

Troubleshoot FDM High Availability Configuration Failure Due to Cloud Services Enrollment Mismatch

Contents

Issue

High Availability (HA) configuration fails between two Firepower 1150 devices managed by Firewall Device Manager (FDM). The configuration process does not complete successfully, preventing the establishment of an HA pair.

The FDM UI on the primary unit shows:

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

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

The secondary FTD unit shows:

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 appsynchistory 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

Primary 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

Secondary 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 Not Detected	Disabled	No Error
10:10:49 UTC Aug 7 2026 Disabled	Negotiation	Set by the config command (failover)
10:10:50 UTC Aug 7 2026 Negotiation	Cold Standby	Detected an Active peer
10:10:52 UTC Aug 7 2026 Cold Standby	App Sync	Detected an Active peer
10:11:39 UTC Aug 7 2026 App Sync	Disabled	

CD App Sync error

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

=====

Environment

- Two Firepower 1150 FTD devices. Other hardware platforms are also affected.
- FTD software version 7.2.8. Other software versions are also affected.
- Both FTD units are managed by FDM and are enrolled in Cisco Cloud Services.

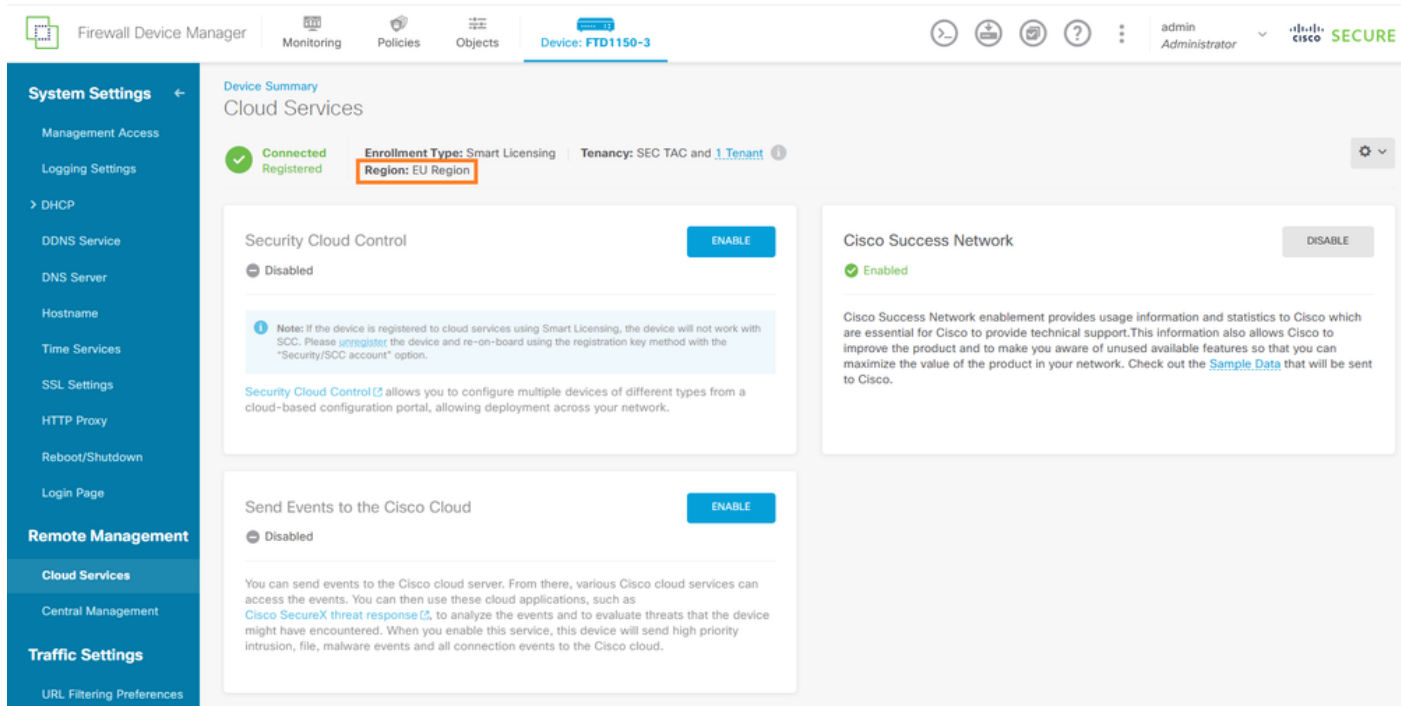
Resolution

The resolution involves aligning the cloud services enrollment status between both firewalls.

Primary cloud services is in registered in the US region:

The screenshot displays the Cisco Firewall Device Manager (FDM) interface for device FTD1150-2. The left sidebar shows the navigation menu with 'System Settings' expanded. The main content area is titled 'Device Summary' and 'Cloud Services'. The status is 'Connected Registered'. The 'Enrollment Type' is 'Smart Licensing' and the 'Region' is 'US Region' (highlighted with a red box). The 'Tenancy' is 'SEC TAC and 1 Tenant'. The 'Security Cloud Control' service is disabled, and the 'Cisco Success Network' service is enabled. The 'Send Events to the Cisco Cloud' service is also disabled.

Secondary cloud services is in registered in the EU region:

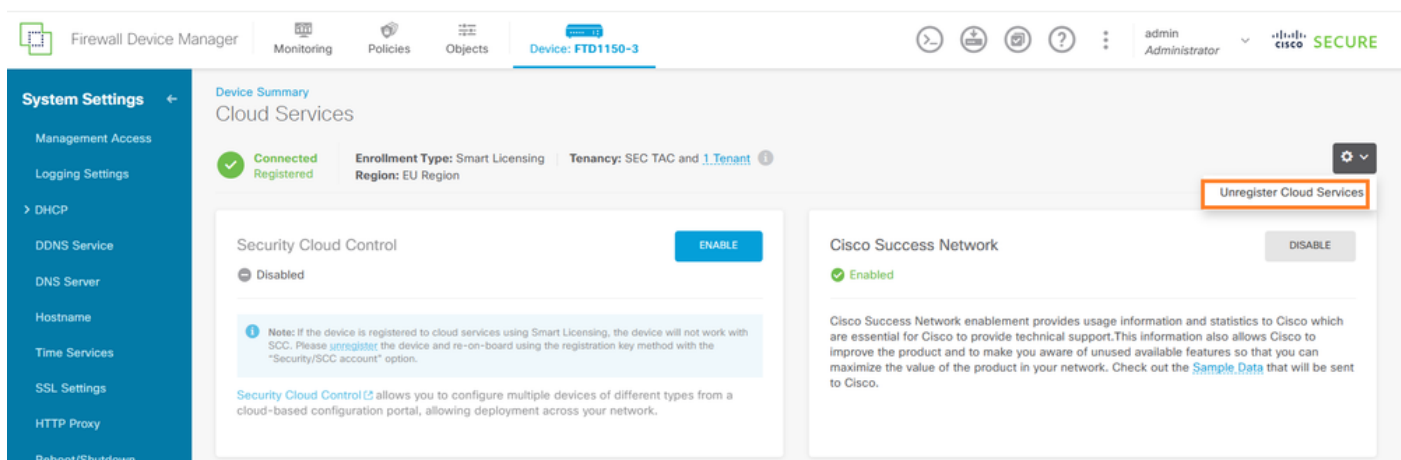


In this case, the user decides to enroll the secondary firewall (FW2) to match the primary firewall (FW1).

Step 1: Enroll FW2 in Cisco Cloud Services

Enroll FW2 into Cisco Cloud Services using the same cloud region as FW1 (US region).

In FW2 FDM interface, navigate to **Device > System Settings > Cloud Services** and unregister the cloud services:



Then, enroll FW2 to the same region used by FW1:

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

Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Security Cloud Control (SCC) for management or want to remain in evaluation mode, then register with the cloud using your SCC or other security account registration key. You can alternatively auto-enroll with SCC 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/SCC Account Smart Licensing

Region

US Region

Service Enrollment

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 2: Retry HA Configuration

After both devices show the same cloud enrollment state, resume the HA configuration:

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.

Failover Criteria

INTERFACE FAILURE THRESHOLD

Resume HA Suspend HA Break HA Switch Mode

In the CLI on the secondary device you see:

```
<#root>
```

```
>
```

Detected an Active mate

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

and a few minutes later:

```
<#root>
```

```
device#
```

```
show failover state
```

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

```
====Configuration State====
```

```
Sync Done - STANDBY
```

```
====Communication State====  
Mac set
```

In general, both devices must be either be enrolled in the same Cisco Cloud Services region, or both must not be enrolled at all.

Cause

The root cause is a Cisco Cloud Services enrollment status mismatch between the two Firepower 1150 devices. FDM blocks HA App Sync when one node is cloud-enrolled and the other is not enrolled or is enrolled in different region. This validation ensures that both devices in an HA pair maintain consistent cloud connectivity and feature availability.

The specific technical cause is that FW1 was enrolled in Cisco Cloud Services US region while FW2 was enrolled in EU region, resulting in an incompatible state for HA pair formation.

Related Content

- [Cisco Firepower Threat Defense High Availability Configuration Guide](#)
- [Cisco Firepower Device Manager System Settings Configuration](#)
- [Configure FTD High Availability Using FDM](#)
- [Cisco Technical Support & Downloads](#)