

클라우드 서비스 등록 불일치로 인한 FDM 고가용성 컨피그레이션 오류 troubleshooting

목차

문제

FDM(Firewall Device Manager)에서 관리되는 두 개의 Firepower 1150 디바이스 간에 HA(고가용성) 컨피그레이션이 실패합니다. 컨피그레이션 프로세스가 성공적으로 완료되지 않아 HA 쌍을 설정할 수 없습니다.

기본 유닛의 FDM UI에는 다음이 표시됩니다.

The screenshot displays the FDM (Firewall Device Manager) interface for configuring High Availability (HA) on a Cisco Firepower 1150 Threat Defense device (FTD1150-2). The page is titled "High Availability Configuration" and includes a message indicating a failure: "One of the units has failed. Please log into the failed unit and view the failover history to determine the cause." The configuration details are as follows:

- 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: Number of failed interfaces exceeds 1
- Interface Timing Configuration:**
 - Poll Time: 5000 (500-15000 milliseconds)
 - Hold Time: 25000 (5000-75000 milliseconds)
- Peer Timing Configuration:**
 - Poll Time: 1000 (200-15000 milliseconds)
 - Hold Time: 15000 (800-45000 milliseconds)

A "SAVE" button is visible at the bottom of the configuration section.

보조 FTD 유닛에는 다음이 표시됩니다.

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

1-211

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

기본 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 -
```

보조 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

환경

- 2개의 Firepower 1150 FTD 디바이스. 다른 하드웨어 플랫폼도 영향을 받습니다.
- FTD 소프트웨어 버전 7.2.8. 기타 소프트웨어 버전도 영향을 받습니다.
- 두 FTD 유닛 모두 FDM에서 관리되며 Cisco Cloud Services에 등록됩니다.

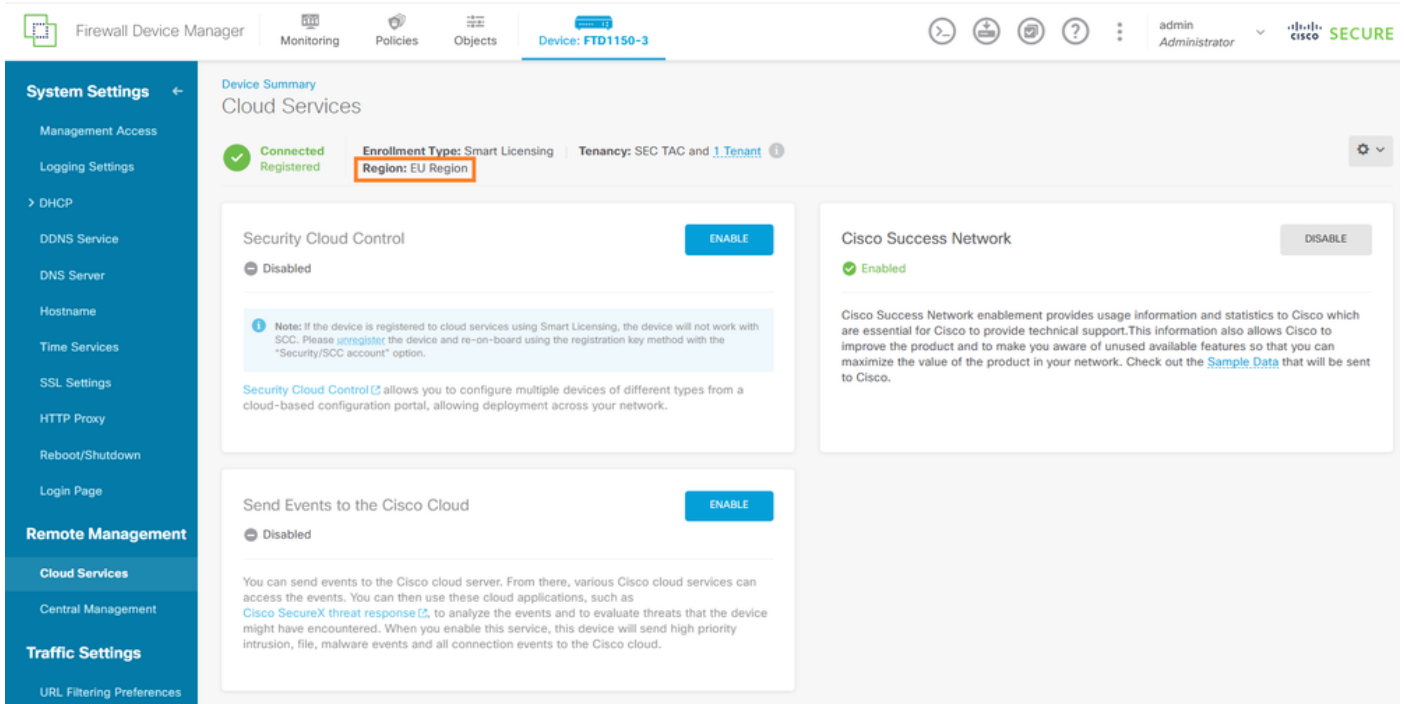
해결

이 문제를 해결하려면 양쪽 방화벽 간에 클라우드 서비스 등록 상태를 조정해야 합니다.

기본 클라우드 서비스는 미국 지역에 등록되어 있습니다.

The screenshot displays the Cisco Firepower Device Manager (FDM) interface for device FTD1150-2. The 'Cloud Services' section is active, showing a 'Connected Registered' status. The 'Enrollment Type' is 'Smart Licensing' and the 'Tenancy' is 'SEC TAC and 1.Tenant'. The 'Region' is set to 'US Region', which is highlighted with an orange box. The 'Security Cloud Control' is currently 'Disabled', and the 'Cisco Success Network' is 'Enabled'. The 'Send Events to the Cisco Cloud' is also 'Disabled'. A note indicates that if the device is registered to cloud services using Smart Licensing, it will not work with SCC unless the 'unregister' option is used. The interface also includes a sidebar with various settings categories and a top navigation bar with icons for monitoring, policies, and objects.

보조 클라우드 서비스는 EU 지역에 등록되어 있습니다.

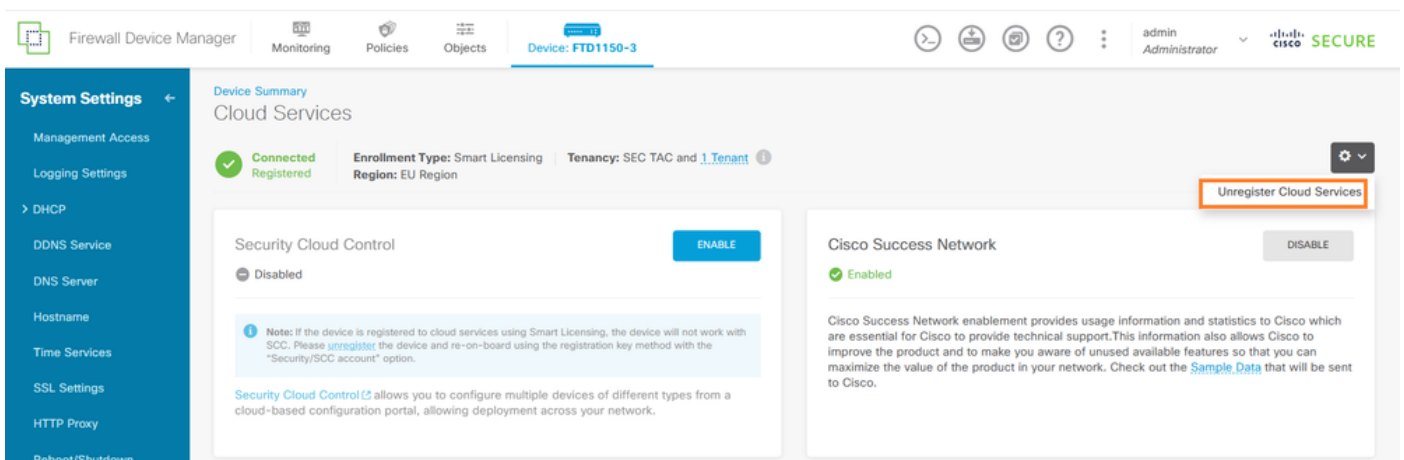


이 경우, 사용자는 기본 방화벽(FW1)과 일치하도록 보조 방화벽(FW2)을 등록하기로 결정한다.

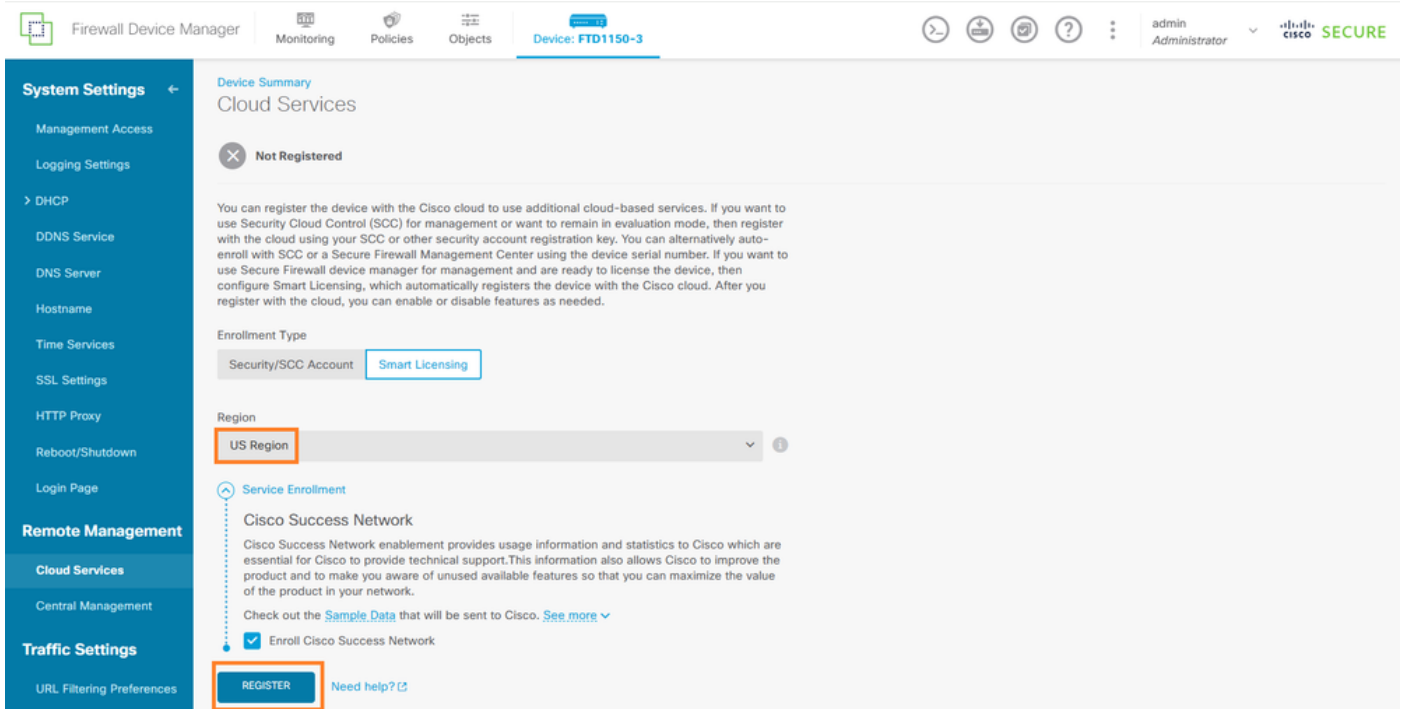
1단계: Cisco 클라우드 서비스에 FW2 등록

FW1과 동일한 클라우드 리전(미국 리전)을 사용하여 FW2를 Cisco 클라우드 서비스에 등록합니다.

FW2 FDM 인터페이스에서 Device(디바이스) > System Settings(시스템 설정) > Cloud Services(클라우드 서비스)로 이동하고 클라우드 서비스의 등록을 취소합니다.

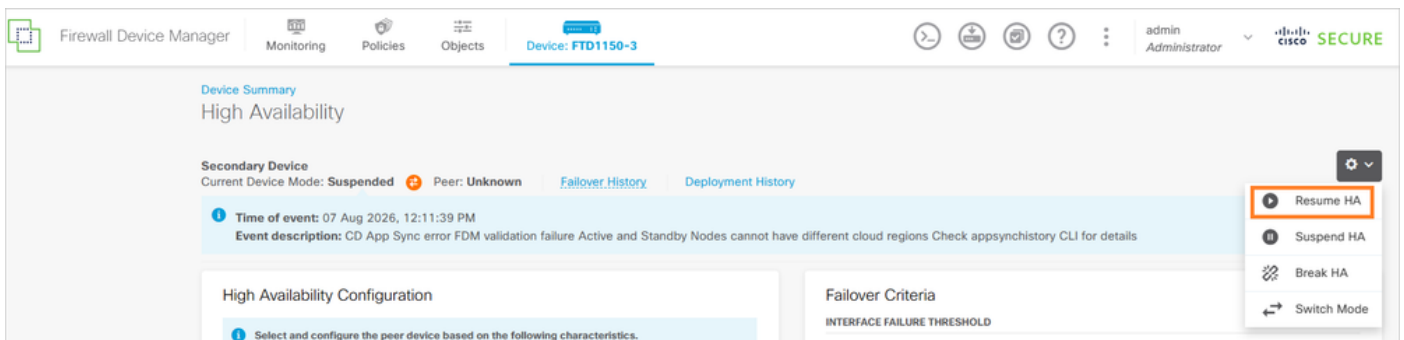


그런 다음 FW2를 FW1에서 사용하는 동일한 지역에 등록합니다.



2단계: HA 컨피그레이션 다시 시도

두 디바이스 모두 동일한 클라우드 등록 상태를 표시하면 HA 컨피그레이션을 다시 시작합니다.



보조 디바이스의 CLI에서 다음을 볼 수 있습니다.

```
<#root>
```

```
>
```

```
Detected an Active mate
```

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

몇 분 후:

<#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

일반적으로 두 디바이스 모두 동일한 Cisco 클라우드 서비스 지역에 등록하거나 둘 다 등록해서는 안 됩니다.

원인

근본 원인은 두 Firepower 1150 디바이스 간의 Cisco Cloud Services 등록 상태가 일치하지 않기 때문입니다. FDM은 한 노드가 클라우드 등록되고 다른 노드가 등록되지 않거나 다른 지역에 등록되어 있는 경우 HA App Sync를 차단합니다. 이러한 검증을 통해 HA 쌍의 두 디바이스 모두 일관된 클라우드 연결 및 기능 가용성을 유지할 수 있습니다.

구체적인 기술적 원인은 FW1이 Cisco Cloud Services US 지역에 등록되어 있는 반면 FW2는 EU 지역에 등록되어 HA 쌍 형성에 호환되지 않는 상태가 되었기 때문입니다.

관련 콘텐츠

- [Cisco Firepower Threat Defense 고가용성 구성 설명서](#)
- [Cisco Firepower 장치 관리자 시스템 설정 구성](#)
- [FDM을 사용하여 FTD 고가용성 구성](#)
- [Cisco 기술 지원 및 다운로드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.