Webex Calling Survivability Gateway Certificate Chain Compatibility Issue

Contents

Issue

When configuring Webex Calling Survivability and enabling test mode in the Control Hub, the gateway fails to synchronize with Webex Cloud servers. The **show voice register session** command does not display the expected registration behavior, and the Control Hub shows synchronization failures.

The telemetry logs display this error during synchronization attempts:

```
2026-08-12T19:22:58.745Z - ERROR - Thread-5 (handle_sgw_events) - wxcc_sgw_manager : TELEMETRYLOG : WxC
```

The gateway fails to establish a secure TLS connection with Webex Cloud for the configured location, preventing proper synchronization and registration of the survivability gateway.

Environment

- Webex Calling Survivability Gateway Configuration
- IOS XE Software Version 17.12.6
- GoDaddy TLS Certificates Installed on the Gateway
- Certificate Chain using GoDaddy TLS Intermediate CA DV - R1v1
- Control Hub Survivability Configuration with Test Mode Enabled

Resolution

This issue was resolved by replacing the certificate with one that uses a supported certificate authority chain.

The problematic certificate was using the newer GoDaddy R1v1 certificate chain, which is not supported by Webex Calling platforms.

Step 1: Verify Current Certificate Chain

Check the currently installed certificates on the gateway:

```
device# show crypto pki certificates
```

The output displays the problematic certificate chain:

<#root>

```
Certificate
  Status: Available
  Certificate Serial Number (hex): 00923AC809A58436DD
  Certificate Usage: General Purpose
  Issuer:
```

cn=GoDaddy TLS Intermediate CA DV - R1v1

```
    o=GoDaddy.com
    c=US
  Subject:
    Name: mhtlc-ls-r1.mhtlc.org
```

cn=mhtlc-ls-r1.mhtlc.org

```
  CRL Distribution Points:
    http://crl.godaddy.com/gdr1v1dv_s1-7.crl
  Validity Date:
    start date: 13:43:39 CDT Jun 25 2026
    end   date: 12:43:39 CST Jan 9 2027
  Associated Trustpoints: webex-sgw
  Storage: nvram:GoDaddyTLSIn#36DD.cer
```

Step 2: Identify Certificate Chain Compatibility Issue

The certificate analysis revealed the gateway was using a certificate signed by **GoDaddy TLS Intermediate CA DV - R1v1**. The cross certificate **(GoDaddy TLS Root CA - R1)** and root certificate **(Go Daddy Root Certificate Authority - G2)** was missing from the gateway.

Webex Calling only supports certificates with the "GoDaddy" root certificate authority per official documentation.

- **CN=Go Daddy Root Certificate Authority - G2**

Step 3: Request New Certificate with Supported Chain

Contact the certificate provider (GoDaddy) to re-key the certificate and ensure it uses the supported certificate chain:

- Request a new certificate for the same domain FQDN (mhtlc-ls-r1.mhtlc.org).
- Specify the certificate must use the **GoDaddy G2 (SHA-2)** certificate chain.
- Ensure all relevant certificates for a complete chain of trust are installed on the SGW router.

Step 4: Install the New Certificate

Once the new certificate with the supported G2 chain is obtained, install it on the survivability gateway and configure the appropriate trustpoint for Webex connectivity.

Perform this step if a publicly known CA root certificate is unavailable with your Cisco IOS XE gateway.

```
crypto pki trustpoint <CA name>
 enrollment terminal
 revocation-check crl
 crypto pki authenticate <CA name>
```

Step 5: Verify Resolution

After installing the new certificate, test the survivability gateway registration:

- Monitor the synchronization process in Control Hub.
- Verify successful registration by running the **show voice register session** command.
- Ensure the telemetry logs no longer show TLS connection failures.

Cause

The root cause was the certificate chain incompatibility between the survivability gateway and Webex

Calling cloud services. The gateway was configured with a certificate signed by **GoDaddy TLS Intermediate CA DV - R1v1**, which is part of the newer corss GoDaddy R1 certificate chain.

Webex Calling only supports certificates that chain up to the **Go Daddy Root Certificate Authority - G2**. The newer R1v1 intermediate certificate authority introduced by GoDaddy is not included in Webex Callings trusted certificate authority list, causing TLS handshake failures during the survivability gateway synchronization process. Additionally, the missing root certificate on the gateway prevented proper certificate chain validation, contributing to the secure connection establishment failures.

Related Content

- What Root Certificate Authorities are Supported for Calls to Cisco Webex Audio and Video Platforms
- Cisco Technical Support & Downloads
- Site Survivability for Webex Calling