

Troubleshoot High-Availability Pairing Failure on FDM

Contents

Issue

High Availability (HA) pairing between two Cisco Firepower 1120 appliances running FTD 7.4.2.4 fails during application synchronization with the secondary node consistently entering a Failed state due to a license registration mode mismatch. The specific error message encountered is:

```
CD App Sync error FDM validation failure License registration mode mismatch between Primary and Secondary
```

The **show app-sync-history** command reveals repeated failures with messages such as:

```
App Sync Status: FAILURE
```

```
Failed Reason: FDM validation failure - License agent compliance mismatch between Primary and Secondary
```

This issue occurred after both firewalls were reset, configurations restored from backup, software updated to FTD version 7.4.2.4, VDB and Snort versions updated, and licenses reapplied with fresh tokens. The secondary firewall remains in a Failed state, preventing HA completion and impacting firewall redundancy.

Environment

- Cisco Firepower 1120 NGFW Appliances configured for High Availability
- Firepower Threat Defense (FTD) version 7.4.2.4-9
- Snort inspection engine: 3.1.53.203 - 175
- VDB: 425.0
- Geolocation database: 2026-03-07-053
- Devices converted from Smart Licensing to PLR (Permanent License Reservation) mode

- Primary device attempting cloud connectivity after PLR conversion
- Both devices restored from the backup

Resolution

The resolution involves identifying and correcting the license registration mode mismatch between the primary and secondary devices, performing cloud deregistration, and completing a full deployment.

Step 1: Identify the License Registration Mode Mismatch

Verify the license registration mode on both devices by checking the app-sync-history for specific failure reasons:

```
show app-sync-history
```

The output shows failures indicating:

```
FDM validation failure - License registration mode mismatch between Primary and Secondary node
```

Step 2: Perform Cloud Deregistration

Since the primary device was still attempting cloud connectivity after conversion from Smart Licensing to PLR mode, cloud deregistration is required.

Configure a temporary proxy in the FDM UI (if no proxy is configured):

Navigate to **System Settings > See More > HTTP Proxy tab** and configure a dummy proxy temporarily [this can be removed later].

SSH into the FTD device and execute the connector script:

```
ssh admin@<device-ip>
```

```
expert
sudo su
/ngfw/var/sf/bin/connector.sh
```

Step 3: Resolve Port 8989 Conflict

If the connector script fails with this error:

```
Error: listen tcp :8989: bind: address already in use
```

Identify and terminate the process using port 8989 (typically Cisco Success Network):

```
netstat -tulpn | grep 8989
kill <pid>
```

Step 4: Complete Cloud Deregistration

Re-run the connector script after resolving the port conflict:

```
/ngfw/var/sf/bin/connector.sh
```

The successful execution must show output similar to:

```
Starting connector
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: https_proxy=http://1xx.xx.x
INFO[0000] [firepower][functions.go:162 common:LogEnv] Environment variable: http_proxy=http://1xx.xx.x
```

Go to FDM GUI, System Settings > Cloud Services > Cloud Services and click on unregister option. Verify the device is unregistered from cloud services.

Step 5: Perform Full Deployment and Resume HA

After cloud deregistration, if HA pairing still fails with the same license mismatch error, perform a full deployment on the active unit through the FDM interface.

Navigate to **Deploy > Deploy Now** and complete the deployment process.

Once deployment is complete, retry HA formation. The devices must successfully form an Active-Standby HA pair with interfaces connected and in a ready state.

Step 6: Verify HA Status

Confirm successful HA formation:

```
show failover
```

The output must show both units in proper HA states with successful synchronization.

Cause

The root cause was a license registration mode mismatch between the primary and secondary Firepower 1120 devices. The devices had been converted from Smart Licensing to PLR (Permanent License Reservation) mode; however, the primary device continued attempting cloud connectivity, leading to a mismatch in license agent/export compliance state during HA validation. This resulted in repeated FDM/FIM validation failures during application synchronization. Additionally, cloud deregistration was initially blocked by a port 8989 conflict related to Cisco Success Network, which required resolution before deregistration could proceed.

Related Content

- [Apply Permanent Licenses in Air-Gapped Networks](#)
- [Reimage a Secure Firewall Threat Defense](#)
- [Cisco Technical Support & Downloads](#)