

Risoluzione dei problemi di configurazione dell'alta disponibilità di FDM a causa di una mancata corrispondenza della registrazione dei servizi cloud

Sommario

Problema

La configurazione ad alta disponibilità (HA, High Availability) non riesce tra due dispositivi Firepower 1150 gestiti da Firewall Device Manager (FDM). Il processo di configurazione non viene completato correttamente. Impossibile stabilire una coppia HA.

L'interfaccia utente di FDM sull'unità primaria mostra:

Firewall Device Manager

Monitoring Policies Objects **Device: FTD1150-2**

admin Administrator

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 of failed interfaces exceeds Number: 1

INTERFACE TIMING CONFIGURATION

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

PEER TIMING CONFIGURATION

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

SAVE

L'unità FTD secondaria mostra:

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

SAVE

CLI FTD principale:

<#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 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

Ambiente

- Due dispositivi Firepower 1150 FTD. Il problema riguarda anche altre piattaforme hardware.
- Software FTD versione 7.2.8. Sono interessate anche altre versioni software.
- Entrambe le unità FTD sono gestite da FDM e sono registrate nei servizi cloud Cisco.

Risoluzione

La risoluzione prevede l'allineamento dello stato di registrazione dei servizi cloud tra entrambi i firewall.

I servizi cloud primari sono registrati negli Stati Uniti:

The screenshot displays the Cisco Firepower Device Manager (FDM) interface for device FTD1150-2. The left sidebar shows the navigation menu with categories: System Settings, Remote Management, and Traffic Settings. The main content area is titled 'Device Summary' and 'Cloud Services'. It shows the device is 'Connected' and 'Registered' with an 'Enrollment Type' of 'Smart Licensing' and a 'Region' of 'US Region' (highlighted with an orange box). Below this, there are three service cards: 'Security Cloud Control' (disabled), 'Cisco Success Network' (enabled), and 'Send Events to the Cisco Cloud' (disabled). Each card has an 'ENABLE' button. A note is present under 'Security Cloud Control' stating that Smart Licensing registration is required for SCC functionality.

I servizi cloud secondari sono registrati nella regione dell'UE:

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 [DISABLE]

Enabled

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 questo caso, l'utente decide di registrare il firewall secondario (FW2) in modo che corrisponda al firewall primario (FW1).

Passaggio 1: Registra FW2 nei servizi cloud Cisco

Registra FW2 nei servizi cloud Cisco utilizzando la stessa area cloud di FW1 (area USA).

Nell'interfaccia FW2 FDM, selezionare Device > System Settings > Cloud Services (Dispositivo > Impostazioni di sistema > Servizi cloud) e annullare la registrazione dei servizi cloud:

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
- 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** [Unregister Cloud Services]

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.

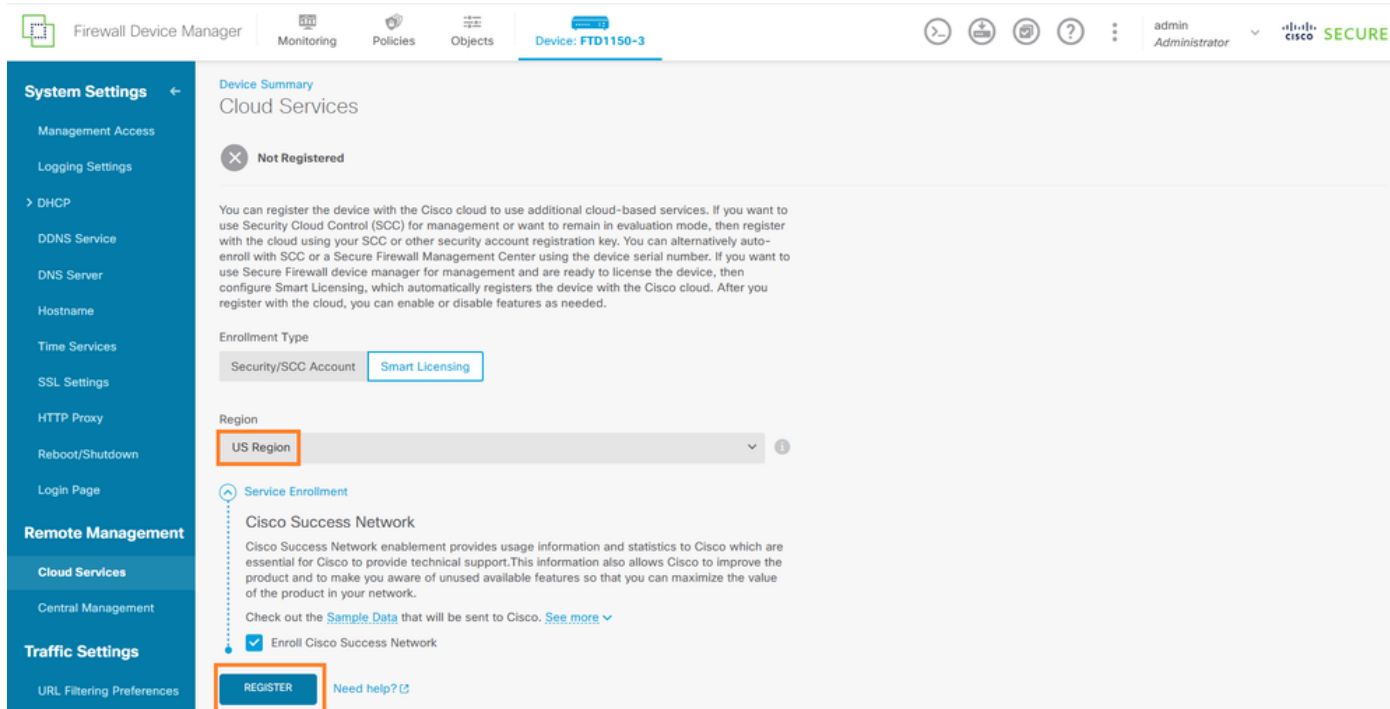
Security Cloud Control allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.

Cisco Success Network [DISABLE]

Enabled

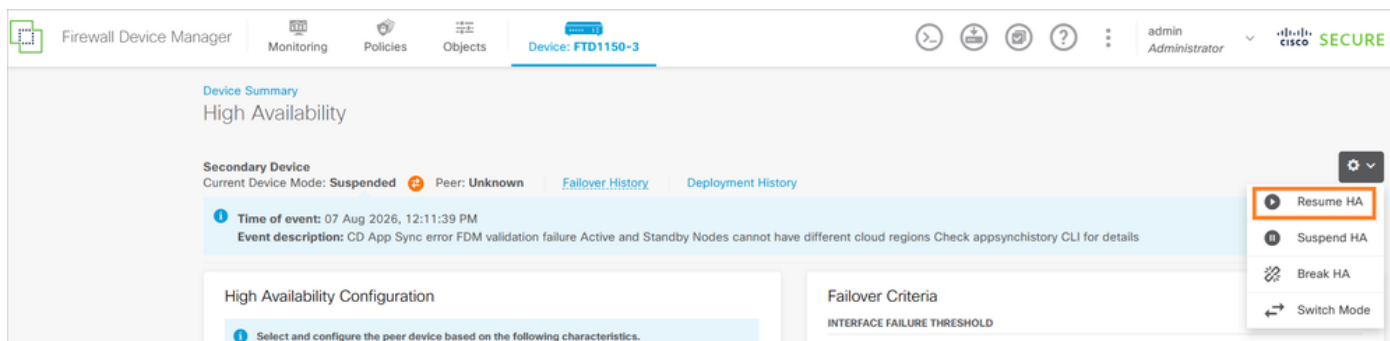
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the [Sample Data](#) that will be sent to Cisco.

Registrare quindi FW2 nella stessa area utilizzata da FW1:



Passaggio 2: Riprova configurazione HA

Dopo che entrambi i dispositivi hanno lo stesso stato di registrazione cloud, riprendere la configurazione HA:



Nella CLI del dispositivo secondario è possibile vedere:

```
<#root>
```

```
>
```

Detected an Active mate

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

e qualche minuto dopo:

```
<#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 generale, entrambi i dispositivi devono essere registrati nella stessa area servizi cloud Cisco, oppure non devono essere registrati per niente.

Causa

La causa principale è una mancata corrispondenza dello stato di registrazione dei servizi cloud Cisco tra i due dispositivi Firepower 1150. FDM blocca la sincronizzazione dell'app HA quando un nodo è registrato nel cloud e l'altro non è registrato o è registrato in un'area diversa. Questa convalida garantisce che entrambi i dispositivi in una coppia HA mantengano una connettività cloud coerente e la disponibilità delle funzionalità.

La causa tecnica specifica è che FW1 è stato registrato in Cisco Cloud Services US regione mentre FW2 è stato registrato in UE regione, con conseguente stato incompatibile per la formazione di coppia HA.

Contenuto correlato

- [Guida alla configurazione di Cisco Firepower Threat Defense High Availability](#)
- [Configurazione delle impostazioni di sistema di Cisco Firepower Device Manager](#)
- [Configura elevata disponibilità FTD tramite FDM](#)
- [Supporto tecnico Cisco e download](#)

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).