

Resolución de problemas de configuración de alta disponibilidad de FDM debido a una discordancia de inscripción de servicios en la nube

Contenido

Problema

La configuración de alta disponibilidad (HA) falla entre dos dispositivos Firepower 1150 administrados por el administrador de dispositivos de firewall (FDM). El proceso de configuración no se completa correctamente, lo que impide el establecimiento de un par HA.

La interfaz de usuario de FDM de la unidad principal muestra:

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	seconds
5000	25000	milliseconds
500-15000 milliseconds	5000-75000 milliseconds	

PEER TIMING CONFIGURATION

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

SAVE

La unidad FTD secundaria muestra:

Firewall Device Manager

Monitoring Policies Objects Device: FTD1150-3

admin Administrator

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

INTERFACE TIMING CONFIGURATION

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

PEER TIMING CONFIGURATION

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

[seconds](#) [milliseconds](#)

[seconds](#) [milliseconds](#)

[SAVE](#)

CLI de FTD principal:

<#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

CLI de FTD secundario:

<#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

Entorno

- Dos dispositivos Firepower 1150 FTD. Otras plataformas de hardware también se ven afectadas.
- Software FTD versión 7.2.8. Otras versiones de software también se ven afectadas.
- Ambas unidades de FTD son administradas por FDM y están inscritas en los servicios en la nube de Cisco.

Resolución

La resolución implica la alineación del estado de inscripción de los servicios en la nube entre ambos firewalls.

Los servicios en la nube principales están registrados en la región de EE. UU.:

The screenshot displays the Cisco Firewall Device Manager (FDM) interface for device FTD1150-2. The 'Cloud Services' section is active, showing the following configuration:

- Connected Registered:** Status is green with a checkmark.
- Enrollment Type:** Smart Licensing
- Tenancy:** SEC TAC and 1 Tenant
- Region:** US Region (highlighted with a red box)

The 'Security Cloud Control' section is currently **Disabled** (indicated by a minus icon). An **ENABLE** button is present. A note states: "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." Below this, a description of Security Cloud Control is provided.

The 'Cisco Success Network' section is currently **Enabled** (indicated by a green checkmark). A **DISABLE** button is present. A description explains that Cisco Success Network enables usage information and statistics to be sent to Cisco for technical support and product improvement.

The 'Send Events to the Cisco Cloud' section is currently **Disabled** (indicated by a minus icon). An **ENABLE** button is present. A description explains that this service allows events to be sent to the Cisco cloud server for analysis and threat detection.

Los servicios secundarios en la nube están registrados en la región de la UE:

The screenshot displays the Cisco Firewall Device Manager (FDM) interface for device FTD1150-3. The left sidebar contains the navigation menu, with 'System Settings' and 'Remote Management' sections. The 'Cloud Services' section is selected under 'Remote Management'. The main content area shows the 'Cloud Services' configuration page. At the top, the device status is 'Connected' and 'Registered'. The 'Enrollment Type' is 'Smart Licensing' and the 'Tenancy' is 'SEC TAC and 1 Tenant'. The 'Region' is 'EU Region'. Below this, there are three sections: 'Security Cloud Control' (disabled), 'Cisco Success Network' (enabled), and 'Send Events to the Cisco Cloud' (disabled). Each section has an 'ENABLE' or 'DISABLE' button. The 'Security Cloud Control' section includes a note about Smart Licensing and a link to the 'Security/SCC account' option. The 'Cisco Success Network' section includes a link to 'Sample Data'. The 'Send Events to the Cisco Cloud' section includes a link to 'Cisco SecureX threat response'.

En este caso, el usuario decide inscribir el firewall secundario (FW2) para que coincida con el firewall principal (FW1).

Paso 1: Inscriba el FW2 en los servicios en la nube de Cisco

Inscriba el FW2 en los servicios en la nube de Cisco con la misma región de nube que el FW1 (región de EE. UU.).

En la interfaz FW2 FDM, navegue hasta Device > System Settings > Cloud Services y cancele el registro de los servicios en la nube:

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] [DISABLE]

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] [DISABLE]

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

A continuación, inscriba el FW2 en la misma región que utiliza el FW1:

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

✗ **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.

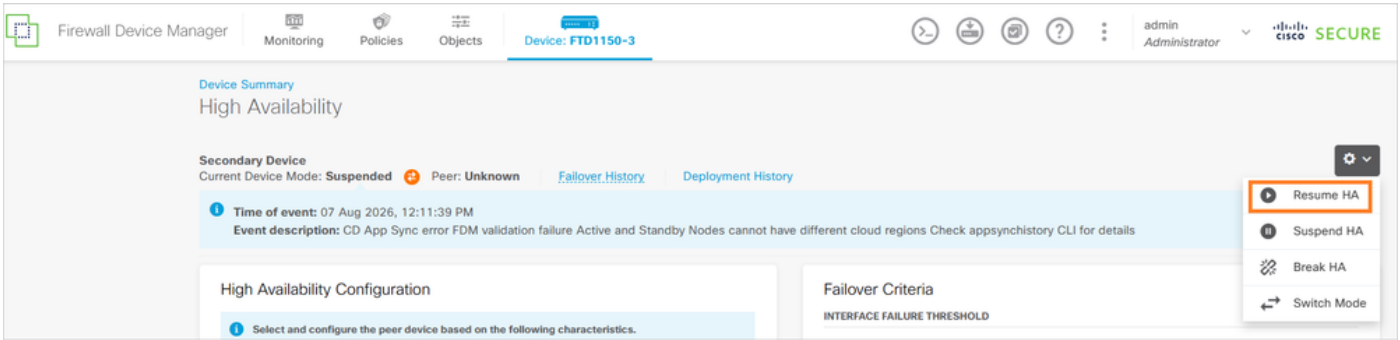
Check out the Sample Data that will be sent to Cisco. See more

☒ Enroll Cisco Success Network

REGISTER | Need help?

Paso 2: Configuración HA de reintento

Después de que ambos dispositivos muestren el mismo estado de inscripción en la nube, reanude la configuración de alta disponibilidad:



En la CLI del dispositivo secundario, verá:

```
<#root>  
>
```

Detected an Active mate

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

y unos minutos más tarde:

```
<#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
```

En general, ambos dispositivos deben estar inscritos en la misma región de servicios en la nube de Cisco o no deben estar inscritos en absoluto.

Causa

La causa principal es un error de coincidencia en el estado de inscripción de los servicios en la nube de Cisco entre los dos dispositivos Firepower 1150. FDM bloquea HA App Sync cuando un nodo está inscrito en la nube y el otro no está inscrito o está inscrito en una región diferente. Esta validación garantiza que ambos dispositivos de un par HA mantengan una conectividad uniforme con la nube y una disponibilidad de funciones.

La causa técnica específica es que el FW1 se inscribió en la región de EE. UU. de servicios en la nube de Cisco mientras que el FW2 se inscribió en la región de la UE, lo que da lugar a un estado incompatible para la formación de pares HA.

Contenido relacionado

- [Guía De Configuración De Alta Disponibilidad De Cisco Firepower Threat Defence](#)
- [Configuración del sistema del administrador de dispositivos Cisco Firepower](#)
- [Configuración de alta disponibilidad de FTD mediante FDM](#)
- [Soporte técnico y descargas de Cisco](#)

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).