Resolve Webex Calling Survivability Gateway Sync Failure Due to Unsupported GoDaddy R1 Certificate Chain

Contents

Issue

Two Survivability Gateways (mcyitsrtr001.centralwire.com and prtitsrtr001.centralwire.com) were registered in Control Hub but failed to synchronize; troubleshooting focused on mcyitsrtr001.centralwire.com. Sync attempts failed consistently with the error message:

```
Sync failed due to internal server error (code - 31117)
```

First observed during a sync attempt on August 5, 2026. Analysis of telemetry and Webex backend (pylon) logs revealed that the gateway was presenting a GoDaddy R1v1 certificate chain (GoDaddy TLS Root CA - R1 hierarchy), which is not supported by Webex services, causing the certificate chain to be rejected and synchronization to fail.

Environment

- Two managed gateways reported: mcyitsrtr001.centralwire.com and prtitsrtr001.centralwire.com (troubleshooting focused on mcyitsrtr001.centralwire.com)
- IOS® XE Version: 17.12.6 (SGW node), 17.15.06 (MGW)
- Webex Calling Survivability Gateway (SGW) configuration
- GoDaddy TLS certificate chain using R1v1 intermediate CA
- Certificate chain: CN=mcyitsrtr001.centralwire.com → GoDaddy TLS Intermediate CA DV - R1v1 → GoDaddy TLS Root CA - R1

Resolution

The issue was resolved by implementing a certificate cross-signing workaround to establish a trusted certificate path. The solution involved installing the GoDaddy R1-to-G2 cross-signed certificate to chain the newer GoDaddy R1 hierarchy to the trusted Go Daddy Root Certificate Authority - G2.



Note: During the certificate changes, the **crypto pki trustpool import clean** command disrupted the gateway's NETCONF-YANG/DMI service, briefly taking the connector offline. `Could not open socket to 192.168.217.55:830`). This was recovered via Steps 6–7 and was a side-effect of the maintenance, not the original sync failure.

Step 1: Install Cisco Trustpool Bundle

Install the **Cisco trustpool bundle** which contains the Go Daddy Root Certificate Authority - G2:

```
crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_union.p7b
```

`import clean` replaces the entire trustpool — it can disrupt services that depend on it (see the connector-offline note listed previously). Use with care.

Step 2: Verify G2 Root Certificate

Confirm that Go Daddy Root Certificate Authority - G2 is present:

```
show crypto pki trustpool | include GoDaddy|Go Daddy
```

Step 3: Remove Self-Signed R1 Trustpoint

Remove the old s**elf-signed R1 trustpoint** (answer **yes** when prompted to remove certificates):

```
no crypto pki trustpoint GoDaddyRootR1
```

Step 4: Install Cross-Signed R1 Certificate

Create a **new trustpoint** with the cross-signed R1 certificate (Subject: GoDaddy TLS Root CA - R1, Issuer: Go Daddy Root Certificate Authority - G2):

```
crypto pki trustpoint GoDaddyCrossR1
enrollment terminal
revocation-check none
exit
crypto pki authenticate GoDaddyCrossR1
<paste cross-signed R1 PEM — Subject: GoDaddy TLS Root CA - R1, Issuer: Go Daddy Root Certificate Autho
quit
yes
```

Step 5: Verify Certificate Chain

Verify that the chain now resolves correctly:

```
show crypto pki certificates webex-sgw
show crypto pki certificates GoDaddyCrossR1
```

Step 6: Restart NETCONF Services

Bounce HTTP(S) server and NETCONF-YANG services (wait approximately 60 seconds between disable and enable):

```
conf t
no netconf-yang
no ip http secure-server
no ip http server
end
```

Wait 60 seconds, then re-enable:

```
conf t
ip http server
ip http secure-server
```

```
netconf-yang
end
write memory
```

Step 7: Reload Gateway (If Necessary)

If NETCONF-YANG still does not serve properly after the service restart, reload the router to fully re-initialize DMI:

```
reload
```

Caution: Possible. The details mentioned here appears to contain procedures or commands that could cause significant impact if executed. Please ensure the above procedures or commands have been evaluated by an SME or Business Unit before executing or recommending.

Step 8: Verify Resolution

After the gateway comes back online, trigger an SGW resync from Control Hub and verify that the sync completes successfully without error code 31117 or "Certificate Server Trusted check failed" messages. **Confirmed resolved** — the gateway presented the full leaf → R1v1 → R1 (issuer G2) chain and the sync completed successfully after the cross-sign workaround.

Cause

The root cause was identified as a certificate trust failure. The Survivability Gateway was presenting a certificate chain using the GoDaddy TLS Root CA – R1 hierarchy (specifically the GoDaddy TLS Intermediate CA DV - R1v1), which is not included in Webex Calling's trusted certificate authority list.

When the Webex backend (pylon) performed a server-certificate trust check during the SIP authentication information request, it could not build a valid certification path to a trusted root certificate. This resulted in a SunCertPathBuilderException with the error "unable to find valid certification path to requested target," causing the HTTP 400 response and sync abortion.

Webex Calling trusts only the older GoDaddy/Starfield roots (such as Go Daddy Root Certificate Authority - G2) but not the newer "GoDaddy TLS" (R1/R1v1) hierarchy.

Related Content

- Supported Certificate Authorities for Webex Hybrid Services
- GoDaddy Certificate Repository
- Cisco Technical Support & Downloads