

# FDM-configuratiefout bij configuratie met hoge beschikbaarheid oplossen als gevolg van onjuiste aansluiting bij inschrijving voor cloudservices

## Inhoud

---

## uitgifte

De configuratie voor hoge beschikbaarheid (HA) mislukt tussen twee Firepower 1150-apparaten die worden beheerd door Firewall Device Manager (FDM). Het configuratieproces is niet succesvol afgerond, waardoor het instellen van een HA-paar wordt voorkomen.

De FDM UI op de primaire eenheid toont:

Firewall Device Manager | Monitoring | Policies | Objects | **Device: FTD1150-2** | admin Administrator | **SECURE**

Device Summary  
High Availability

Primary Device  
Current Device Mode: **Active** | Peer: **Disabled** | [Failover History](#) | [Deployment History](#)

One of the units has failed. Please log into the failed unit and view the failover history to determine the cause.

High Availability Configuration

Select and configure the peer device based on the following characteristics.

**GENERAL DEVICE INFORMATION**

|                       |                                     |
|-----------------------|-------------------------------------|
| Model                 | Cisco Firepower 1150 Threat Defense |
| Software              | 10.0.0-140                          |
| VDB                   | 416.0                               |
| Intrusion Rule Update | 20251124-2043                       |

**FAILOVER LINK**

|                      |                 |
|----------------------|-----------------|
| Interface            | Ethernet1/1     |
| Type                 | IPv4            |
| Primary IP/Netmask   | 192.168.10.1/24 |
| Secondary IP/Netmask | 192.168.10.2/24 |

**STATEFUL FAILOVER LINK**

The same as the Failover Link.

**Failover Criteria**

**INTERFACE FAILURE THRESHOLD**

|                                     |        |
|-------------------------------------|--------|
| Failure Criteria                    | Number |
| Number of failed interfaces exceeds | 1      |

**INTERFACE TIMING CONFIGURATION**

|                        |                         |
|------------------------|-------------------------|
| Poll Time              | Hold Time               |
| 5000                   | 25000                   |
| 500-15000 milliseconds | 5000-75000 milliseconds |

**PEER TIMING CONFIGURATION**

|                        |                        |
|------------------------|------------------------|
| Poll Time              | Hold Time              |
| 1000                   | 15000                  |
| 200-15000 milliseconds | 800-45000 milliseconds |

**SAVE**

De secundaire FTD-eenheid toont:

Firewall Device Manager

Monitoring

Policies

Objects

Device: FTD1150-3

admin Administrator

SECURE

Device Summary

High Availability

Secondary Device

Current Device Mode: Suspended Peer: Unknown

[Failover History](#)
[Deployment History](#)

Time of event: 07 Aug 2026, 12:11:39 PM

Event description: CD App Sync error FDM validation failure Active and Standby Nodes cannot have different cloud regions Check appsynhistory CLI for details

High Availability Configuration

Select and configure the peer device based on the following characteristics.

GENERAL DEVICE INFORMATION

Model

Cisco Firepower 1150 Threat Defense

Software

10.0.0-140

VDB

416.0

Intrusion Rule Update

20251124-2043

FAILOVER LINK

Interface

Ethernet1/1

Type

IPv4

Primary IP/Netmask

192.168.10.1/24

Secondary IP/Netmask

192.168.10.2/24

Failover Criteria

INTERFACE FAILURE THRESHOLD

Failure Criteria

Number

Number of failed interfaces exceeds

1

1-211

INTERFACE TIMING CONFIGURATION

Poll Time

Hold Time

5000

25000

500-15000 milliseconds

5000-75000 milliseconds

seconds

milliseconds

PEER TIMING CONFIGURATION

Poll Time

Hold Time

1000

15000

200-15000 milliseconds

800-45000 milliseconds

seconds

milliseconds

SAVE

Primaire FTD-CLI:

```
<#root>
```

```
>
```

```
show app-sync-history
```

```
=====APP SYNC HISTORY=====
-----
App Sync Time: 10:11:10 UTC Aug 07 2026
Role: Active Unit
App Sync Status: FAILURE
Failed Phase: WaitRemoteConfigApply
```

```
Failure Reason: Cluster App Un Archive failure on Standby/Slave Unit Node Id: 1 FDM validation failure -
```

Secundaire FTD-CLI:

```
<#root>
```

```
device#
```

```
show failover
```

## Failover Off (pseudo-Standby)

Failover unit Secondary  
Failover LAN Interface: failover-link Ethernet1/1 (up)  
Reconnect timeout 0:00:00  
Unit Poll frequency 1 seconds, holdtime 15 seconds  
Interface Poll frequency 5 seconds, holdtime 25 seconds  
Interface Policy 1  
Monitored Interfaces 2 of 1288 maximum  
MAC Address Move Notification Interval not set  
failover replication http

>

## show app-sync-history

=====APP SYNC HISTORY=====

App Sync Time: 10:11:06 UTC Aug 07 2026  
Role: Standby Unit  
App Sync Status: FAILURE  
Failed Phase: OnBoxValidators

**Failure Reason: FDM validation failure - Active and Standby Nodes cannot have different cloud regions.**

device#

## show failover history

| From State                              | To State     | Reason                                  |
|-----------------------------------------|--------------|-----------------------------------------|
| 08:45:29 UTC Aug 7 2026<br>Not Detected | Disabled     | No Error                                |
| 10:10:49 UTC Aug 7 2026<br>Disabled     | Negotiation  | Set by the config command<br>(failover) |
| 10:10:50 UTC Aug 7 2026<br>Negotiation  | Cold Standby | Detected an Active peer                 |
| 10:10:52 UTC Aug 7 2026<br>Cold Standby | App Sync     | Detected an Active peer                 |
| 10:11:39 UTC Aug 7 2026<br>App Sync     | Disabled     |                                         |

**CD App Sync error**

**FDM validation failure - Active and Standby Nodes cannot have different cloud regions.. Check app-sync-h**

## milieu

- Twee Firepower 1150 FTD-apparaten. Ook andere hardwareplatforms worden getroffen.
- FTD-softwareversie 7.2.8. Ook andere softwareversies worden getroffen.
- Beide FTD-eenheden worden beheerd door FDM en zijn ingeschreven in Cisco Cloud Services.

## resolutie

De oplossing houdt in dat de inschrijvingsstatus voor cloudservices tussen beide firewalls wordt afgestemd.

Primaire clouddiensten zijn geregistreerd in de Amerikaanse regio:

The screenshot displays the Cisco Firepower Device Manager (FDM) interface for device FTD1150-2. The left sidebar shows the navigation menu with 'System Settings' expanded, and 'Cloud Services' selected under 'Remote Management'. The main content area shows the 'Cloud Services' configuration page. At the top, it indicates the device is 'Connected Registered' with an 'Enrollment Type' of 'Smart Licensing' and a 'Region' of 'US Region' (highlighted with an orange box). Below this, there are three main sections: 'Security Cloud Control' (currently 'Disabled' with an 'ENABLE' button), 'Cisco Success Network' (currently 'Enabled' with a 'DISABLE' button), and 'Send Events to the Cisco Cloud' (currently 'Disabled' with an 'ENABLE' button). Each section includes a brief description of the service and its benefits.

Secundaire clouddiensten zijn geregistreerd in de EU-regio:

Firewall Device Manager | Monitoring | Policies | Objects | Device: FTD1150-3 | admin Administrator | cisco SECURE

**System Settings** ←

- Management Access
- Logging Settings
- > DHCP
- DDNS Service
- DNS Server
- Hostname
- Time Services
- SSL Settings
- HTTP Proxy
- Reboot/Shutdown
- Login Page
- Remote Management**
- Cloud Services**
- Central Management
- Traffic Settings**
- URL Filtering Preferences

Device Summary  
Cloud Services

✓ Connected Registered | Enrollment Type: Smart Licensing | Tenancy: SEC TAC and 1 Tenant | Region: EU Region

**Security Cloud Control** [ENABLE] [DISABLED]

Note: If the device is registered to cloud services using Smart Licensing, the device will not work with SCC. Please [unregister](#) the device and re-on-board using the registration key method with the "Security/SCC account" option.

Security Cloud Control allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.

**Cisco Success Network** [ENABLE] [DISABLED]

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.

**Send Events to the Cisco Cloud** [ENABLE] [DISABLED]

You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as [Cisco SecureX threat response](#), to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, this device will send high priority intrusion, file, malware events and all connection events to the Cisco cloud.

In dit geval besluit de gebruiker om de secundaire firewall (FW2) in te schrijven die overeenkomt met de primaire firewall (FW1).

## Stap 1: Schrijf FW2 in voor Cisco Cloud Services

Schrijf FW2 in bij Cisco Cloud Services met dezelfde cloudregio als FW1 (Amerikaanse regio).

Navigeer in de FW2 FDM-interface naar Apparaat > Systeeminstellingen > Cloudservices en verwijder de registratie van de cloudservices:

Firewall Device Manager | Monitoring | Policies | Objects | Device: FTD1150-3 | admin Administrator | cisco SECURE

**System Settings** ←

- Management Access
- Logging Settings
- > DHCP
- DDNS Service
- DNS Server
- Hostname
- Time Services
- SSL Settings
- HTTP Proxy
- Reboot/Shutdown

Device Summary  
Cloud Services

✓ Connected Registered | Enrollment Type: Smart Licensing | Tenancy: SEC TAC and 1 Tenant | Region: EU Region

**Security Cloud Control** [ENABLE] [DISABLED]

Note: If the device is registered to cloud services using Smart Licensing, the device will not work with SCC. Please [unregister](#) the device and re-on-board using the registration key method with the "Security/SCC account" option.

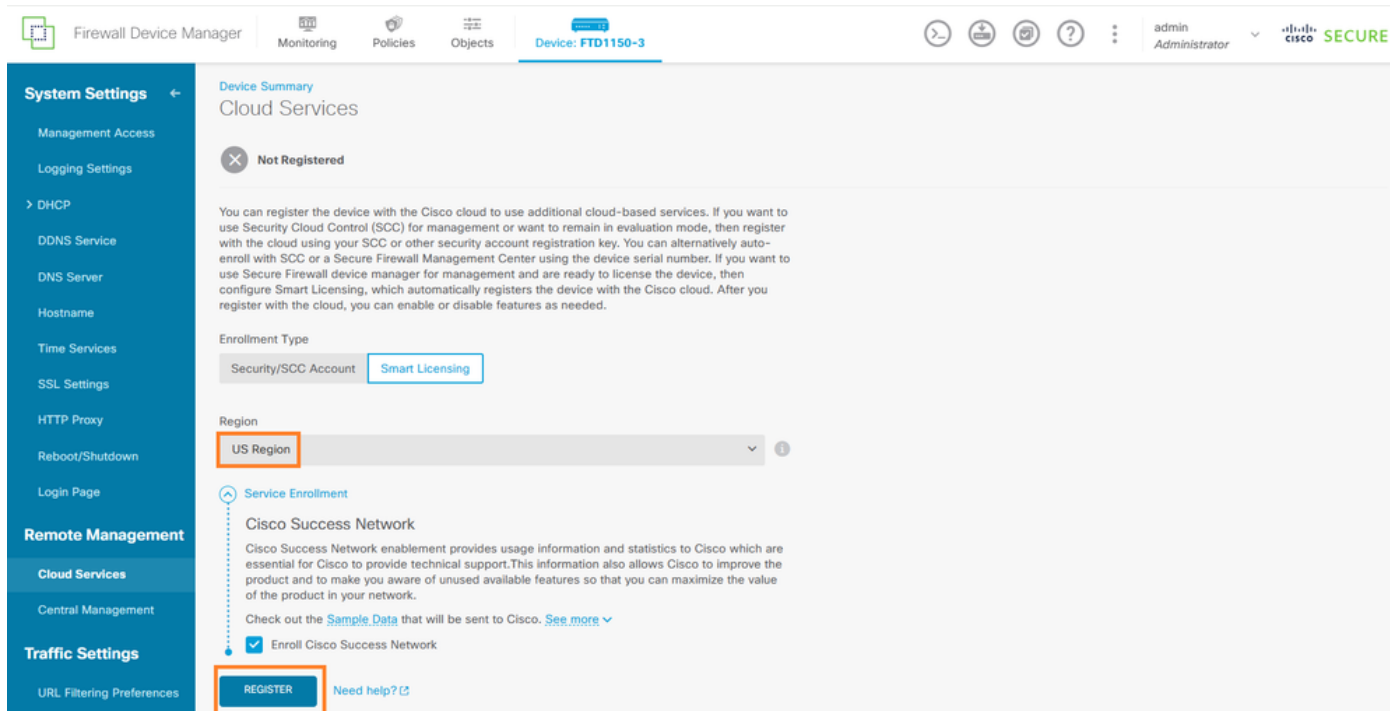
Security Cloud Control allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.

**Cisco Success Network** [ENABLE] [DISABLED]

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.

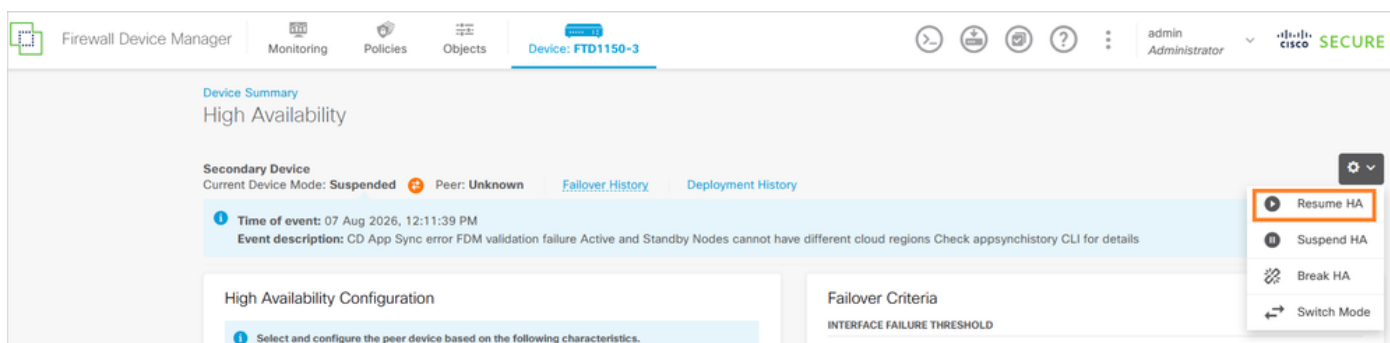
**Unregister Cloud Services**

Schrijf FW2 vervolgens in in hetzelfde gebied dat door FW1 wordt gebruikt:



## Stap 2: HA-configuratie opnieuw proberen

Nadat beide apparaten dezelfde status voor de inschrijving voor de cloud hebben, hervat u de configuratie van de HZ:



In de CLI op het secundaire apparaat ziet u:

```
<#root>
```

```
>
```

Detected an Active mate

Secondary: Switching to Ok for reason Detected an Active peer.

En een paar minuten later:

```
<#root>
```

```
device#
```

```
show failover state
```

|                              | State         | Last Failure Reason | Date/Time |
|------------------------------|---------------|---------------------|-----------|
| <b>This host - Secondary</b> |               |                     |           |
|                              | Standby Ready | None                |           |
| <b>Other host - Primary</b>  |               |                     |           |
|                              | Active        | None                |           |

====Configuration State====

**Sync Done - STANDBY**

====Communication State====

Mac set

Over het algemeen moeten beide apparaten ofwel zijn ingeschreven in dezelfde Cisco Cloud Services-regio, of beide moeten helemaal niet zijn ingeschreven.

## Oorzaak

De hoofdoorzaak is een Cisco Cloud Services inschrijving status mismatch tussen de twee Firepower 1150-apparaten. FDM blokkeert HA App Sync wanneer een node cloud-ingeschreven is en de andere niet is ingeschreven of is ingeschreven in verschillende regio's. Deze validatie zorgt ervoor dat beide apparaten in een HA-paar consistente cloudconnectiviteit en beschikbaarheid van functies behouden.

De specifieke technische oorzaak is dat FW1 was ingeschreven in de Amerikaanse regio Cisco Cloud Services, terwijl FW2 was ingeschreven in de EU-regio, wat resulteerde in een onverenigbare staat voor de vorming van HA-paren.

## Gerelateerde inhoud

- [Cisco Firepower Threat Defense Configuratiegids voor hoge beschikbaarheid](#)
- [Systeeminstellingen van Cisco Firepower Device Manager](#)
- [FTD High Availability configureren met FDM](#)
- [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.