

Secure SIP Cisco UCM Configuration

Secure SIP Queue Manager Enterprise and Auto Attendant configuration

Effective Spring 2020, Imagicle Queue Manager Enterprise and relevant Auto Attendant module supports Secure SIP trunk and Secure RTP audio streams, for calls which are placed with Secure SIP (SIP/TLS) for the signalling and SRTP for the audio stream. Please note this requires at least CuCM versions 11.0 or newer.

Requirements

Before trying to enable Secure calls, please make sure Imagicle Queue Manager is fully configured to handle Non-Secure calls with clear RTP.

Mixed mode must be enabled on your Unified CallManager, and you must be able to effectively place and receive secure calls to and from the agents' phones.

Cisco Unified CallManager® Configuration

To be able to handle QME secure calls, you need to:

1. Configure Enterprise Parameters for SRTP.
2. Load the Imagicle digital certificate on CuCM, categorized as CallManager-trust
3. Create a SIP Trunk Security Profile which references the Imagicle Certificate
4. Create a SIP trunk which points to the Imagicle Application Suite machine, port 5063, and uses the SIP Trunk Security Profile

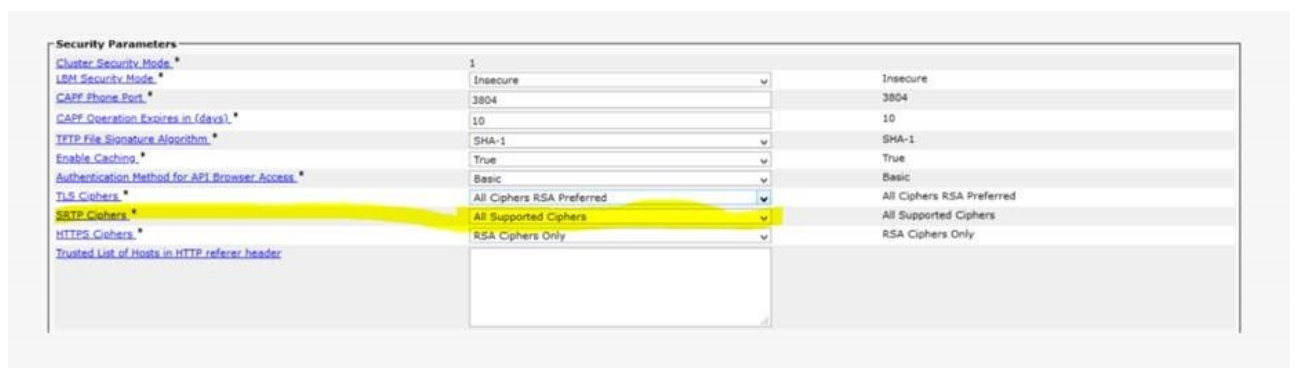
Warning: if a firewall is set between the CallManager nodes and the Application Suite servers, the TCP port 5063 must be allowed on both sides.

Configure Enterprise Parameters for SRTP

The longest cipher key length supported by Imagicle Queue Manager Enterprise for SRTP voice encryption is **128 bit**. Therefore, the SRTP cipher set configured on CUCM shall allow such key length.

On CUCM admin portal:

- Select *System -> Enterprise Parameters*
- Move to the "*Security Parameters*" section and ensure the parameter **SRTP Ciphers** allows AES-128 bit cipher algorithm (hence choose "All Supported Ciphers").



Download the Imagicle Certificate from IAS and Upload it on CUCM

Please follow the procedure highlighted [here](#).

Creating a SIP Trunk Security Profile with Encryption

From the Cisco Unified CM Administration menu, select System, Security, Sip Trunk Security Profile.

Add a new item with the following properties:

- **Incoming Transport Type:** TLS
- **Outgoing Transport Type:** TLS
- **Incoming port:** 5063
- **Accept Out of Dialog Refer:** enabled
- **Accept Unsolicited Notification:** enabled
- **Accept replaces header:** enabled
- **X.509 Subject Name:** enter the Imagicle Digital Certificate Common Name you noted before.

SIP Trunk Security Profile Information	
Name*	SIP Trunk Encrypted Security Profile Imagicle
Description	SIP Trunk Encrypted Security Profile Imagicle 5063
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	WIN-TN8S35M6791
Incoming Port*	5063
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

Please mind the certificate name. Do not enter the certificate description. Do not enter the full Subject Name. Enter the **Common Name**.

If you are unsure, select System, Security, Certificate, and press the Find button. Locate the Imagicle certificate. The **Common Name** is displayed in the Subject Name column, just after CN=

Status

i 4 records found

Certificate Configuration (1 - 4 of 4)

Find Certificate Configuration where

Subject Name

begins with

Find

Clear Filter

Subject Name ^	Issuer Name
O=Imagicle S.p.a.,CN=DEV060	O=Imagicle S.p.a.,CN=DEV060
O=Imagicle S.p.a.,CN=WIN-TN8S35M6791	O=Imagicle S.p.a.,CN=WIN-TN8S35M6791
O=Imagicle S.p.a.,CN=Windows2012Pol	O=Imagicle S.p.a.,CN=Windows2012Pol

NOTE: If you need to manage multiple QME nodes, you must specify in the X.509 Subject Name of the SIP Trunk security profile the list of the involved certificates CN (one for each Imagicle server), separated by comma.
For instance: WIN-TN8S35M6791,WIN-TN3V45K2V27

Creating a SIP Trunk for Secure SIP Queue Manager

A Secure Sip Trunk is a standard SIP trunk with the following properties:

- A descriptive name, such as QME_SIP_Trunk_Encrypted
- **SRTP Allowed** enabled
- **Run On All Active Unified CM Nodes** enabled

☐ Transmit UTF-8 for Calling Party Name

☐ Transmit UTF-8 Names in QSIG APDU

☐ Unattended Port

☒ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Consider Traffic on This Trunk Secure*

When using both sRTP and TLS

Route Class Signaling Enabled*

Default

Use Trusted Relay Point*

Default

☐ PSTN Access

☒ Run On All Active Unified CM Nodes

- **Destination Address:** the IP Address of the Imagicle Application Suite server
- **Destination Port:** 5063
- **SIP Trunk Security Profile:** reference the one you just created

Route Patterns

A route pattern is needed to route incoming, encrypted calls to the Queue Manager Enterprise. The route pattern pointing to *QME_SIP_Trunk_Encrypted* should be defined accordingly with the PBX numbering plan and with the queues phone number. For example, defining a route pattern 8XX will allow to manage queues with phone number 801, 802, etc..

The route patterns and the other rules used to send calls to QME should never change the called party number. This way QME will be able to tell which calls are coming back from the operators or other queues.

Pattern Definition	
Route Pattern*	7XXX
Route Partition	PT_ImagicleProduzioneInterni
Description	Towards Imagicle QME
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	192.168.204.165 (Edit)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error
Call Classification*	OffNet
<input type="checkbox"/> Allow Device Override <input checked="" type="checkbox"/> Provide Outside Dial Tone <input type="checkbox"/> Allow Overlap Sending <input type="checkbox"/> Urgent Priority	
<input type="checkbox"/> Require Forced Authorization Code	
Authorization Level*	0
<input type="checkbox"/> Require Client Matter Code	

Another route pattern must be defined to match the Camp-On prefix. Ensure that allows to reach the configured prefix followed by all the digits of the internal extensions.

Pattern Definition	
Route Pattern*	*!
Route Partition	PT_ImagicleProduzioneInterni
Description	QME CampOn
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence*	Default
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	192.168.204.165 (Edit)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error
Call Classification*	OnNet
<input type="checkbox"/> Allow Device Override <input checked="" type="checkbox"/> Provide Outside Dial Tone <input type="checkbox"/> Allow Overlap Sending <input type="checkbox"/> Urgent Priority	
<input type="checkbox"/> Require Forced Authorization Code	
Authorization Level*	0
<input type="checkbox"/> Require Client Matter Code	

Once the system is configured and running, if your extensions are (for example) four digits long (3001, 3002...) you can test Camp-On by dialling *3001.

TAPI devices association

CTI/TAPI Monitoring of operators/agents phones is required. Pls. follow the guidance available [here](#).

Mixed environments

QME can manage on its secure SIP trunk only calls from/to secure devices. If you need the QME can manage calls both from secure and unsecure devices, you need to:

- define two SIP trunks for each QME server (one not secure and one secure, as described above);
- configure secure devices (phones/VG) to reach QME queues through the secure SIP trunk;
- configure unsecure devices (phones/VG) to reach QME queues through the unsecure SIP trunk;

that basically requires to define on CUCM:

- 2 different partitions;
- 2 different CSS;
- 2 different route lists (secure + unsecure);
- 2 different route patterns for each queue number or range to be routed to QME;