
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Enabling and Troubleshooting Encrypted Calling Between UCM and Webex Calling

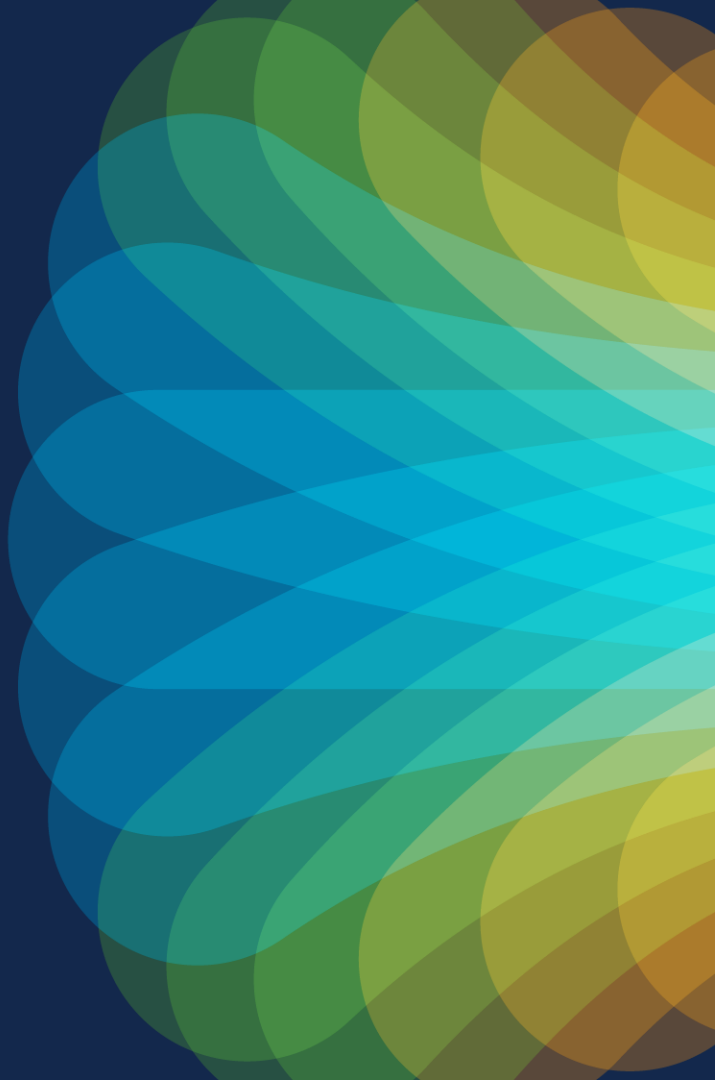
Michael Huang – Customer Delivery Engineering Technical Leader
Jamie Wang – Technical Consulting Engineer

BRKCOL-2197

Agenda

- Introduction
- Secure Connections
- Securing LGW with UCM
- Securing IP Phones
- Troubleshooting Secure Connections

Introduction



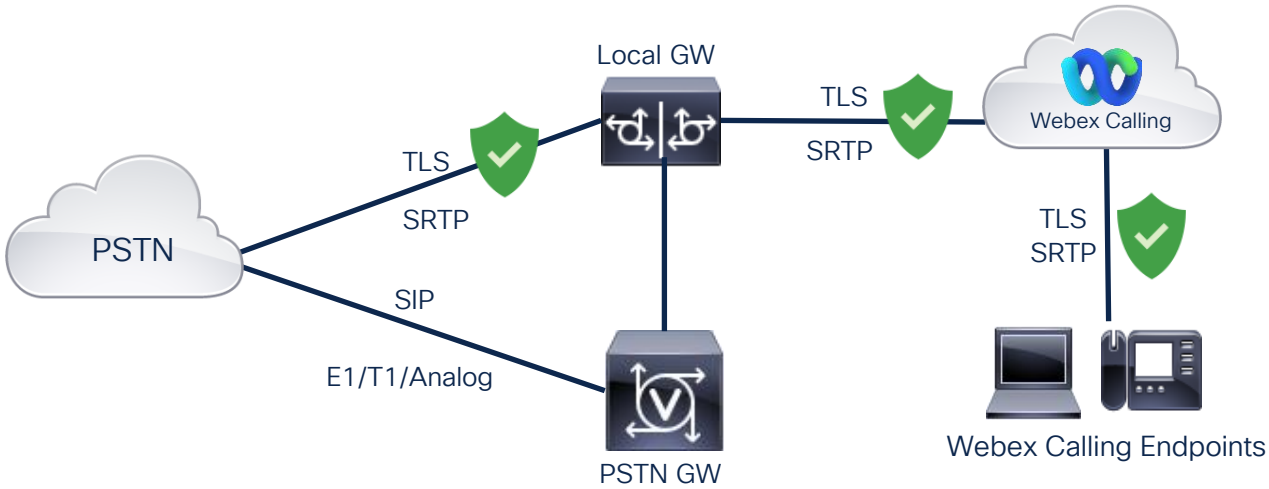
UCM with Webex Calling Deployment Models

- Moving from on-premise UCM to Webex Calling begins with setting up a Local Gateway (LGW) to establish a connection between Webex Calling and UCM.
- Three deployment models for deploying Local Gateway with Webex Calling
  - Standalone Local Gateway
  - Co-located PSTN Gateway with Local Gateway and UCM
  - Local Gateway and separate PSTN gateway with UCM

UCM with Webex Calling Deployment Models

Standalone Local Gateway

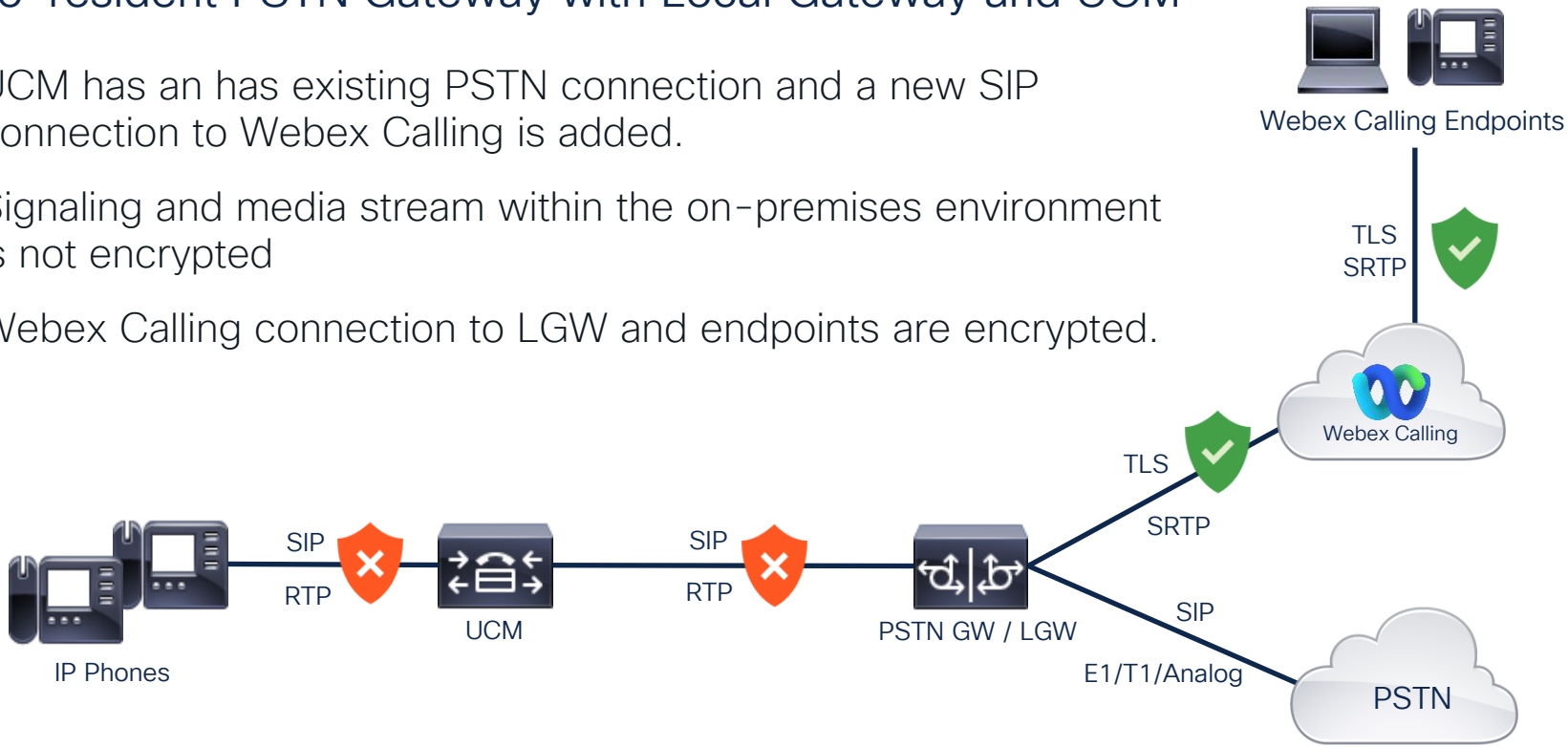
- Local Gateway (LGW) routes calls from Webex Calling to the local PSTN via a SIP trunk or leverages an existing PSTN gateway to go PSTN.
- This model has no UCM/IP PBX involved and Local GW has a secure connection to Webex Calling.



UCM with Webex Calling Deployment Models

Co-resident PSTN Gateway with Local Gateway and UCM

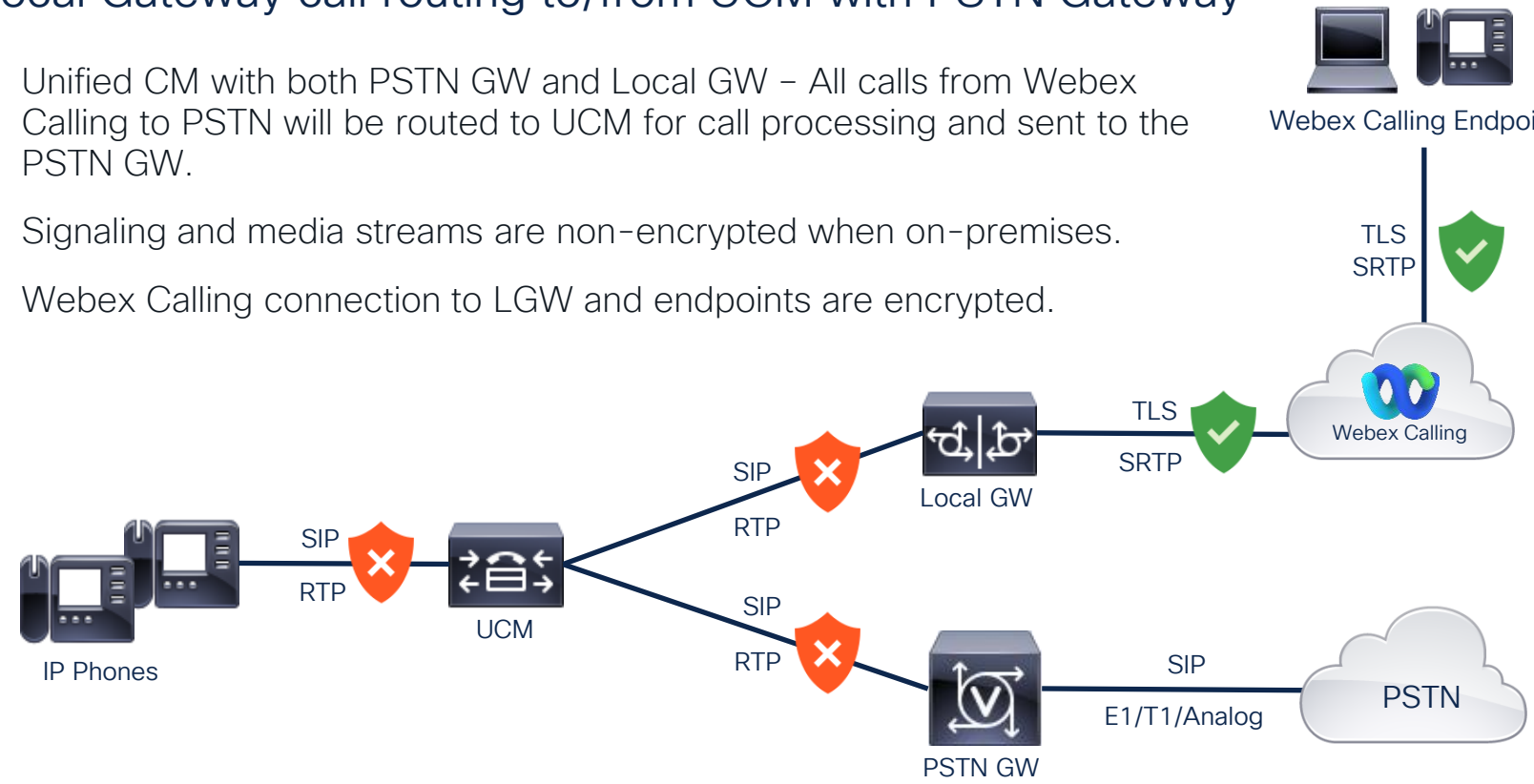
- UCM has an has existing PSTN connection and a new SIP connection to Webex Calling is added.
- Signaling and media stream within the on-premises environment is not encrypted
- Webex Calling connection to LGW and endpoints are encrypted.



UCM with Webex Calling Deployment Models

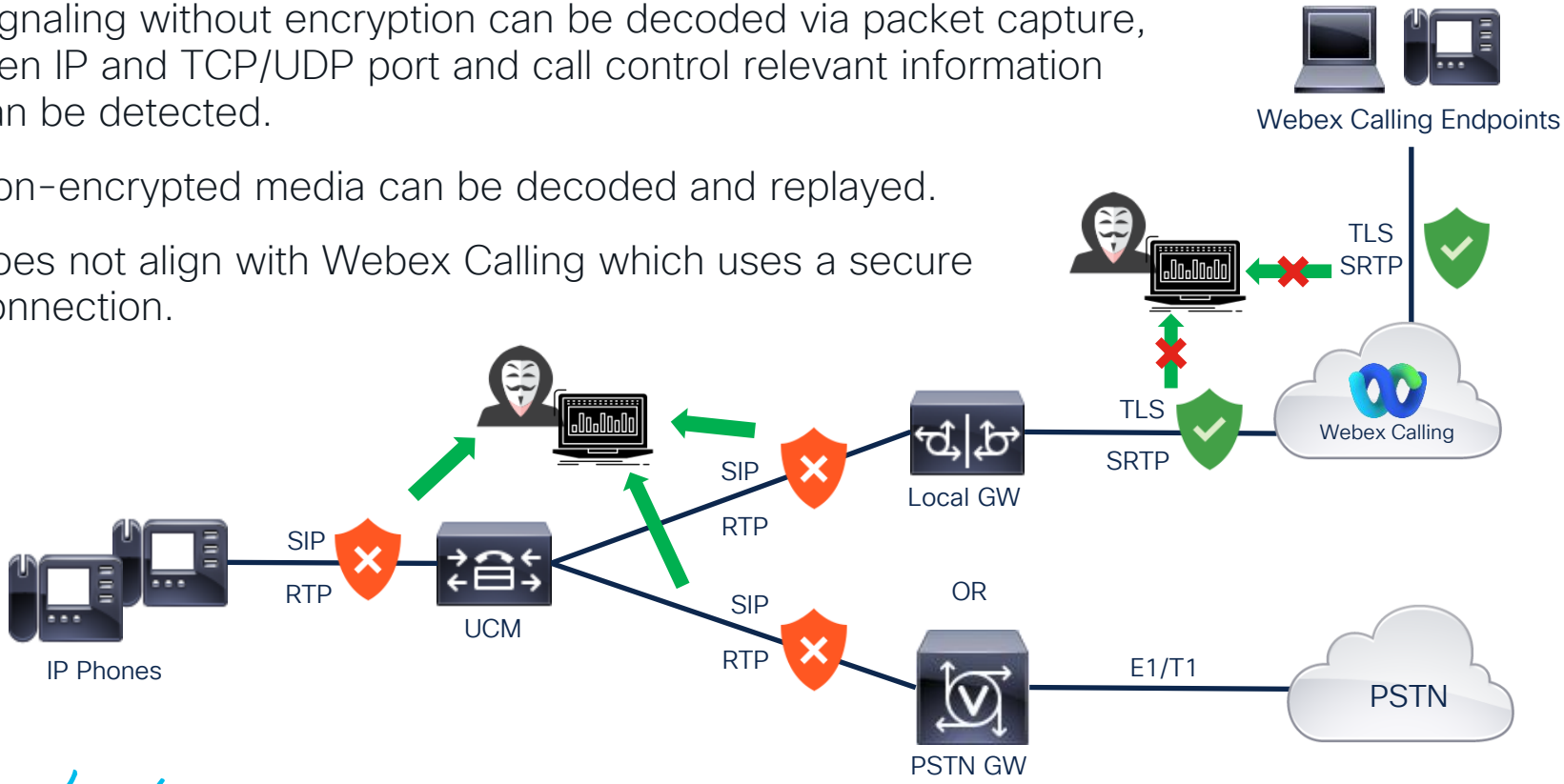
Local Gateway call routing to/from UCM with PSTN Gateway

- Unified CM with both PSTN GW and Local GW – All calls from Webex Calling to PSTN will be routed to UCM for call processing and sent to the PSTN GW.
- Signaling and media streams are non-encrypted when on-premises.
- Webex Calling connection to LGW and endpoints are encrypted.



Potential Threats from Non-Secure Connections

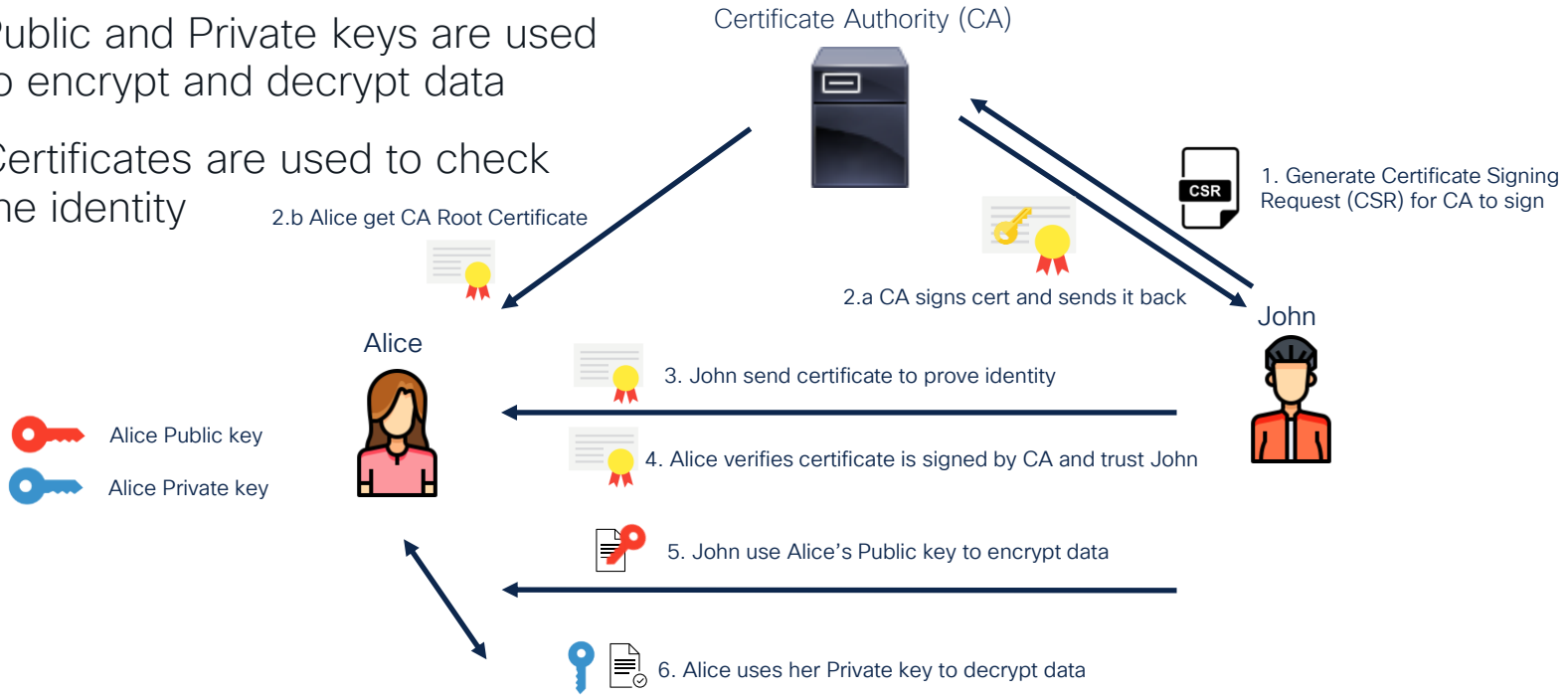
- Signaling without encryption can be decoded via packet capture, then IP and TCP/UDP port and call control relevant information can be detected.
- Non-encrypted media can be decoded and replayed.
- Does not align with Webex Calling which uses a secure connection.



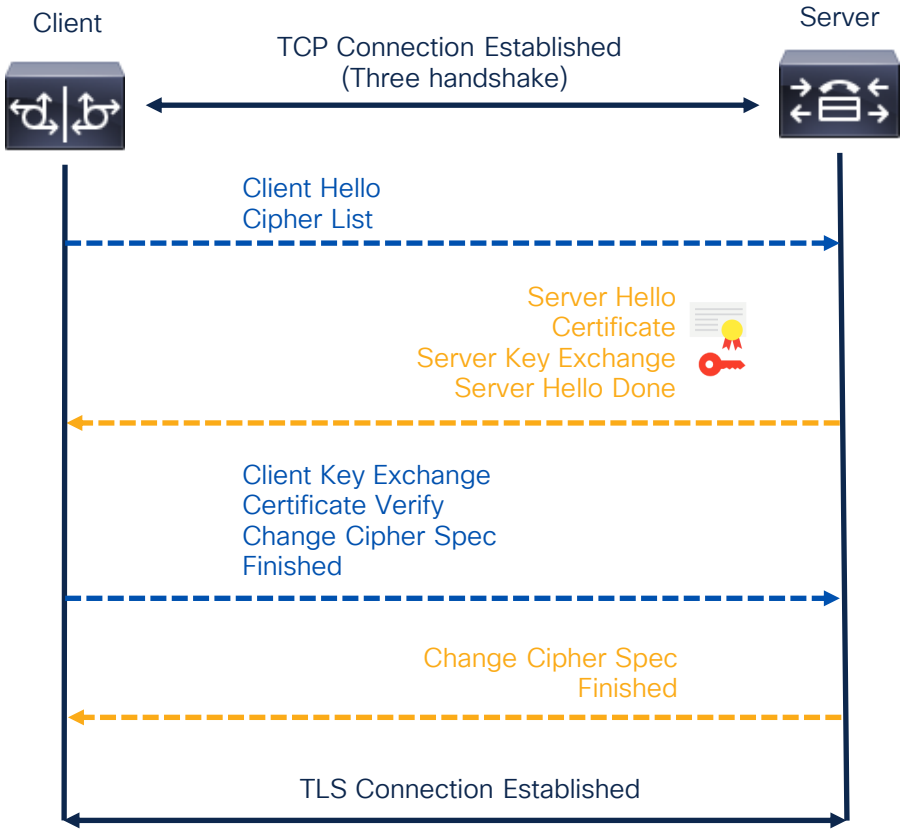
Secure Connections Introduction

Public / Private Keys & Certificates

- Public and Private keys are used to encrypt and decrypt data
- Certificates are used to check the identity



TLS Connection Establishment



Secure LGW with UCM

Verify UCM Security Mode

Unified CM provides two security for phones and endpoints:

- Non-Secure mode is the default mode after installation and does not provide secure signaling or media services.
- Secure mode (Mixed mode) supports secure IP Phones and endpoints.

In order to verify if UCM is in non-secure or secure mode, navigate to:

Unified CM Administration → Enterprise Parameters → Check 'Cluster Security Mode'

1 = Secure / Mixed mode 0 = Non-Secure mode

UCM Mixed Mode

In order to move the UCM cluster security into Mixed mode with the use of CTL feature, complete these steps:

- Enter command ‘utils ctl set-cluster mixed-mode’ into the CLI on the UCM publisher:

```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want
to continue? (y/n): y

Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run
these services.
```

Note: Above output is captured on UCM14. On 11.5, different services need to be restarted. Please pay attention to the output before restarting services.

- Navigate to UCM Admin Page > System > Enterprise Parameters and verify whether the cluster was set to Mixed mode (a value of 1 indicates Mixed mode):

Security Parameters

Cluster Security Mode *	1

UCM Mixed Mode

Use ‘show ctl’ to check if the CTL file was installed and verify if all the CTL file entries for different functions were generated, including ‘System Administrator Security Token’, ‘CCM+TFTP’, ‘CAPF’.

```
admin: show ctl
The checksum value of the CTL file:
2a2cfe620cbd50e95a188bfdae26744c(MD5)
50a7dad45ab3dfc24a49cf4935a91a10d462694d(SHA1)

Length of CTL file: 8686
The CTL File was last modified on Fri Mar 24 16:50:24 CST 2023

---<snap>---

        CTL Record #:1
                  ----
BYTEPOS TAG             LENGTH  VALUE
------- ---             ------  -----
1       RECORDLENGTH    2       1644
2       DNSNAME         11      cucm125pub
3       SUBJECTNAME     53      CN=cucm125pub.ccbu.cn;OU=tac;O=cisco;L=sh;ST=sh;C=CN
4       FUNCTION        2       System Administrator Security Token
5       ISSUERNAME      53      CN=cucm125pub.ccbu.cn;OU=tac;O=cisco;L=sh;ST=sh;C=CN
6       SERIALNUMBER    16      5D:85:5B:07:07:14:EE:02:C7:11:72:E1:DB:E4:62:02
7       PUBLICKEY       270
8       SIGNATURE       256
9       CERTIFICATE     947     B2 97 C6 7F EB 76 16 42 D9 5D 6D BB 00 D8 A7 F9 1F EE 1C 28 (SHA1 Hash HEX)
10      IPADDRESS       4       10.74.85.141
This etoken was not used to sign the CTL file.
```

Enable TLS to Secure LGW to UCM

In order to setup the secure connection between LGW and UCM, LGW needs to

1. Generate a key for use with a service (crypto key generate)
2. Configure a trustpoint and link the key. (crypto pki trustpoint)
3. Generate a certificate signing request (CSR) (crypto pki enroll)
4. Provide the CSR to a CA for signing
5. Import the Root and/or intermediate CA certificates (crypto pki authenticate)
6. Import the Server certificates (crypto pki import)

*Note: Enable NTP and make sure UCM and the Gateway are synced with the time source before doing any certificate operations.

Enable TLS to Secure LGW to UCM

1. Generate a key for service

Key Pair Generation

crypto key generate rsa general-keys modulus 2048 label SecureLGW

OR

crypto key generate ec keysize 521 label SecureLGW

RSA keypair consist of a public and private key and the key size from 512 – 4096. The label is the name of the key.

The EC keypair is stronger than RSA and is used for features that require ECDSA certificates.

Use command 'show crypto key mypubkey rsa/ec <keyname> to verify the key

```
vcube#show crypto key mypubkey rsa SecureLGW
% Key pair was generated at: 07:26:36 UTC Apr 19 2023
Key name: SecureLGW
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  <snip》
```

Enable TLS to Secure LGW to UCM

2. Create trustpoint to store the certificate.

Use terminal to generate CSR

Specifies the subject name in certificate request

Specifies which key pair to associate with the certificate.

RSAkeypiar or ECkeypair

Trust Point Configuration

```
crypto pki trustpoint SecureLGW
 enrollment terminal
 serial-number none
 fqdn none
 ip-address none
 subject-name CN=SecureLGW.dltaclab.cisco.com
 revocation-check none
 rsakeypair SecureLGW
```

Enable TLS to Secure LGW to UCM

3. Generate CSR and obtain the certificates from the CA.

Generate CSR and obtain the certificate of LGW from CA

```
vcube(config)#crypto pki enroll SecureLGW
% Start certificate enrollment ..

% The subject name in the certificate will include: CN=SecureLGW.dltaclab.cisco.com
% The fully-qualified domain name will not be included in the certificate
Display Certificate Request to terminal? [yes/no]: yes
Certificate Request follows:

MIICejCCAWICAQAwFDESMBAGA1UEAxMJU2VjdXJlTEdXMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAs4G/7wwiaJAiYWXDJ3umk15EaK7YDFYw/iOYA5xN
<snip>
o4c378M1RjZgrQEwpYDQYPdh2Y/jlCyq07yXYp1GskF9x3tRw9Siur/NRQdGhpBa
gCFZjTsJ9Yz7+t1/vsc2wGn+dPyPtjeg1uJoTlny7FkhLZR6pYyW8WFSnlyvxNwD
dYZNnfOSFS5yX1i/uzM=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
```

→ Check SubjectName

→ Send this CSR to CA to be signed. CA responds with 1 root certificate and 1 signed server certificate (and possibly one or more intermediate CA certs).

Root.cer
certnew.cer

Enable TLS to Secure LGW to UCM

4. Import the CA Root Certificate

Import Root Certificate to LGW

vcube(config)#**crypto pki authenticate SecureLGW**

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
MIIDszCCApugAwIBAgIQZvgq8FS3FYtC0kg28MUcizANBgkqhkiG9w0BAQsFADBs
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xGDAW
<snip>
mfhG3tgwPtc7fdJ4AfaA8EDlGtZsBBTGV7XtAPNhD2lu9p05QFCJEEEZGEHUwGmD
hjgtxmHdbyM+XmetbYfbysmNm875y2dinqKjhyKS+sUfnvAg06sV
-----END CERTIFICATE-----
```

Paste the CA Root certificate and press enter

Certificate has the following attributes:
Fingerprint MD5: 7F0B1962 D6CD06CD 6F997730 5397C215
Fingerprint SHA1: 0E143F10 7B3E76AE 067F3534 ADA16040 77DDBE01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Enable TLS to Secure LGW to UCM

5. Import the Server Certificate

Import Certificate to LGW

vcube(config)#**crypto pki import SecureLGW certificate**
% The fully-qualified domain name will not be included in the certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFnjCCBIagAwIBAgITcAAAAEBUSHOhYLvwuAAAAAAAQDANBgkqhkiG9w0BAQsF
ADBsMRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28x
<snip>
RujpsM/UAfE7J1GPFYd5Yw6Z5yoPT58/BOszm4qD/c7Ctz3J4vTo7vRp7vY8Njc3
dbc7vZz34ObeAZ9+8gp6EwcQEFvBFmc4eBMWmxW7JNLUAip/u+Lh6nkLW76nFRxM
xv8=
-----END CERTIFICATE-----

Paste the server certificate and press enter

% Router Certificate successfully imported

Enable TLS to Secure LGW to UCM

6. Verify the certificate

show crypto pki certificate verbose SecureLGW

```
vcube#show crypto pki certificates verbose SecureLGW

Certificate
  Status: Available

Issuer:
  cn=HydrantID Server CA O1
  ou=HydrantID Trusted Certificate Service
  o=IdenTrust
  c=US
Subject:
  Name: securelgw.dltaclab.cisco.com
  c=US
  st=California
  l=San Jose
  o=Cisco Systems Inc.
  cn=securelgw.dltaclab.cisco.com

Validity Date:
  start date: 10:19:52 UTC Apr 26 2023
  end   date: 10:18:52 UTC Apr 25 2024

Cert install time: 09:58:39 UTC Apr 26 2023
 Associated Trustpoints: SecureLGW
 Key Label: SecureLGW
```

Issuer CA

Subject of LGW

Validity Date

Associated Trustpoint

CA

```
CA Certificate
  Status: Available

Issuer:
  cn=IdenTrust Commercial Root CA 1
  o=IdenTrust
  c=US
Subject:
  cn=HydrantID Server CA O1
  ou=HydrantID Trusted Certificate Service
  o=IdenTrust
  c=US

Validity Date:
  start date: 16:56:15 UTC Dec 12 2019
  end   date: 16:56:15 UTC Dec 12 2029

Cert install time: 09:51:53 UTC Apr 26 2023
 Associated Trustpoints: SecureLGW
```

Intermediate CA

Validity Date

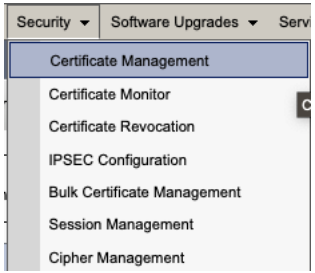
Associated Trustpoint

Enable TLS to Secure LGW to UCM

7. Import the certificate to UCM

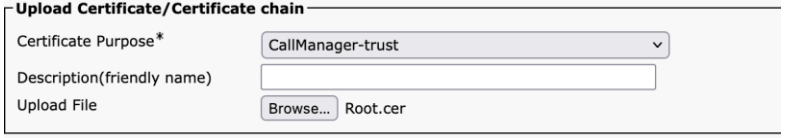
Navigate to Cisco Unified OS Administration

Select ‘Certificate Management’ from the Security menu.

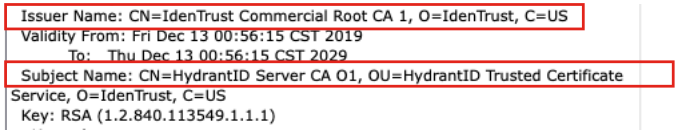


Click ‘Upload Certificate/Certificate chain’ button.

From ‘Certificate Purpose’, choose ‘CallManager-trust’
Click ‘Browse’ and choose the root certificate file.
Then click ‘Upload’.



A new entry with subject name of the CA should now show up in the list of certificates. Click the file to view and check if the Issuer and Subject Name match your CA.



Enable TLS to Secure LGW to UCM

8. Enable Signaling Encryption

Associate trustpoint with sip process

```
sip-ua
 crypto signaling remote-addr <UCM IP> 255.255.255.255 trustpoint SecureLGW
```

Define remote use TLS signaling

```
voice class uri 200 sip
 pattern dtg=jp.gw2710.lgu

dial-peer voice 200201 voip
 description Inbound/Outbound Webex Calling
 destination dpg 300
 incoming uri request 200

voice class dpg 300
 dial-peer 301 preference 1
```

Enable TLS on dial-peer outgoing to UCM

```
dial-peer voice 301 voip
 description Outgoing dial-peer to CUCM-Group-1 for inbound from Webex Calling
 destination-pattern BAD.BAD
 session protocol sipv2
 session transport tcp tls
 session server-group 301
 voice-class codec 99
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
```

```
voice class server-group 301
 ipv4 <UCM IP>
```

Enable TLS on dial-peer incoming from UCM

```
dial-peer voice 300 voip
 description Incoming dial-peer from CUCM for Webex Calling
 session protocol sipv2
 session transport tcp tls
 destination dpg 200
 incoming uri via 300
 voice-class codec 99
 voice-class sip tenant 300
 dtmf-relay rtp-nte
 no vad
```

OR

Enable TLS globally

```
voice service voip
 sip
  session transport tcp tls
```

Enable Security on UCM SIP Trunk

1. Create a SIP Trunk Security Profile

SIP Trunk Security Profile Information

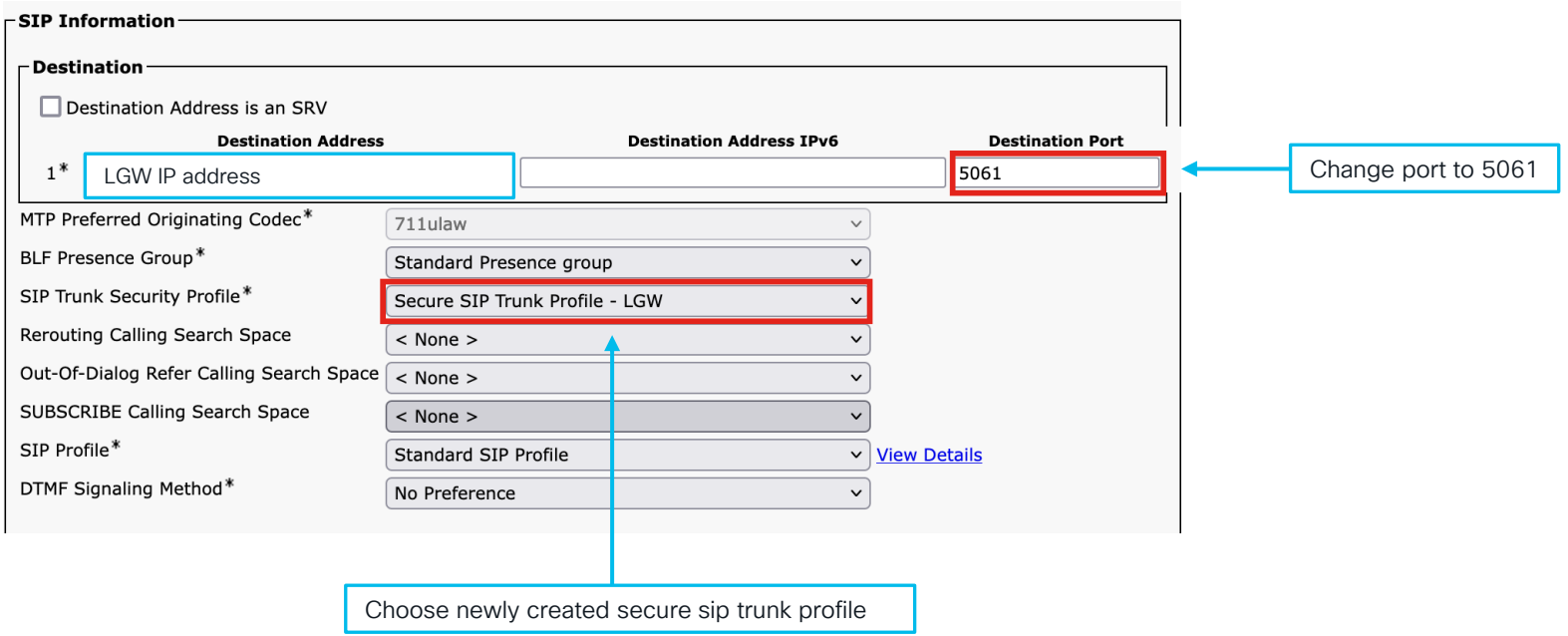
Name*	Secure SIP Trunk Profile - LGW
Description	Secure SIP Trunk Profile for Webex Calling LGW
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	SecureLGW.dltaclab.cisco.com
Incoming Port*	5061

Make sure the Subject name matches the configuration on LGW.

```
crypto pki trustpoint SecureLGW
  enrollment terminal
  serial-number none
  fqdn none
  ip-address none
  subject-name CN=SecureLGW.dltaclab.cisco.com
  revocation-check none
  eckeypair SecureLGW
```

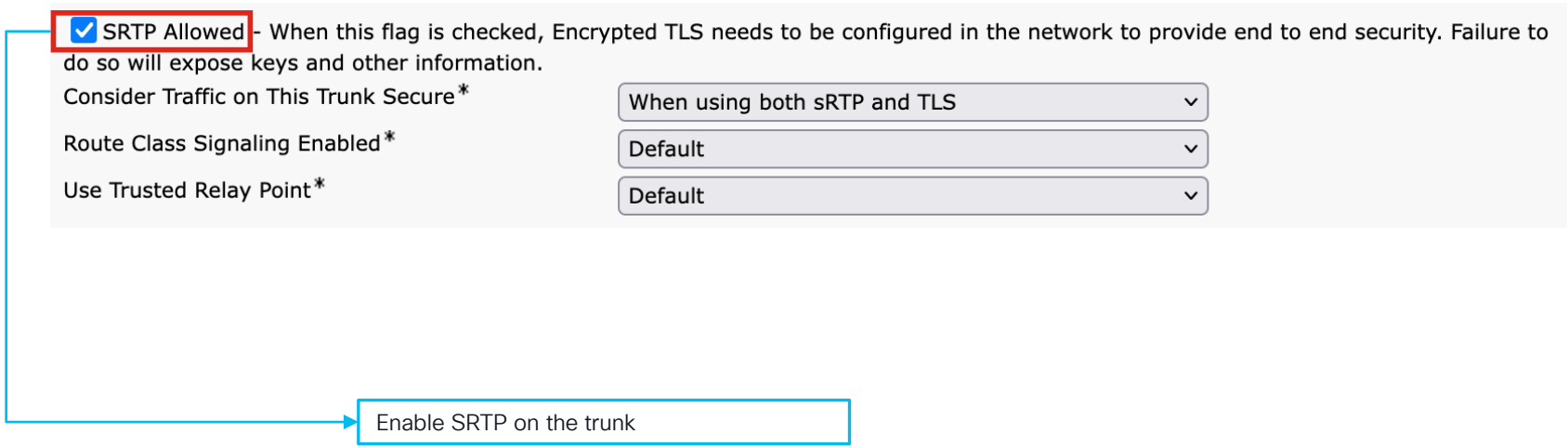
Enable Security on UCM SIP Trunk

2. Create a SIP Trunk to the LGW with the newly created Secure SIP Trunk Profile



Enable Security on UCM SIP Trunk

3. Check ‘SRTP Allowed’ in the SIP Trunk Configuration



Secure Media Example

Secure media means the RTP steam need to be encrypted.

The SDP on the right, used to negotiate SRTP, has a new attribute called a=crypto which indicates the crypto suite and key parameters.

SDP for non-secure RTP

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 9559 740 IN IP4
10.1.1.137
s=SIP Call
c=IN IP4 10.1.1.137
t=0 0
m=audio 36116 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
```

From Cisco IOS XE Everest Release 16.5.1b onwards, the following crypto suites are enabled by default on the SRTP leg:

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM
- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32

SDP for secure RTP

```
v=0
o=CiscoSystemsSIP-GW-UserAgent 4720 857 IN IP4
10.1.1.137
s=SIP Call
c=IN IP4 10.1.1.137
t=0 0
m=audio 36118 RTP/SAVP 0 8 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Key and Salt will follow immediately.

Master Key and Salt

Crypto Suite

Enable Secure Media on LGW

1. Define SRTP Crypto Suites (Optional)

```
voice class srtp-crypto 1
 crypto 1 AEAD_AES_256_GCM
 crypto 2 AEAD_AES_128_GCM
 crypto 3 AES_CM_128_HMAC_SHA1_80
 crypto 4 AES_CM_128_HMAC_SHA1_32
```

Configure SRTP cipher suites which can be used on dial-peers or globally

2.a Enable SRTP on dial-peer

```
dial-peer voice 301 voip
 description Outgoing dial-peer to CUCM-Group-1 for inbound
from Webex Calling
 destination-pattern BAD.BAD
 session protocol sipv2
 session transport tcp tls
 session server-group 301
 voice-class codec 99
 voice-class sip tenant 100
 srtp
 dtmf-relay rtp-nte
 voice-class sip srtp-crypto 1
 no vad
```

Enable SRTP

Apply crypto suite (Optional)

2.b Enable SRTP globally

```
voice service voip
 srtp
  sip
   srtp-crypto 1
```

Secure IP Phone

Enabling Encryption on Phones

- Secure Cisco phones can use a pre-installed MIC (Manufacturer-Installed Certificate) to register securely with Cisco Unified CM without certificate management, but LSC (Locally-Significant Certificates) can be created and installed for extra security using the CAPF (Certificate Authority Proxy Function) service.
- Cisco Video Endpoints have no MIC installed by default, so an LSC is necessary to enable secure mode on these devices.
- SIP OAuth Mode allows you to use OAuth refresh tokens for all device authentication in secure environments.

Create Phone Security Profile

- Go to System → Security → Phone Security Profile.
- Find the phone model you want to configure and click the Non-Secure Profile.
- Copy it and rename it with another name to indicate this is a secure profile.
- Change the Device Security Mode to :
  - Encrypted: Both signaling and media are encrypted.
  - Authenticated: Provide authentication for the phone
- Make sure Transport Type will set to TLS.

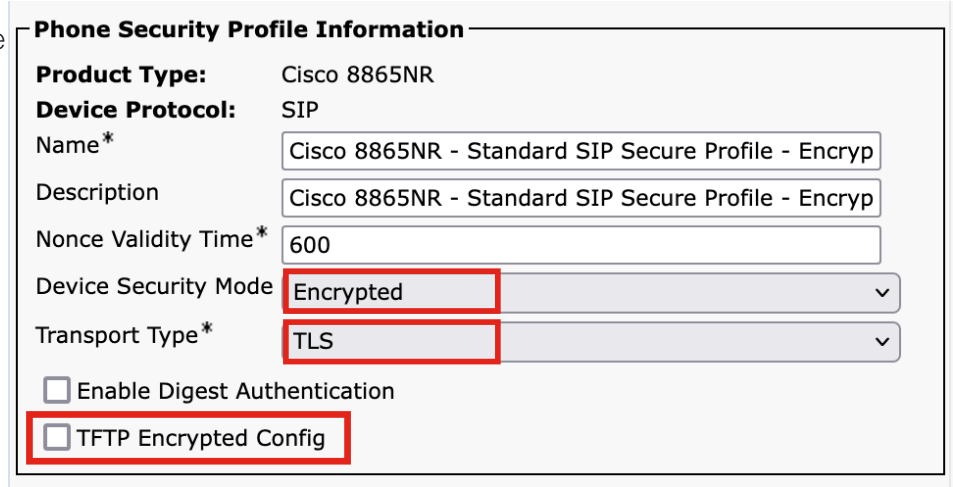
*Note: Use 'Universal Device Template' instead of per-model profile if different models need to be updated.

Encrypted indicates signaling and media are both encrypted

Authenticated signs the signaling message to prevent tampering

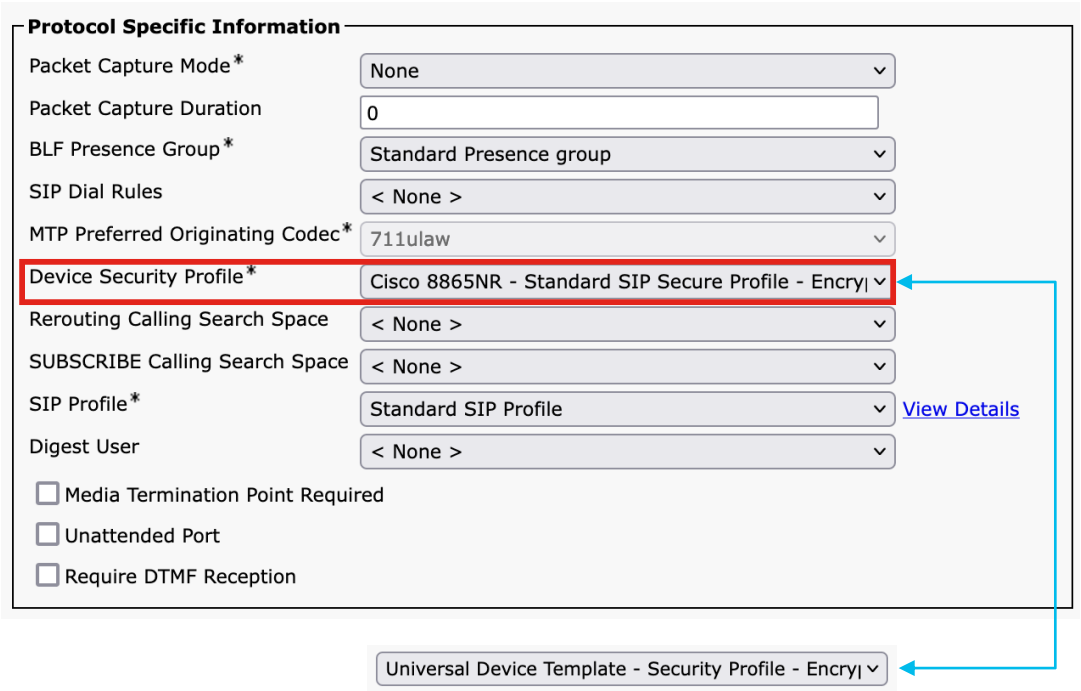
Change Transport Type to TLS for secure connection.

To encrypt configuration files on the TFTP server, check this.

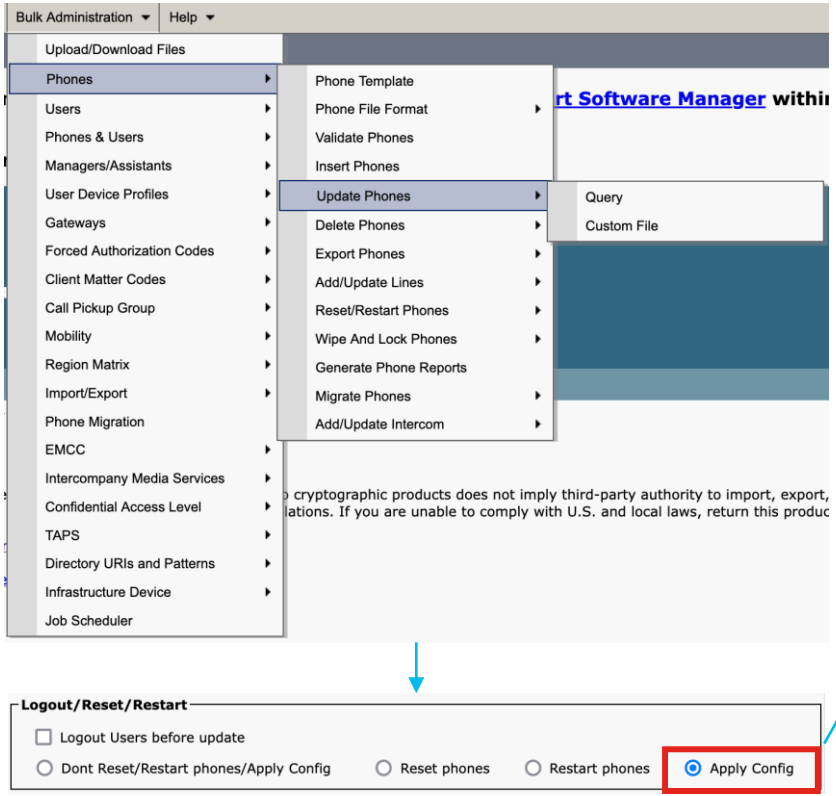


Apply Phone Security Profile

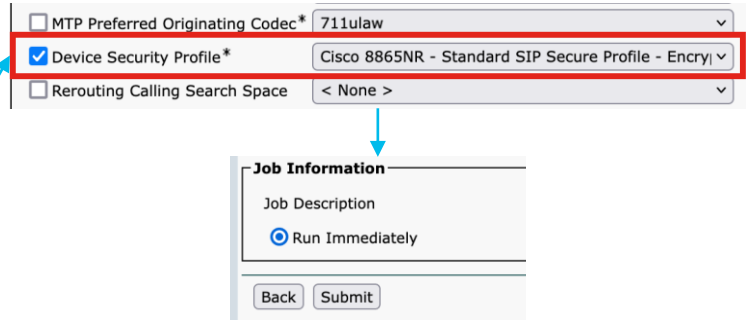
- Go to the phone configuration page
- Change Device Security Profile to the newly created Device Security Profile or Universal Device Profile.



Apply Phone Security Profile



- If you need to update all phones, use BAT
  - Query phone type you want to update
  - Choose ‘Apply Config’
  - Check Device Security Profile and choose the secure profile
  - Choose ‘Run Immediately’
  - Submit



Apply Phone Security Profile

- Step 1: Configure CAPF on UCM.
  - Under the CAPF section, change Certificate Operation to ‘Install/Upgrade’. Choose ‘By Null String’ for Authentication Mode. Then save and apply configuration.

Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	
Generate String	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	
Operation Completes By	2023 04 05 12 (YYYY:MM:DD:HH)

Certificate Operation Status: Upgrade Success

Note: Security Profile Contains Addition CAPF Settings.

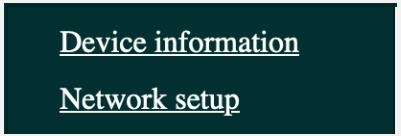
Apply Phone Security Profile

Step 2: Verify Phone / Endpoint Settings

- Log in to the device web page, then do the following:

Phone

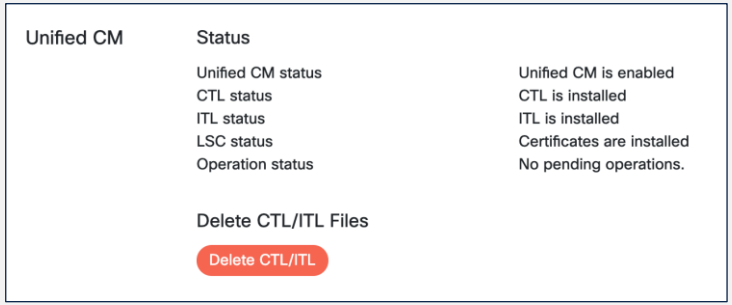
Click **Network Setup** from left bar and check that Security mode is Encrypted.



Security mode	Encrypted

Video Endpoint

Go to **Security** and check UCM Certificates.



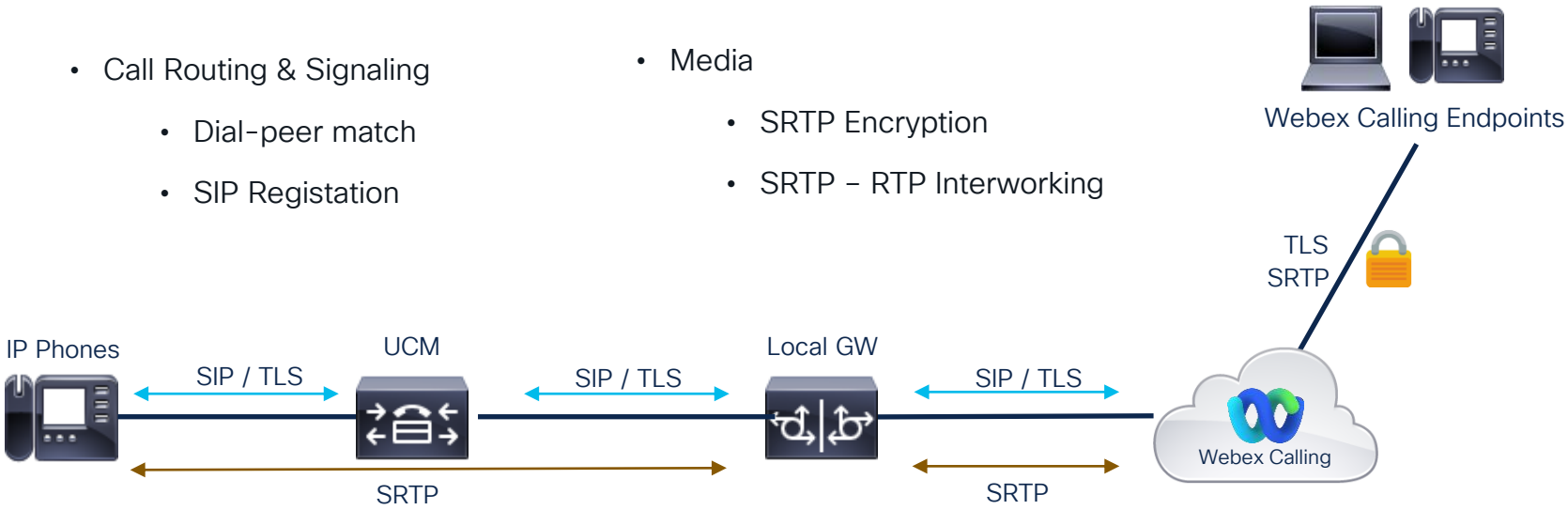
Troubleshooting Secure Connections

Narrow Down the Problem

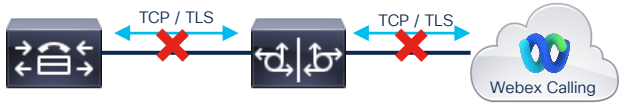
- Network
  - TCP session establishment
  - TLS session negotiation

- Call Routing & Signaling
  - Dial-peer match
  - SIP Registation

- Media
  - SRTP Encryption
  - SRTP – RTP Interworking



Verifying TLS Connectivity



- Verify if the TLS connection is established

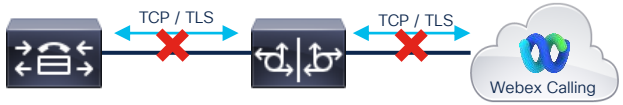
```
vcube#show sip-ua connections tcp tls detail
Total active connections      : 3
No. of send failures          : 0
No. of remote closures        : 18
No. of conn. failures         : 2
No. of inactive conn. ageouts : 0
Max. tls send msg queue size of 1, recorded for 139.177.68.10:8934
TLS client handshake failures : 2
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
<snap>

Remote-Agent:139.177.68.10, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher                          Curve
  =========== ======= ========== =========== ============= =========== ============================== =====
         8934       5 Established           0 10.1.1.137     TLSv1.2     ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:10.1.1.151, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher                          Curve
  =========== ======= ========== =========== ============= =========== ============================== =====
        26467      47 Established           0 10.1.1.137     TLSv1.2     ECDHE-RSA-AES256-GCM-SHA384 P-521
         5061      48 Established           0 10.1.1.137     TLSv1.2     ECDHE-RSA-AES256-GCM-SHA384 P-521
```

Connection failures and handshake failures indicate the TLS establishment failed. Keep monitoring if counters increment.

To Webex Calling TLS connection

To UCM TLS connection

Verifying TCP/TLS Connectivity



- Confirm that the TCP session is established via ‘debug ip tcp transactions’
- Confirm TLS negotiation process via ‘debug crypto pki message / transactions’

```
Mar 26 11:00:35.312: TCP0: state was LISTEN -> SYNRCVD [5061 -> 10.1.1.151(26467)]
Mar 26 11:00:35.312: TCP: tcb 7F99C8F723C0 connection to 10.1.1.151:26467, peer MSS 1460, MSS is 516
Mar 26 11:00:35.312: TCP: Selective ack is disabled from the CLI
Mar 26 11:00:35.313: TCP: sending SYN, seq 2858937177, ack 272952486
Mar 26 11:00:35.313: TCP0: Connection to 10.1.1.151:26467, advertising MSS 1460
Mar 26 11:00:35.313: TCP0: state was SYNRCVD -> ESTAB [5061 -> 10.1.1.151(26467)]
```

```
Mar 26 11:00:35.314: CRYPTO_PKI: (A3AD6) Session started - identity selected (SecureLGW)
Mar 26 11:00:35.370: <<< TLS 1.2 Handshake [length 00A9], ClientHello
Mar 26 11:00:35.376: >>> TLS 1.2 Handshake [length 0039], ServerHello
Mar 26 11:00:35.378: >>> TLS 1.2 Handshake [length 02FC], Certificate
Mar 26 11:00:35.427: >>> TLS 1.2 Handshake [length 0191], ServerKeyExchange
<snap>
Mar 26 11:00:35.491: CRYPTO_PKI: Added x509 peer certificate - (951) bytes
Mar 26 11:00:35.492: CRYPTO_PKI: create new ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 24
Mar 26 11:00:35.492: CRYPTO_PKI: (A3AD7)validation path has 1 certs
Mar 26 11:00:35.492: CRYPTO_PKI: Found a issuer match
Mar 26 11:00:35.492: CRYPTO_PKI: (A3AD7) Using CUCM to validate certificate
Mar 26 11:00:35.492: CRYPTO_PKI: Added 1 certs to trusted chain.
```

Server Certificate

TCP session established. Listen → SYNRCVD(SYN received) →?ESTAB (Established)

TLS negotiation successful. LGW sends hello to UCM, UCM replies with Sever Hello and sends the server certificate, client verifies the certificate .

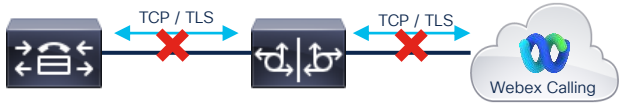
Packet Capture on IOS-XE

- Packet capture is an efficient way to diagnose network issues such as packet lost, blocked ports, etc. IOS-XE provides an integrated packet capture function to capture packets as they traverse through the device. Below is the CLI command to explain how to enable / start / stop and export packet captures.

Command	Explanation
monitor capture Test interface g1 both	Interface to capture packets on
monitor capture Test match any	Match all packets. Can filter IP or MAC
monitor capture Test limit packet-len 9500	Max packet size (optional)
monitor capture Test limit pps 5000	Max packets per second (optional)
monitor capture Test limit packets 1000	Max packets (optional)
monitor capture Test buffer size 100	Max amount of memory the capture can consume
monitor capture Test access-list TCP	ACL to limit what is captured (optional)
monitor capture Test start	Start capture
monitor capture Test stop	Stop capture
monitor capture Test export ftp : //10.1.2.31/test1.pcap	Export packet to FTP server

Use ‘show monitor capture’ to check the settings and status.

Diagnosing Network Issue



- Verify packet capture on LGW. Use ‘monitor capture’ command to capture packet via the interface which connects to Webex and UCM.

10384	2023-03-26 07:15:01.902953	[redacted].137	[redacted]	151	TCP	54	26351 → 5061 [ACK] Seq=2780993825 Ack=4099632847 Win=4128 Len=0
10513	2023-03-26 07:17:55.827944	[redacted].151	[redacted]	137	TCP	74	25064 → 5061 [SYN] Seq=2535835015 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3375831784 TSecr=0 WS=128
10514	2023-03-26 07:17:55.829943	[redacted].137	[redacted]	151	TCP	58	5061 → 25064 [SYN, ACK] Seq=708381285 Ack=2535835016 Win=4128 Len=0 MSS=1460
10515	2023-03-26 07:17:55.829943	[redacted].151	[redacted]	137	TCP	54	25064 → 5061 [ACK] Seq=2535835016 Ack=708381286 Win=64240 Len=0
10518	2023-03-26 07:17:55.908949	[redacted].151	[redacted]	137	TLSv1.2	228	Client Hello
10519	2023-03-26 07:17:55.909941	[redacted].137	[redacted]	151	TCP	54	5061 → 25064 [ACK] Seq=708381286 Ack=2535835190 Win=3954 Len=0
10520	2023-03-26 07:17:55.948940	[redacted].137	[redacted]	151	TLSv1.2	1331	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
10521	2023-03-26 07:17:55.948940	[redacted].151	[redacted]	137	TCP	54	25064 → 5061 [ACK] Seq=2535835190 Ack=708382563 Win=63850 Len=0
10522	2023-03-26 07:17:55.970942	[redacted].151	[redacted]	137	TCP	1514	25064 → 5061 [ACK] Seq=2535835190 Ack=708382563 Win=63850 Len=1460 [TCP segment of a reassembled PDU]
10523	2023-03-26 07:17:55.970942	[redacted].151	[redacted]	137	TLSv1.2	1514	Certificate
10524	2023-03-26 07:17:55.970942	[redacted].151	[redacted]	137	TLSv1.2	707	Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
10525	2023-03-26 07:17:55.970942	[redacted].137	[redacted]	151	TCP	54	5061 → 25064 [ACK] Seq=708382563 Ack=2535838110 Win=1034 Len=0
10526	2023-03-26 07:17:55.973948	[redacted].137	[redacted]	151	TCP	54	5061 → 25064 [ACK] Seq=708382563 Ack=2535838763 Win=2015 Len=0
10527	2023-03-26 07:17:55.973948	[redacted].137	[redacted]	151	TCP	54	[TCP Window Update] 5061 → 25064 [ACK] Seq=708382563 Ack=2535838763 Win=3475 Len=0
10528	2023-03-26 07:17:55.996942	[redacted].137	[redacted]	151	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
10529	2023-03-26 07:17:55.996942	[redacted].151	[redacted]	137	TCP	54	25064 → 5061 [ACK] Seq=2535838763 Ack=708382614 Win=63850 Len=0

TCP 3-way handshake Session Establishment

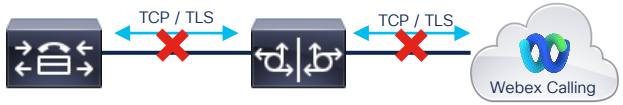
If the TCP connection cannot be established, please verify following:

- TLS port set on UCM Trunk Security profile & SIP trunk are 5061. Verify in packet packet capture if port is 5061.
- Verify if remote replies with SYN ACK. If not, then TCP port may be blocked by a firewall or access list.

TLS negotiation

- TLS alert message indicates an error during certificate exchange. Need to verify the server certificate and CA root certificate.
- Also need to check if the certificate is expired or not.

Network Problem – Example



TCP session closed without TLS message exchange

1188	2023-04-14 18:52:34.309981	[redacted]	139.177.68.10	TCP	58	16440 → 8934 [SYN] Seq=0 Win=4128 Len=0 MSS=536
1189	2023-04-14 18:52:34.311980	139.177.68.10	[redacted]	TCP	58	8934 → 16440 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
1190	2023-04-14 18:52:34.312972	[redacted]	139.177.68.10	TCP	54	16440 → 8934 [ACK] Seq=1 Ack=1 Win=4128 Len=0
1191	2023-04-14 18:52:34.314970	[redacted]	139.177.68.10	TCP	54	16440 → 8934 [FIN, PSH, ACK] Seq=1 Ack=1 Win=4128 Len=0
1192	2023-04-14 18:52:34.315977	[redacted]	139.177.69.10	TCP	58	14239 → 8934 [SYN] Seq=0 Win=4128 Len=0 MSS=536
1193	2023-04-14 18:52:34.316969	139.177.68.10	[redacted]	TCP	54	8934 → 16440 [FIN, ACK] Seq=1 Ack=2 Win=29200 Len=0
1194	2023-04-14 18:52:34.316969	[redacted]	139.177.68.10	TCP	54	16440 → 8934 [ACK] Seq=2 Ack=2 Win=4128 Len=0

TCP 3-way handshake Established without problem.

No TLS message exchange and TCP session closed.

```
Apr 14 10:52:34.309: TCP: sending SYN, seq 1838465272, ack 0
Apr 14 10:52:34.309: TCP0: Connection to 139.177.68.10:8934, advertising MSS 536
Apr 14 10:52:34.310: TCP0: state was CLOSED -> SYNSENT [16440 -> 139.177.68.10(8934)]
Apr 14 10:52:34.313: TCP0: state was SYNSENT -> ESTAB [16440 -> 139.177.68.10(8934)]
Apr 14 10:52:34.313: TCP: tcb 7F99C89E1AF0 connection to 139.177.68.10:8934, peer MSS 1460, MSS is 536
Apr 14 10:52:34.313: TCB7F99C89E1AF0 getting property TCP_VRFTABLEID (20)
Apr 14 10:52:34.313: //-1/xxxxxxxxxxxx/SIP/Error/sip_tls_generate_opssl_ctx:
Invalid trustpoint label
Apr 14 10:52:34.313: //-1/xxxxxxxxxxxx/SIP/Error/sip_tls_tcp_createconnfailed_to_spi:
 TLS create conn failed to SPI (addr:139.177.68.10, port:8934)
Apr 14 10:52:34.313: //-1/xxxxxxxxxxxx/SIP/Error/httpish_msg_free:
 Freeing NULL pointer!
Apr 14 10:52:34.315: TCP0: state was ESTAB -> FINWAIT1 [16440 -> 139.177.68.10(8934)]
Apr 14 10:52:34.315: TCP0: sending FIN
```

From 'debug voice ccapi inout', no valid trustpoint used to establish TLS session.

Check if trustpoint used for crypto signaling is configured under 'sip-ua'

```
sip-ua
 transport tcp tls v1.2
 crypto signaling default trustpoint <trustpoint name>
```

Network Problem – Example

TLS Alert with Certificate Error

1129	2023-04-15 23:14:18.405969	[redacted]	151	[redacted]	.137	TCP	74	25007 → 5061 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=866275601 TSecr=0 WS=128
1130	2023-04-15 23:14:18.406976		137		.151	TCP	58	5061 → 25007 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
1131	2023-04-15 23:14:18.406976		151		.137	TCP	54	25007 → 5061 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1132	2023-04-15 23:14:18.418969		212		.137	TCP	54	60408 → 22 [ACK] Seq=15201 Ack=148289 Win=65535 Len=0
1133	2023-04-15 23:14:18.418969		212		.137	TCP	54	60408 → 22 [ACK] Seq=15201 Ack=148389 Win=65535 Len=0
1134	2023-04-15 23:14:18.477972		151		.137	TLSv1.2	228	Client Hello
1135	2023-04-15 23:14:18.478963		137		.151	TCP	54	5061 → 25007 [ACK] Seq=1 Ack=175 Win=3954 Len=0
1136	2023-04-15 23:14:18.544969		137		.151	TLSv1.2	1331	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
1137	2023-04-15 23:14:18.544969		151		.137	TCP	54	25007 → 5061 [ACK] Seq=175 Ack=1278 Win=63850 Len=0
1138	2023-04-15 23:14:18.545961		151		.137	TLSv1.2	61	Alert (Level: Fatal, Description: Unknown CA)
1139	2023-04-15 23:14:18.545961		151		.137	TCP	54	25007 → 5061 [FIN, ACK] Seq=182 Ack=1278 Win=63850 Len=0
1140	2023-04-15 23:14:18.545961		137		.151	TCP	54	5061 → 25007 [ACK] Seq=1278 Ack=183 Win=3947 Len=0
1141	2023-04-15 23:14:18.550966		137		.151	TCP	54	5061 → 25007 [FIN, PSH, ACK] Seq=1278 Ack=183 Win=3947 Len=0
1142	2023-04-15 23:14:18.550966		151		.137	TCP	54	25007 → 5061 [ACK] Seq=183 Ack=1279 Win=63850 Len=0

TLS negotiate failed. Alert message generate and TCP session closed.

```
Apr 15 15:14:18.481: <<< TLS 1.2 Handshake [length 00A9], ClientHello
Apr 15 15:14:18.481:     01 00 00 A5 03 03 4B 75 18 EC 14 B6 3D 8D E2 05
Apr 15 15:14:18.491: >>> TLS 1.2 Handshake [length 0039], ServerHello
Apr 15 15:14:18.491:     02 00 00 35 03 03 BA F3 89 18 1B 73 7F 81 0C E9
Apr 15 15:14:18.492: >>> TLS 1.2 Handshake [length 02FC], Certificate
Apr 15 15:14:18.492:     0B 00 02 F8 00 02 F5 00 02 F2 30 82 02 EE 30 82
Apr 15 15:14:18.536: >>> TLS 1.2 Handshake [length 0191], ServerKeyExchange
Apr 15 15:14:18.536:     0C 00 01 8D 03 00 19 85 04 01 77 0F E2 C2 C8 C8
Apr 15 15:14:18.544: >>> TLS 1.2 Handshake [length 0023], CertificateRequest
Apr 15 15:14:18.544:     0D 00 00 1B 02 01 40 00 14 06 01 06 03 05 01 05
Apr 15 15:14:18.551: <<< TLS 1.2 Alert [length 0002], fatal unknown_ca
Apr 15 15:14:18.551:     02 30
Apr 15 15:14:18.551:
Apr 15 15:14:18.551: SSL3 alert read:fatal:unknown CA
Apr 15 15:14:18.551: SSL_accept:failed in error
```

unknown CA means client site has no CA root certificate to verify the server certificate.

Check if client side has CA root certificate.

Signaling – SIP Registration

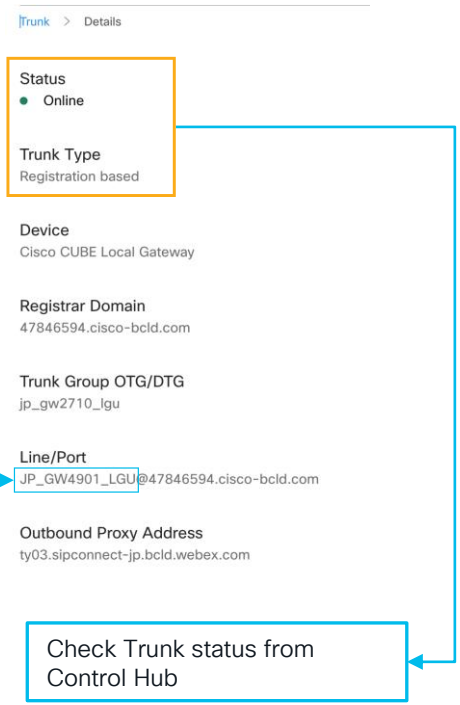
- If the LGW does not register to Webex then use ‘show sip-ua register status’ command. Then use ‘debug sip message’ to check if the options ping keep alive is working. Finally verify the ‘Line/Port’ configuration.

```
vcube#show sip-ua register status

Tenant:  200
-------------------- Registrar-Index  1 ---------------------
Line                              peer      expires(sec) reg survival  P-Associ-URI
================================= ========= ============ === ========  ============
JP_GW4901_LGU                     -1         51           yes normal
```

Received:
OPTIONS sip:**10.1.1.137:5061**;transport=tls SIP/2.0
Via:SIP/2.0/TLS 139.177.68.10:8934;branch=z9hG4bKBroadworksSSE.-10.1.1.137V47186-0-100-1014665373-1679809185878-
From:<**sip:139.177.68.10**>;tag=1014665373-1679809185878-
To:<sip:10.1.1.137>
Call-ID:**SSE05394587826032319469159 23@139.177.68.10**
CSeq:100 OPTIONS
Max-Forwards:0
Content-Length:0

```
voice class tenant 200
  credentials number JP_GW4901_LGU
username JP_GW2710_LGU password 6 ***
realm BroadWorks
```

Sent:
SIP/2.0 200 OK
Via: SIP/2.0/TLS 139.177.68.10:8934;branch=z9hG4bKBroadworksSSE.-10.1.1.137V47186-0-100-1014665373-1679809185878-
From: <**sip:139.177.68.10**>;tag=1014665373-1679809185878-
To: <sip:10.1.1.137>;tag=EB68861-2696
Date: Sun, 26 Mar 2023 13:39:34 GMT
Call-ID: **SSE05394587826032319469159 23@139.177.68.10**
Server: Cisco-SIPGateway/IOS-17.3.5



Call Routing

- LGW inbound and outbound call failed. Use 'debug voice ccapi inout' to check if the dial-peer is matched correctly.

```
Mar 26 14:01:38.400: //-1/8FB29175BC16/CCAPI/cc_api_call_setup_ind_common:
  Interface=0x7F99BDB795B0, Call Info(
  Calling Number=+12092375678,(Calling Name=)(TON=Unknown, NPI=Unknown, Screening=User, Passed, Presentation=Allowed),
  Called Number=88991(TON=Unknown, NPI=Unknown),
  Calling Translated=FALSE, Subscriber Type Str=Unknown, FinalDestinationFlag=TRUE,
  Incoming Dial-peer=200201, Progress Indication=NULL(0), Calling IE Present=TRUE,
  Source Trkgrp Route Label=, Target Trkgrp Route Label=, CLID Transparent=FALSE), Call Id=19347

Mar 26 14:01:38.404: //19347/8FB29175BC16/CCAPI/ccIFCallSetupRequestPrivate:
  Interface=0x7F99BDB795B0, Interface Type=3, Destination=, Mode=0x0,
  Call Params(Calling Number=+12092375678,(Calling Name=Michael Huang)(TON=Unknown, NPI=Unknown, Screening=User, Passed, Presentation=Allowed),
  Called Number=88991(TON=Unknown, NPI=Unknown), Calling Translated=FALSE,
  Subscriber Type Str=Unknown, FinalDestinationFlag=TRUE, Outgoing Dial-peer=301, Call Count On=FALSE,
  Source Trkgrp Route Label=, Target Trkgrp Route Label=, tg_label_flag=0, Application Call Id=)
```

```
Mar 26 14:08:05.539: cc_api_get_xcode_stream : 5013
Mar 26 14:08:05.550: //19385/7672872BBC37/CCAPI/cc_api_call_disconnected:
  Cause Value=127, Interface=0x7F99BDB795B0, Call Id=19385
```

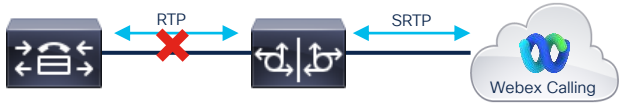
```
dial-peer voice 301 voip
 description Outgoing dial-peer to CUCM-Group-1 for inbound from Webex Callin
 destination-pattern BAD.BAD
 session protocol sipv2
 session server-group 301
 voice-class codec 99
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad
```

Indicates the call outgoing to UCM failed due to interworking failure.

Transport protocol is not TLS on LGW. But on UCM, it is TLS with port 5061.

Fix: Check the dial-peer From / To UCM is configured with 'session transport tcp tls' and make sure UCM SIP Trunk security profile has the right port 5061 set.

Media Problem



- Call can be established, but media is not encrypted.

```
vcube#show sip-ua calls
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID                : AB82E9BD-CB1C11ED-BD30BCAD-462B7A40@10.1.1.137
  State of the call        : STATE_ACTIVE (7)
  Substate of the call     : SUBSTATE_NONE (0)
  Calling Number           : +12092371113
  Called Number            : 88991
  Called URI               : sip:88991@10.1.1.151
Media Source IP Addr:Port: [10.1.1.137]:36438
  Media Dest IP Addr:Port  : [10.1.1.151]:36216
  Media Stream 2
  State of the stream      : STREAM_ACTIVE
```

```
Call 1
SIP Call ID                : SSE065243320260323172486590 2@139.177.68.10
  State of the call        : STATE_ACTIVE (7)
  Substate of the call     : SUBSTATE_NONE (0)
  Calling Number           : 2371113
  Called Number            : 88991
  Called URI               : sip:88991@10.1.1.137:5061;transport=tls;dtg=jp_gw2710_lgu
Media Source IP Addr:Port: [10.1.1.137]:36432
  Media Dest IP Addr:Port  : [135.84.169.39]:42350
  Local Crypto Suite       : AES_CM_128_HMAC_SHA1_80
  Remote Crypto Suite      : AES_CM_128_HMAC_SHA1_80
  Local Crypto Key         : J7c1urlRN0f75VZG37wMz+UQMdwPr5rkrvx3WbwH
  Remote Crypto Key        : Oh4t4jyptoyr3yvudBjpHDhlihAh7Y8zSCce77hT
  Media Stream 2
  State of the stream      : STREAM_ACTIVE
```

'show sip-ua calls' indicates the call has two legs. The call leg to UCM (left side) has no crypto suite which means the media is not encrypted. The call leg to Webex Calling (right side) has a crypto suite and key which indicates media is encrypted.

Media Problem

- ‘show call active voice brief’ can also identify if the call is SRTP or not

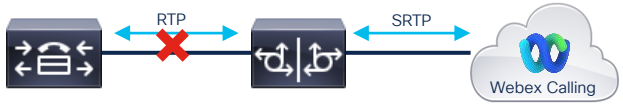
```
0     : 19741 252248470ms.1 (15:11:11.187 UTC Sun Mar 26 2023) +3390 pid:300 Answer 88991 active
 dur 00:00:10 tx:490/98000 rx:508/101600 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 10.1.1.151:36224 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No
ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:18cf8af211e35e05b2f2b84374f4f48b
 RemoteUUID:c5f0824300105000a000501cb00cab25
 VRF: NA
0     : 19742 252248470ms.2 (15:11:11.187 UTC Sun Mar 26 2023) +3370 pid:200201 Originate 1113 active
 dur 00:00:10 tx:505/106050 rx:490/102900 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 135.84.169.39:43532 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No
ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:bb69bcc300804a5092fa0a43ef47999e
 RemoteUUID:18cf8af211e35e05b2f2b84374f4f48b
 VRF: NA
```

Webex Calling leg is encrypted. But UCM leg is not encrypted.

Call from 88991 to 1113. Incoming dial-peer is 300, outgoing dial-peer is 200201

Call from UCM IP and port to Webex Calling IP and port.

Media Problem



- Check the dial-peer setting and the sip-ua encryption setting

```
dial-peer voice 301 voip
 description Outgoing dial-peer to CUCM-Group-1 for inbound from Webex Calling
 destination-pattern BAD.BAD
 session protocol sipv2
 session transport tcp tls
 session server-group 301
 voice-class codec 99
 voice-class sip tenant 100
 dtmf-relay rtp-nte
 no vad

dial-peer voice 300 voip
 description Incoming dial-peer from CUCM for Webex Calling
 session protocol sipv2
 session transport tcp tls
 destination dpg 200
 incoming uri via 300
 voice-class codec 99
 voice-class sip tenant 300
 dtmf-relay rtp-nte
 no vad
```

No ‘srtp’ configured under dial-peer to force media encryption.

Media Problem

- ‘debug ccsip message’ and ‘debug voice ccapi inout’ can help identify a media negotiation issue.

Outgoing call to Webex Calling Invite SDP:

```
<snip>
m=audio 36450 RTP/SAVP 0 8 101
c=IN IP4 10.1.1.137
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=ptime:20
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
<snip>
```

Receive 200OK with SDP:

```
<snip>
m=audio 42706 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=sendrecv
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Send 200OK to UCM with SDP:

```
<snip>
m=audio 36448 RTP/SAVP 0 101
c=IN IP4 10.1.1.137
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=crypto:1 AEAD_AES_256_GCM inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
a=crypto:2 AEAD_AES_128_GCM inline:xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxx
a=crypto:4 AES_CM_128_HMAC_SHA1_32 inline:xxxxxxxxxxxxxxxxxxxxxxxxxxx
<snip>
```

Receive ACK from UCM with SDP:

```
<snip>
m=audio 36222 RTP/AVP 0 101
a=extmap:4 http://protocols.cisco.com/timestamp#100us
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Mar 26 15:07:57.036: //19723/F25C27800000/CCAPI/cc_api_call_disconnected:
Cause Value=65, Interface=0x7F99BDB795B0, Call Id=19723

Media Problem

- Need to check ‘SRTP Allowed’.
- Need to have ‘srtp’ configured under dial peer to / from UCM.

```
SIP Call ID                : A16346DB-CB2511ED-BE50BCAD-
462B7A40@10.1.1.137
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : +12092371113
   Called Number           : 88991
   Called URI              : sip:88991@10.1.1.151
<snap>
Media Source IP Addr:Port: [10.1.1.137]:36462
     Media Dest IP Addr:Port  : [10.1.1.151]:48104
     Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80 (
                                 AEAD_AES_256_GCM
                                 AEAD_AES_128_GCM
                                 AES_CM_128_HMAC_SHA1_80
                                 AES_CM_128_HMAC_SHA1_32 )
     Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
     Local Crypto Key         : 2tNJpfqr4sRXnOXwCMWytYRsETqmqzcwBdrhbDeu
     Remote Crypto Key        : I7g4AawPo0Hpp4wgsfv1OeaTwG64hEhQ2ZRwhpT4
```

After correcting the configuration, the 'show sip-ua calls' and 'show call active voice brief' commands indicate that the media is encrypted.

```
1046 : 19985 255100920ms.1 (15:58:43.637 UTC Sun Mar 26 2023) +3670
pid:300 Answer 88991 active
 dur 00:00:03 tx:157/32970 rx:176/36960 dscp:0 media:0 audio tos:0xB8
video tos:0x0
 IP 10.1.1.151:48112 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms
g711ulaw TextRelay: off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a
timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:2e60f40fc0f057078d01bc9bc7656e69
 RemoteUUID:b894999700105000a000501cb00cab25
 VRF: NA
1046 : 19986 255100930ms.1 (15:58:43.647 UTC Sun Mar 26 2023) +3650
pid:200201 Originate 1113 active
 dur 00:00:03 tx:172/36120 rx:157/32970 dscp:0 media:0 audio tos:0xB8
video tos:0x0
 IP 135.84.169.40:21854 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0
delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a
timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:55691c2a00804536a51f5b770ab0da67
 RemoteUUID:2e60f40fc0f057078d01bc9bc7656e69
 VRF: NA
```

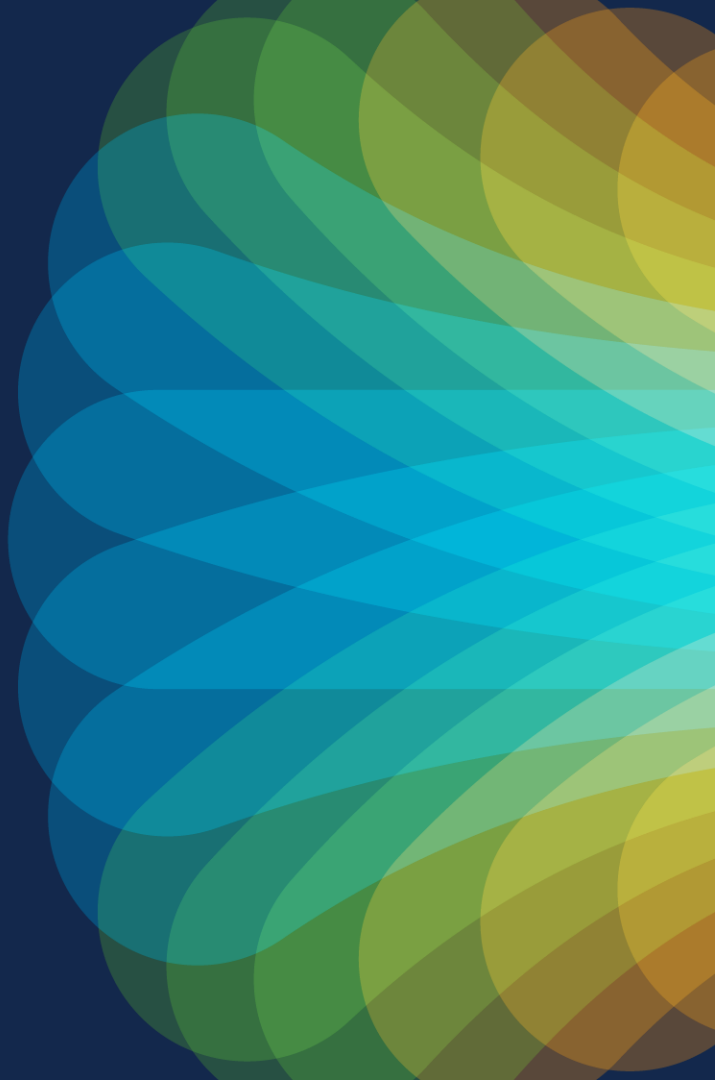
Key Takeaways

- Steps to enable secure connections between UCM and Webex Calling
  - CUCM Configuration(Certificate, Secure SIP Trunk, Secure IP Phone and Endpoint)
  - Secure LGW Configuration

- How to troubleshoot Secure Connections
  - Network problem(TCP and TLS negotiation)
  - Call Routing & Signaling problem（SIP registration and dial-peer matching）
  - Media problem（SRTP encryption and SRTP-RTP interworking）

The bridge to possible

Thank you




cisco Live!
Let's go
#CiscoLive