

Solucionar Problemas de Falha de Configuração de Alta Disponibilidade do FDM Devido a Incompatibilidade de Registro dos Serviços de Nuvem

Contents

Problema

A configuração de alta disponibilidade (HA) falha entre dois dispositivos Firepower 1150 gerenciados pelo Gerenciador de dispositivos de firewall (FDM). O processo de configuração não é concluído com êxito, impedindo o estabelecimento de um par HA.

A interface do usuário do FDM na unidade principal mostra:

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

A unidade secundária de FTD 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 do 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 do FTD secundário:

```
<#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

- Dois dispositivos Firepower 1150 FTD. Outras plataformas de hardware também são afetadas.
- Software FTD versão 7.2.8. Outras versões de software também são afetadas.
- As duas unidades de FTD são gerenciadas pelo FDM e estão inscritas no Cisco Cloud Services.

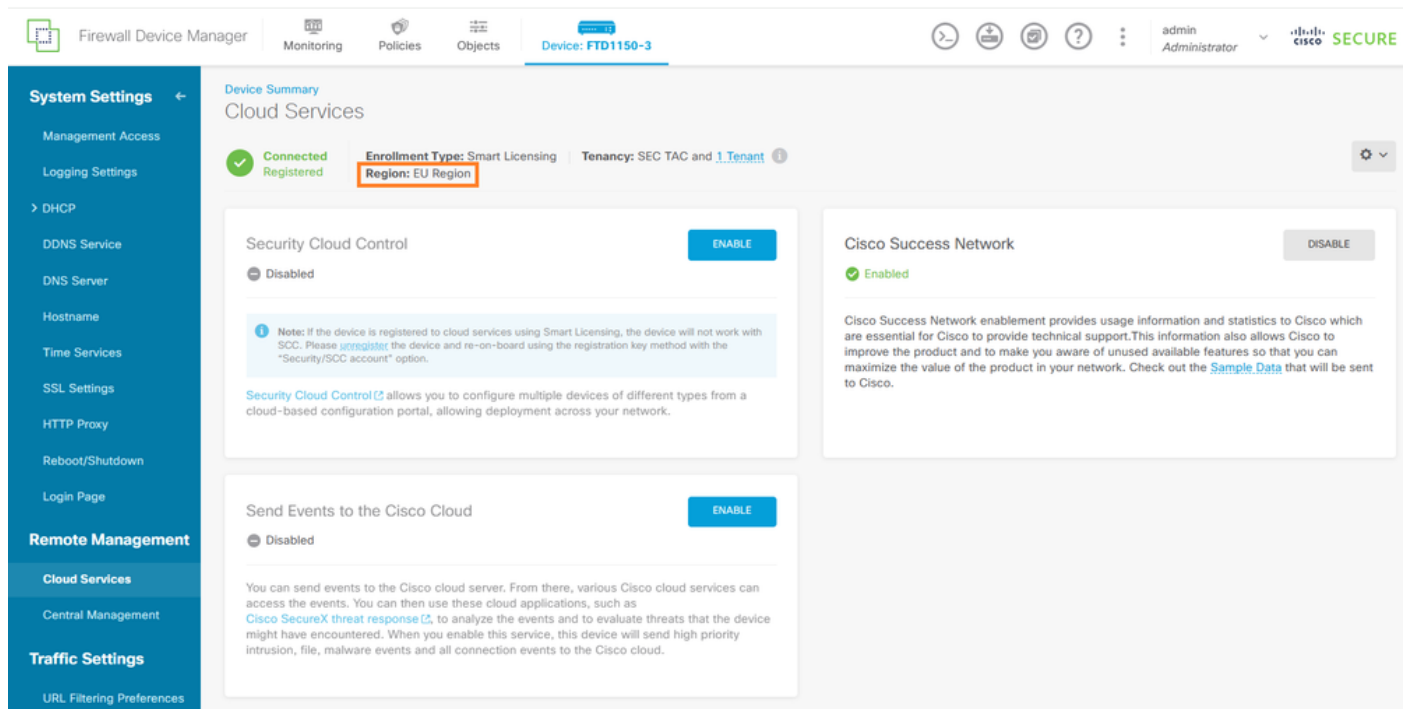
Resolução

A resolução envolve o alinhamento do status de inscrição dos serviços de nuvem entre os dois firewalls.

Os principais serviços em nuvem estão registrados na região dos EUA:

The screenshot displays the Cisco Firewall Device Manager (FDM) interface for device FTD1150-2. The left sidebar shows the navigation menu with 'System Settings' and 'Remote Management' sections. The main content area is titled 'Cloud Services' and shows the device is 'Connected' and 'Registered'. The 'Enrollment Type' is 'Smart Licensing' and the 'Region' is 'US Region'. The 'Tenancy' is 'SEC TAC and 1 Tenant'. Below this, there are three configuration 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: '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..

Os serviços em nuvem secundários estão registrados na região da UE:



Nesse caso, o usuário decide registrar o firewall secundário (FW2) para corresponder ao firewall primário (FW1).

Passo 1: Inscreva o FW2 nos serviços em nuvem da Cisco

Inscreva o FW2 nos Cisco Cloud Services usando a mesma região da nuvem que o FW1 (região dos EUA).

Na interface do FDM do FW2, navegue para Device > System Settings > Cloud Services e cancele o registro dos serviços de nuvem:

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

Unregister Cloud Services

Security Cloud Control: Disabled [ENABLE]

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: Enabled [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.

Em seguida, inscreva o FW2 na mesma região usada pelo 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.

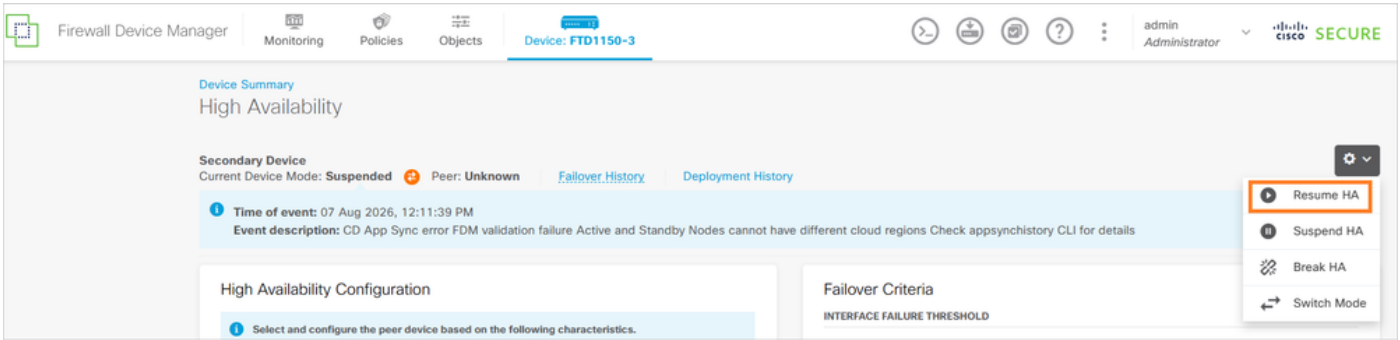
Check out the [Sample Data](#) that will be sent to Cisco. [See more](#)

☒ Enroll Cisco Success Network

REGISTER | Need help?

Passo 2: Repetir configuração de HA

Depois que os dois dispositivos mostrarem o mesmo estado de registro em nuvem, retome a configuração de HA:



Na CLI do dispositivo secundário, você verá:

```
<#root>  
>
```

Detected an Active mate

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

e alguns minutos mais 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
```

Em geral, ambos os dispositivos devem ser registrados na mesma região do Cisco Cloud Services ou não devem ser registrados.

Causa

A causa principal é uma incompatibilidade de status de inscrição dos Serviços em nuvem da Cisco entre os dois dispositivos Firepower 1150. O FDM bloqueia a Sincronização de Aplicativos HA quando um nó está inscrito na nuvem e o outro não está inscrito ou está inscrito em uma região diferente. Essa validação garante que ambos os dispositivos em um par HA mantenham conectividade de nuvem e disponibilidade de recursos consistentes.

A causa técnica específica é que o FW1 foi inscrito na região dos EUA do Cisco Cloud Services, enquanto o FW2 foi inscrito na região da UE, resultando em um estado incompatível para a formação de pares de HA.

Conteúdo relacionado

- [Guia de configuração de alta disponibilidade do Cisco Firepower Threat Defense](#)
- [Configuração das configurações do sistema do gerenciador de dispositivos Cisco Firepower](#)
- [Configurar Alta Disponibilidade de FTD Usando FDM](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.