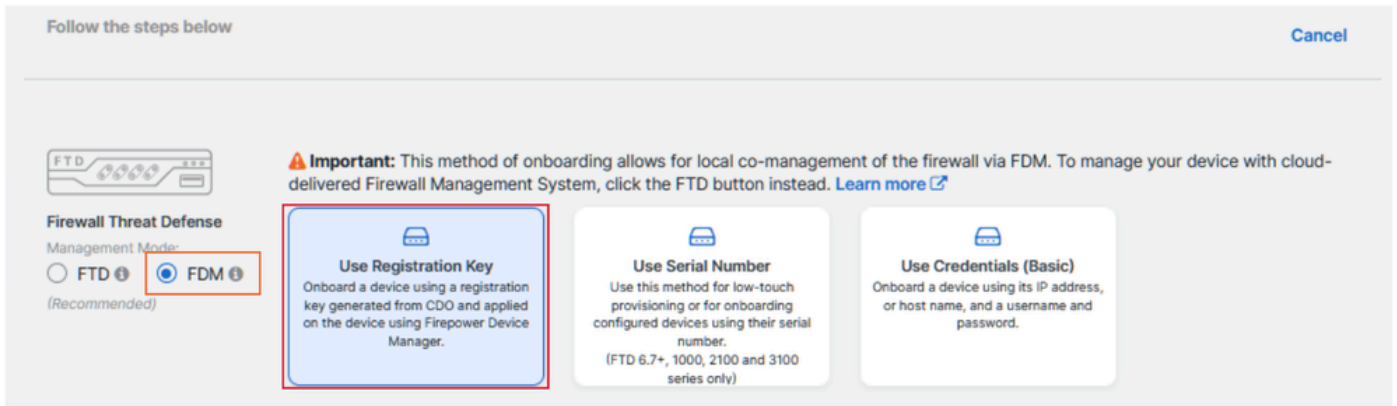
No Secure Device Connector found to communicate with some types of devices. [Set up a Secure Device Connector](#)

 <b>ASA</b> Adaptive Security Appliance (8.4+)	 <b>Multiple ASAs</b> Adaptive Security Appliance (8.4+)	 <b>FTD</b> Cisco Secure Firewall Threat Defense
 <b>Meraki</b> Meraki Security Appliance	 <b>Integrations</b> Enable basic CDO functionality for integrations	 <b>VPC</b> <b>AWS VPC</b> Amazon Virtual Private Cloud
 <b>Duo Admin</b> Duo Admin Panel	 <b>Umbrella Organization</b> View Umbrella Organization Policies from CDO	 <b>Import</b> Import configuration for offline management

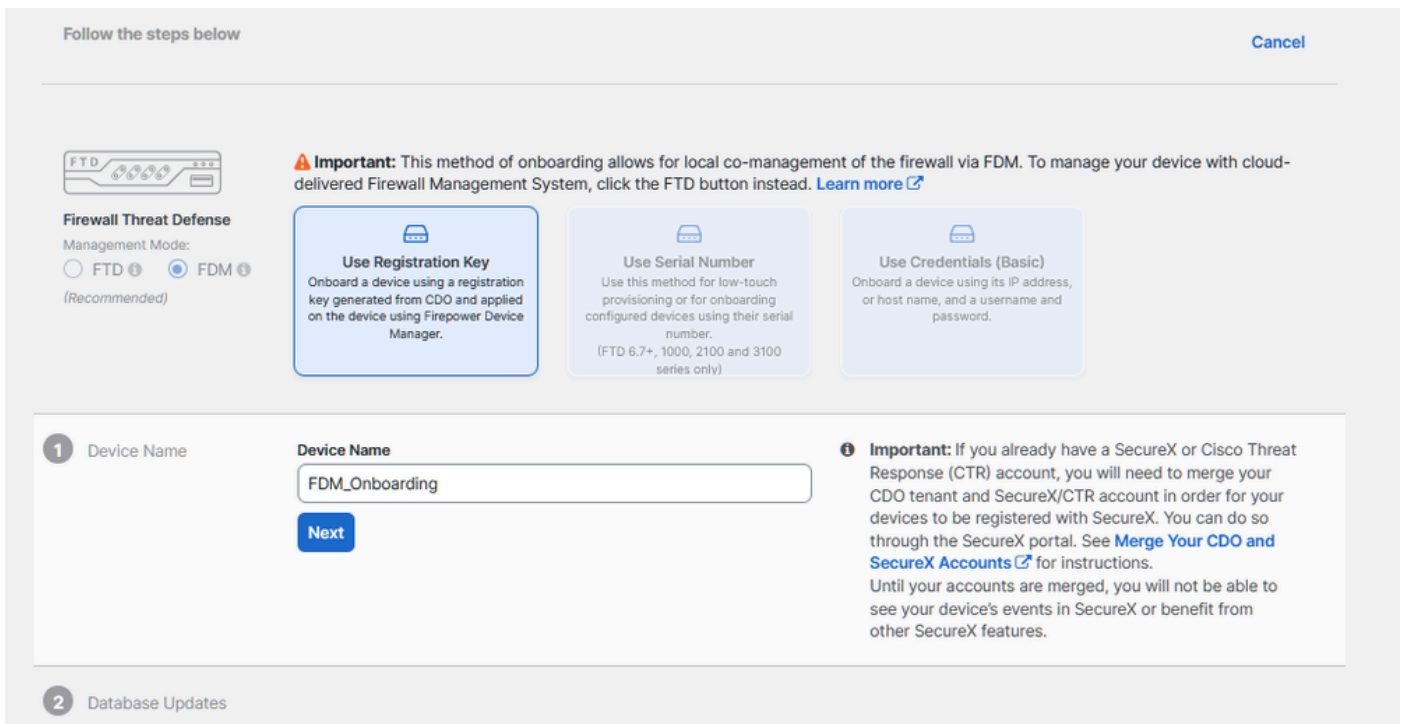
Stap 4 Ga verder naar het gedeelte "Onboard FTD Device" om het registratieproces te starten. Het is belangrijk om de beschikbare methoden voor het onboarden van een Threat Defence Device op te merken:

- **Op serienummer:** deze methode is van toepassing op fysieke apparaten zoals de Firepower 1000, Firepower 2100 of Secure Firewall 3100 reeks met ondersteunde softwareversies. Het vereist het chassis- of PCA-serienummer en een netwerkverbinding met het internet.
- **Door de sleutel van de Registratie:** Dit is de aangewezen methode voor aan boord, bijzonder voordelig voor apparaten die IP adressen via DHCP ontvangen, aangezien het helpt connectiviteit met CDO handhaven zelfs als er een verandering in het apparaat IP adres is.
- **Credentials gebruiken:** Dit alternatief betreft het invoeren van de apparaatreferenties en het IP-adres van de buitenkant, binnen of de beheerinterface, aangepast aan de apparaatconfiguratie binnen het netwerk.

Voor dit proces, selecteer de optie FDM en dan de optie Use Registration Key om consistente connectiviteit met CDO te verzekeren, ongeacht mogelijke veranderingen in het apparaat IP adres.



Stap 5. Voer de gewenste apparaatnaam in het veld Apparaatnaam in en specificeer de beleidstoewijzing. Kies ook de Subscription License die aan het apparaat moet worden gekoppeld.



Stap 6. De sectie van de Updates van het Gegevensbestand wordt gevormd door gebrek om veiligheidsupdates onmiddellijk uit te voeren en opstellingen terugkomende updates. Als u deze instelling wijzigt, worden geen bestaande updateschema's gewijzigd die zijn ingesteld met de Secure Firewall-apparaatbeheer.

1 Device Name **FDM\_Onboarding**

---

2 Database Updates  Immediately perform security updates, and enable recurring updates.

Databases **Geolocation, Intrusion Rule, VDB, Security Intelligence Feeds**

Schedule **Weekly on Mo at 02:00 AM** [Set Schedule](#)

**Next**

---

3 Create Registration Key

---

4 Smart License

---

5 Done

Stap 7. In het gedeelte CLI-registratiesleutel genereert CDO automatisch een registratiesleutel. Het verlaten van de onboarding interface vóór voltooiing resulteert in het creëren van een plaatsaanduiding voor het apparaat in de inventaris. De registratiesleutel kan indien nodig op een later tijdstip van deze locatie worden opgehaald.

1 Device Name **FDM\_Onboarding**


---

2 Database Updates **Enabled**

---

3 Create Registration Key

1 Copy registration key

`8M80kxwbQ2s7c8k4R54e477887028fsfa` 

2 Paste the registration key copied above in the Cloud Services management in FDM. [Learn more](#)

**Next**

---

4 Smart License

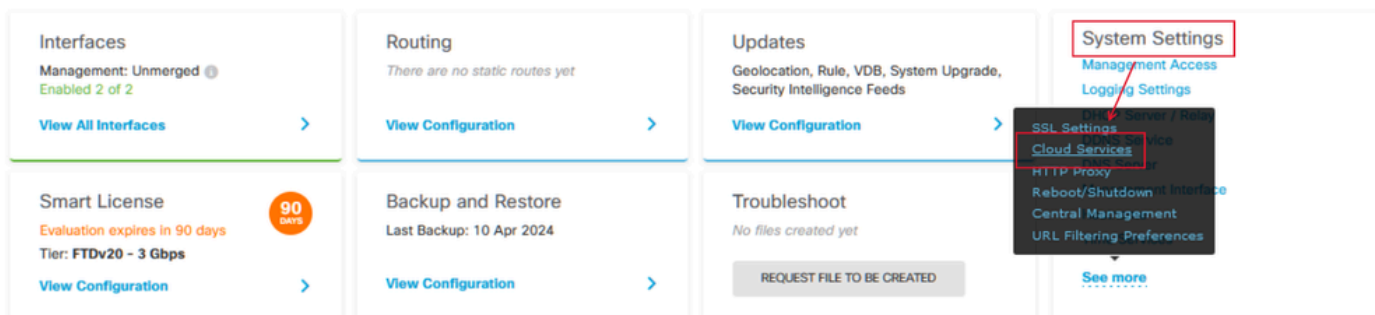
---

5 Done

Stap 8. Klik op het pictogram Kopiëren om de gegenereerde registratiesleutel te kopiëren.

Stap 9. Ga naar het Secure Firewall Device Manager-apparaat dat is bedoeld voor instap via CDO.

Stap 10. Selecteer Cloud Services in het menu Systeeminstellingen.




Stap 11. Wijs het juiste Cisco-cloudgebied in de vervolgkeuzelijst Regio aan, uitgelijnd met de geografische locatie van de huurder:

- Selecteer op [defenseorchestrator.com](https://defenseorchestrator.com) de optie UCS.
- Selecteer EU voor [defenseorchestrator.eu](https://defenseorchestrator.eu).
- Selecteer voor [apj.cdo.cisco.com](https://apj.cdo.cisco.com) APJ.

## Device Summary

# Cloud Services

 **Not Registered**

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

### Enrollment Type

**Security/CDO Account**

Smart Licensing

### Region

US Region

### Registration Key

85038aebd2b7c06d454e4778972df6fa

### Service Enrollment


#### Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

#### Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) 

Enroll Cisco Success Network

**REGISTER**

Need help? 

Stap 12. Kies in het gedeelte Inschrijftype voor de Security-account.



## Device Summary

# Cloud Services



Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

### Enrollment Type

Security/CDO Account

Smart Licensing

### Region

US Region

### Registration Key

85038aebd2b7c06d454e4778972df6a

## Service Enrollment

### Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

### Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▾

Enroll Cisco Success Network

REGISTER

Need help?

Step 13. Plakt de registratiesleutel in het veld Registratiesleutel.

## Device Summary

# Cloud Services



Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

### Enrollment Type

Security/CDO Account

Smart Licensing

### Region

US Region

### Registration Key

85038aebd2b7c06d454e4778972d96fa



### Service Enrollment

#### Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

#### Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▼

Enroll Cisco Success Network

REGISTER

Need help?

Stap 14. Voor apparaten op versie 6.7 of hoger controleert u of Cisco Defense Orchestrator is ingeschakeld in het gedeelte Service Enrollment.

## Device Summary

# Cloud Services



Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

### Enrollment Type

Security/CDO Account

Smart Licensing

### Region

US Region

### Registration Key

65038aebd2b7c06d454e4778973df6fa



### Service Enrollment

#### Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

#### Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#)

Enroll Cisco Success Network

REGISTER

Need help?

Stap 15. (Optioneel) Bekijk de details van de Cisco Success Network Enrollment. Als u niet wilt deelnemen, deselecteert u het aankruisvakje Cisco Success Network (Cisco-succesnetwerk)

registreren).

Stap 16. Selecteer Registreer en accepteer de Cisco Disclosure. De Secure Firewall Device Manager dient de registratie in bij de CDO.

**Device Summary**  
Cloud Services

**Not Registered**

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

**Enrollment Type**

Security/CDO Account Smart Licensing

**Region**

US Region

**Registration Key**

#5038aebd3b7c06d454e4778972d96a

**Service Enrollment**

**Cisco Defense Orchestrator**

Cisco Defense Orchestrator is a cloud-based management solution for Cisco devices. Select this option if you want to register with your account.

Enable Cisco Defense Orchestrator

**Cisco Success Network**

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#)

Enroll Cisco Success Network

**REGISTER** Need help?

**Cisco Disclosure**

Your device establishes a secure connection to the Cisco Cloud so that your device can participate in additional service offerings from Cisco such as technical support services, cloud management and monitoring services. Your device will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network, Cisco SecureX threat response and Cisco Defense Orchestrator. Disabling all will disconnect the device from the cloud.

Disconnection of Cisco Success Network, Cisco SecureX threat response and Cisco Defense Orchestrator will not impact the receipt of updates or operation of the Smart Licensing capabilities; such functions will continue to operate normally.

**DECLINE** **ACCEPT**

Stap 17. Terug in CDO, in het gebied van het creëren van de registratiesleutel, kies Volgende.

Stap 18. (Optioneel) Identificeer en selecteer de licenties die zijn bedoeld voor het apparaat. Selecteer vervolgens Volgende.

Stap 19. Neem de apparatenstatus in de overgang van de Inventaris van CDO van Onvoorzien aan Plaatsing waar, dan aan Syncing, en tenslotte, aan Synced.

## Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Navigeer naar de CDO portal en controleer de apparaatstatus, die Online en Synced aangeeft. Bovendien kan de verificatie van de status worden uitgevoerd via de FDM GUI. Navigeer naar **Systeem > Cloud Services** om de verbindingstatus voor Cisco Defense Orchestrator en Cisco Success Network te bekijken. De interface geeft een Connected-status weer, ter bevestiging van een succesvolle integratie met de services.

The screenshot displays the 'Cloud Services' configuration page in the Firewall Device Manager. At the top, it shows 'Device Summary' with 'Cloud Services' status as 'Connected Registered'. Below this, three service cards are visible: 'Cisco Defense Orchestrator' (Enabled), 'Cisco Success Network' (Enabled), and 'Send Events to the Cisco Cloud' (Disabled). Each card includes a 'DISABLE' button and descriptive text. The left sidebar contains a menu with categories like System Settings, Remote Management, and Cloud Services.

## Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

- Oplossing voor FQDN-fout voor cloudservice

Als de apparaatregistratie mislukt vanwege het onvermogen om de cloud service FQDN op te lossen, controleer dan de netwerkverbinding of DNS-configuratie en probeer het apparaat opnieuw aan boord te brengen.

- Ongeldige registratie-sleutelfout

Wanneer de apparaatregistratie niet is voltooid vanwege een ongeldige registratiesleutel in Firewall Device Manager, gaat u verder met het kopiëren van de juiste registratiesleutel van Cisco Defense Orchestrator en probeert u het registratieproces opnieuw. Als het apparaat al een slimme licentie heeft, verwijdert u de slimme licentie voordat u de registratiesleutel in Firewall Device Manager invoert.

- Onvoldoende licentie

In gevallen waarin de aansluitstatus van het apparaat "Onvoldoende licentie" aangeeft, gaat u verder met:

1. Laat het apparaat enige tijd vrij om de licentie te verkrijgen, aangezien Cisco Smart Software Manager een periode kan vereisen om een nieuwe licentie op het apparaat toe te passen.
2. Als de apparaatstatus ongewijzigd blijft, verfris u het CDO-portal door u uit te loggen en vervolgens opnieuw in te loggen om mogelijke netwerkcommunicatieproblemen tussen de licentieserver en het apparaat op te lossen.
3. Als de portal verfrissing de apparaatstatus niet bijwerkt, neem dan de volgende maatregelen:
  - Genereert een nieuwe registratiesleutel van [Cisco Smart Software Manager](#) en kopieert deze. Raadpleeg de [Generate Smart Licensing](#)-video voor informatie.
  - Selecteer in de navigatiebalk CDO de pagina Inventaris.
  - Kies het apparaat dat wordt vermeld met de status Onvoldoende licentie.
  - Klik in het venster Apparaatdetails op Licenties beheren onder de waarschuwing Onvoldoende licenties. Het venster Licenties beheren wordt weergegeven.
  - Plakt in het veld Activeren de nieuwe registratiesleutel en selecteer Apparaat registreren.

Nadat de nieuwe registratiesleutel met succes wordt toegepast, moet de staat van de apparatenconnectiviteit in "Online"veranderen.

Raadpleeg voor uitgebreide informatie over het registreren van Firepower Device Manager (FDM) met behulp van alternatieve methoden voor de registratiesleutel de gedetailleerde documentatie op de link [Probleemoplossing voor FDM-beheerde apparaten](#).

Deze bron biedt stapsgewijze instructies en tips voor probleemoplossing voor verschillende registratietechnieken die kunnen worden gebruikt om met succes on-board FDM naar Cisco Defense Orchestrator (CDO) te implementeren.

## Gerelateerde informatie

- [Probleemoplossing voor FDM-beheerde apparaten](#)
- [FDM-apparaten beheren met Cisco Defense Orchestrator](#)
- [Cisco Technical Support en downloads](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.