

October 8, 2018





Page 2

Introduction

This document is intended to support you with the integration of XCAPI into an existing environment of the Cisco Unified Communications Manager. In the following sections we describe the essential configuration steps for SIP trunking to allow optimal interworking of both, the XCAPI and the Cisco Unified Communications Manager.

Though being based on the Cisco Unified Communications Manager 12 series, this document is applicable with other versions given a few adjustments.

At this point we suppose that the Cisco Unified Communications Manager environment and the physical or virtual application server is available and accessible through the network. Application server in this context mean, a server with a recent available Microsoft Windows operating system with latest updates and patches included. Further, that the XCAPI and the CAPI 2.0 voice or fax application is properly installed. It is also supposed that the public network access via ISDN and/or SIP is given and properly working, also in context with the custom and country dependent numberings and call routings. The same goes for the networking (LAN, WAN, DMZ, NAT, Firewall) itself as such topics are beyond the scope of this document and thus not shown here at all. Please refer to the respective manufacturer documentations, manuals and examples in such cases.

However, independent of the deployed application, the SIP connection can be tested with the XCAPI's included test application (xtest.exe) that is available within the XCAPI's installation folder (by default $\Program Files (x86)\TE-SYSTEMS\XCAPI\)$. This test tool allows to check with inbound and outbound calls, fax and testing several supplementary services.

We recommend to visit our YouTube channel frequently for XCAPI related tutorials about licensing, the test tool, line monitor, tracing, analyzing and others. Registered community users can check about latest documents, TechNotes and releases for XCAPI.

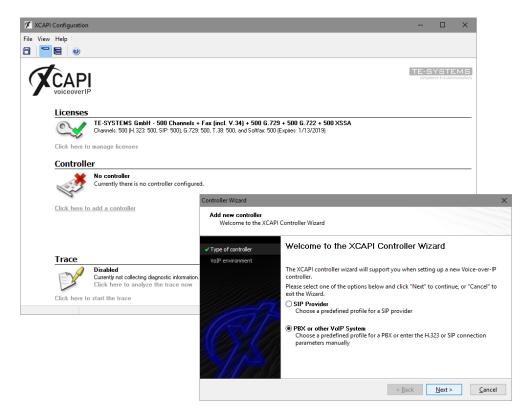


XCAPI Configuration

Please start up the XCAPI configuration to create a new controller assigned to the Cisco Unified Communications Manager.

If you've just installed the XCAPI and start the configuration tool for the first time or no controller is available at all, the XCAPI controller wizard will pop up automatically. To start up the XCAPI controller wizard manually, the hyperlink labeled **Click here to add a controller** on the main page has to be clicked.

Next select PBX or other VoIP System in the initial Type of controller dialog and proceed with the Next button.





Page 4

2.1 VoIP Environment

The next dialog lists some common Voice-over-IP environments. Selecting one of those will set up the XCAPI controller with a selection of near-optimal presets, sparing you manual configuration.

Add new controller Select the Voice-over-I	P environment
Type of controller VoIP environment	Select the environment for the new controller to operate in. If the list below does not contain your PBX you should select a compatible or one of the generic environments
Description and channels	
Signaling protocol Cisco CallManager/Cisco Unified Communications Manager	Avaya IP Office 8.0/9.0 Avaya SES (Session Enablement Services) AVM FRITZIBox WLAN 7370 AVM FRITZIBox WLAN 7370 beroNet beroffix VoIP Gateways bintec elmeg be.IP Series brekeke SIP Server/brekeke PBX Cisco Gutified Communications Manager Cisco Gutified Communications Manager Clarity Communication Center Dialogic® 1000 Media Gateway Dialogic® 2000 Media Gateway

2.2 Description and Channels

When the VoIP environment was selected, the next dialog allows to set a description for the controller. Also the number of channels that the new controller will be able to provide can be set. Here you enter how many simultaneous connections the XCAPI controller should handle when communicating with the Cisco Unified Communications Manager and the bound CAPI 2.0 application.

Add new controller Provide a description	and select the number of channels
✓ Type of controller ✓ VoIP environment	Please enter a meaningful description for the new controller and decide how many channels should be available for applications. Please consider that the effective number of available channels depend on the installed license.
Description and channels	
Signalling protocol Cisco CallManager/Cisco Unified Communications Manager	Description Cisco Unified Communications Manager Channels 20
	< Back Next > Cancel



Page 5

2.3 Signaling Protocol

The next dialog shows a list of signaling protocols which are supported for the given Voiceover-IP environment. According to this example the SIP protocol is selected.

Type of controller	Each voice-over-ip network operates with a specific voice-over-ip protocol like H.323 or SIP. The list below contains any voice-over-ip protocol that may be used with the
VoIP environment	selected environment. Please select the protocol from the list that is used in your
Description and channels	network.
Signalling protocol	H.323 SIP
Cisco CallManager/Cisco Unified Communications Manager	Ph-
Network Interface	
Port Allocation	
Confirmation	

2.4 IP Address of the Cisco Unified Communications Manager

Next the IP address or host name of Cisco's environment must be provided. In this example the CUCM's Ethernet address is using 172.18.0.124.

Controller Wizard		\times
Add new controller Provide the address o	f the Cisco CallManager/Cisco Unified Communications Manager	
Type of controller VoIP environment Description and channels	Provide the IP address of the Cisco device in the network. If there is more than one Cisco device present in the network be sure to provide the IP address of the Cisco device that you want to use.	
 Signalling protocol 	CCM/CUCM address	
 Cisco CallManager /Cisco Unified Communications Manager 	172.18.0.124	
Network Interface Port Allocation Confirmation		
	< <u>Back</u> <u>Next</u> <u>Cancel</u>	



Page 6

2.5 Network Interface

Afterwards, select the network interface that will control the inbound and outbound communications. Note that this is the XCAPI controller used Ethernet interface which will be leveraged for the SIP communication with the Cisco Unified Communications Manager.

Add new controller Select the network inte	rface	
/ Type of controller / VoIP environment / Description and channels	network, your syster	and gateway requires a physical connection to the voice-over- n needs a network-interface-controller (nic) with a link to this ct a certain nic from the list below.
Signalling protocol	Device	Comment
Cisco CallManager/Cisco Unified Communications Manager	172.16.0.153 172.16.0.153 172.10.0.1	Ethernet [B8-AE-ED-22-33-C3] Loopback Pseudo-Interface 1 Loopback Pseudo-Interface 1
Network Interface Port Allocation Confirmation		

2.6 Port Allocation

On demand and in the case of any router or firewall restrictions for UDP (RTP/T.38) a port range can be specified. In this example no range will be set which allows the XCAPI controller to use a random port range between 1024 and 65535.

Controller Wizard	×
Add new controller Provide information ab	nout port allocation
Yype of controller VoIP environment Vorpervision and channels Signalling protocol Gisco CallManager/Cisco Unified Communications Manager Network Interface Port Allocation Confirmation	If you want to operate this system behind a router/gateway it might be necessary to constrain local udp ports to a certain range. Constrain local udp ports to the following range 10000 - 10120
	< Back Next > Cancel



Page 7

2.7 Confirmation

The final wizard dialog performs some checks on the configuration parameters you've made. If errors are detected, use the **Back** button to correct the respective erroneous dialogs. Use the **Finish** button in order to create the new controller.

Controller Wizard		×
Add new controller Confirm that the prov	vided information is correct	
 ✓ Type of controller ✓ VoIP environment 	Click Finish to add the new controller with the configuration ye	ou have had made.
 VolP environment Description and channels 		
 Signalling protocol 		
 Cisco CallManager/Cisco Unified Communications Manager 		
✓ Network Interface		
Port Allocation		
Confirmation		
	< <u>B</u> ack <u>F</u> ini	sh <u>C</u> ancel

Now, the created controller is listed on the main page of XCAPI's configuration tool. Use the **save** button and exit the tool.

🛠 XCAPI C	Configuration			-		×		
File View I	Help							
A					YSTE			
ļ	Licenses							
	C.,	TE-SYSTEMS GmbH - 500 Channels + Fax (incl. V.34) + 500 (Channels: 500 (H.323: 500, SIP: 500), G.729: 500, T.38: 500, and Solifax:						
(Click here to	manage licenses						
9	Controlle	r						
	Click here to	Cisco Unified Communications Manager (172.15.0.153) 20 channels using TU 6.711 4-2w (54 kbit) (8000 Hz), TU 6.711 µ- at Cisco CallManager/Cisco Unified Communications Manager usi = Disable # Remove A Move up * Move down add a controller		ephone-Ev	ent (RFC	2833)		
	Trace							
-	De	Disabled Currently not collecting diagnostic information. Click here to analyze the trace now						
	Click here to	start the trace	Information				×	
			The configuration is now stored. Please marked are still active for the changes to take effe	estart all C ct.	API appli	cations th	at	
			Th fro	m the dev	ics applie ice becau n. The dia	ation has use the XC agnostics a	API has t	o perfo



Please note that the bound CAPI 2.0 application with its services must be completely stopped and restarted for the XCAPI controller changes to take effect. Restarting any of the XCAPI services won't help at all. Alternatively the Server where XCAPI is running on can be restarted. If enabled, the XCAPI diagnostic monitor pops-up with a re-initialization notification on success. Alternatively check with the **Events** tab of the **XCAPI Line Monitor** about a configuration update notification (Event ID 20).





In order to establish the communication between the Cisco Unified Communications Manager and the created XCAPI controller, a SIP trunk must be created. This enables XCAPI to be recognized as device handler for the Cisco environment. After creating the SIP trunk, a **Route Pattern** must be created for proper call-legs and call routings.

The SIP trunk must be related to some SIP and SIP Security Profiles. Some examples will be described in the following sections.

3.1 SIP Trunk Security Profile

First of all it is necessary to specify a **SIP Trunk Security Profile** which has to be applied to the XCAPI SIP trunk. The **SIP Trunk Security Profile** can be created or changed through the **Security** submenu of the **[System ▼]** tab. This profile can be used with or without **Digest Authentication**. Both methods will be described in detail here.

Besides the profile defaults, you may have to set the parameters **Accept Out-of-Dialog REFER**, **Accept Unsolicited Notification** and **Accept Replaces Header** for allowing supplementary services such as call transfer via SIP refer or message waiting indications via SIP Notify. Such services and XCAPI related configurations will be described in the chapter **Call Transfer** and **Message Waiting Indications** from page 37.

Sys	stem 🔻 Call Routing 👻 Media Reso	irces	Advanced Features Device	Application •	User Management 🔻
	Service Parameters				
	Security •		Certificate		
	Application Server		Phone Security Profile		
	Licensing		SIP Trunk Security Profile		
	Geolocation Configuration		CUMA Server Security Profile		
	Geolocation Filter	Г			
	E911 Messages				



3.1.1 SIP Trunk Security Profile without Digest Authentication

For running a SIP trunk without any digest authentication the **Enable Digest Authentication** must be disabled.

SIP Trunk Security Profile Configuration							
SIP Trunk Security Profile Informati	on						
Name*	XCAPI Non Secure SIP Trunk Profile						
Description	XCAPI Non Secure SIP Trunk Profile						
Device Security Mode	Non Secure V						
Incoming Transport Type*	TCP+UDP v						
Outgoing Transport Type	TCP v						
Enable Digest Authentication							
Nonce Validity Time (mins)*	600						
X.509 Subject Name							
Incoming Port*	5060						
Enable Application level authorization							
Accept presence subscription							
✓ Accept out-of-dialog refer**							
Accept unsolicited notification							
Accept replaces header							
Transmit security status	Transmit security status						
Allow charging header							
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter v						

3.1.2 SIP Trunk Security Profile with Digest Authentication

For this example the existing **Non Secure SIP Trunk Profile** will be copied, renamed to **XCAPI Non Secure SIP Trunk Profile with Digest Authentication** and adapted for using digest authentication. Of course a new SIP trunk could be created, it is just mandatory to set the **Enable Digest Authentication** parameter.

SIP Trunk Security Profile Inform	nation	
Name*	XCAPI Non Secure SIP Trunk Profile with Digest Authe	ntication
Description	XCAPI Non Secure SIP Trunk Profile with Digest Authe	ntication
Device Security Mode	Non Secure 🗸]
Incoming Transport Type*	TCP+UDP v	j
Outgoing Transport Type	TCP ¥]
Enable Digest Authentication		
Nonce Validity Time (mins)*	600	
X.509 Subject Name		
Incoming Port*	5060	
Enable Application level authoriza	tion	
Accept presence subscription		
✓ Accept out-of-dialog refer**		
Accept unsolicited notification		
Accept replaces header		
Transmit security status		
Allow charging header		
SIP V.150 Outbound SDP Offer Filteri	ng* Use Default Filter	1



Page 10

3.2 SIP Trunking

A new SIP trunk can be created by selecting the **Trunk** entry through the Cisco Unified Communications Manager [**Device** ▼] menu.

As described in the previous **SIP Trunk Security Profiles** chapters from **page 8**, the XCAPI related **SIP Trunk** can be used with or without digest authentication. The only difference has to be made by the selection of the corresponding **SIP Trunk Security Profile** which has the **Enable Digest Authentication** parameter set or not. If digest authentication is required additional configurations have to be made.

System 🔻	Call Routing 🔻	Media Resources 🔻	Advanced Features 🔻	Dev	vice 🔻	Application -	User Management 🔻
					CTI Ro	oute Point	
					Gatek	eeper	
					Gateway		
					Phone		
					Trunk		
					Remot	e Destination	
					Device	e Settings	



3.2.1 SIP Trunking without Digest Authentication

voiceoverIP

According to the selected protocol and the XCAPI SIP controller, the **Trunk Type** must be assigned to **SIP**. The **Device Protocol** parameter will be automatically set to **SIP** and the **Trunk Service Type** is used with **None (Default)**.

System Call Routing	✓ Media Resources ▼	Advanced Features 👻	Device 👻	Application -	User Management 👻	Bulk Administration 👻	Help 🔻
Trunk Configuration							
Next							
Status Status: Ready							
Trunk Information							
Trunk Type*	SIP Trunk		~				
Device Protocol*	SIP		~				
Trunk Service Type*	None(Default)		~				
Next							
i *- indicates req	uired item.						

The shown **Trunk Configuration** is basically used with the system given defaults. The **Device Name** identifier as well as the **Description** is set to xcapi.te-systems.de, the host name of the XCAPI controller's assigned Ethernet interface IP address.

Trunk Configuration		
- Device Information		
Product:	SIP Trunk	
Device Protocol:	SIP	
Trunk Service Type	None(Default)	
Device Name*	xcapi.te-systems.de	
Description	xcapi.te-systems.de	
Device Pool*	Default v	
Common Device Configuration	< None > v	
Call Classification*	Use System Default v	
Media Resource Group List	< None > v	
Location*	Hub_None v	
AAR Group	< None > v	
Tunneled Protocol*	None v	
QSIG Variant*	No Changes 🗸	
ASN.1 ROSE OID Encoding*	No Changes v	
Packet Capture Mode*	None v	
Packet Capture Duration	0	
Media Termination Point Required		
Retry Video Call as Audio		
Path Replacement Support		
Transmit UTF-8 for Calling Party Name		
Transmit UTF-8 Names in QSIG APDU		
Unattended Port		
SRTP Allowed - When this flag is checked, Er Failure to do so will expose keys and other in	ncrypted TLS needs to be configured in the network to provide en nformation.	nd to end security.
Consider Traffic on This Trunk Secure*	When using both sRTP and TLS v	
Route Class Signaling Enabled*	Default v	
Use Trusted Relay Point*	Default v	
PSTN Access		
Run On All Active Unified CM Nodes		



For the **Call Routing Information (Inbound and Outbound Call)** the parameter **Redirecting Diversion Header Delivery** has to be set. This enables the delivery of the origin and redirecting number through SIP. All other parameters are used with their defaults.

unk Configuration								
ntercompany Media Eng	gine (IME	.)						
.164 Transformation Profile	e < None	>		¥				
ILPP and Confidential A	ccess Lev	vel Information —						
ILPP Domain	< None >			~				
Confidential Access Mode	< None >			~				
Confidential Access Level	< None >			~				
	_							
all Routing Information	1							
Remote-Party-Id								
Asserted-Identity sserted-Type*								
	Default Default			~				
rust Received Identity*		of pult)		~				
	rust All (D	erault)		•				
Inbound Calls	_							
Significant Digits*		di		~				
Connected Line ID Presen		Default		~				
Connected Name Presenta	ation*	Default		~				
Calling Search Space		None >		Ý	-			
AAR Calling Search Space	• 🛓	None >		Ý]			
Prefix DN	L							
Redirecting Diversion I	Header De	slivery - Inbound						
If the administrator se Otherwise, the value of	configured	is used as the prefix	cupless the field	Lie omety in which	h case there is no	prefix assigne	d.	
otherwise, the value of	garaa		concess the new	ris empty in whic		Settings	Default Prefix Settir	ngs
Number Type		Prefix		trip Digits	Clear Prefix	Settings arch Space		ngs
		Prefix Default			Clear Prefix			ngs
Number Type Incoming Number	y Setting	Prefix Default	dicates call proce	trip Digits	Clear Prefix Calling Sec None >	el setting (De prefix assigne	Use Device Pool CSS	neter).
Number Type Incoming Number ¬Incoming Called Party If the administrator se	y Setting: to the pret	Prefix Default	dicates call proce	trip Digits	Clear Prefix Calling Sec None >	el setting (De prefix assigne	Use Device Pool CSS	neter).
Number Type Incoming Number	y Setting: to the pret	Prefix Default s fix to Default this ind is used as the prefix	dicates call proce	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Sec None >	el setting (De prefix assigne	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number	y Setting: its the prei	Prefix Default s fix to Default this in is used as the prefix Prefix	dicates call proce	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Sec < None > efix at the next level h case there is no Clear Prefix Calling S	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number - Incoming Called Party If the administrator se Otherwise, the value or Number Type Incoming Number - Connected Party Setti	y Setting: ets the pretionfigured	Prefix Default 5 Tix to Default this in is used as the prefix Prefix Default	dicates call proce	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Sec < None > efix at the next level h case there is no Clear Prefix Calling S	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number	y Setting: ets the pretionfigured	Prefix Default 5 Tix to Default this in is used as the prefix Prefix Default	dicates call proce	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Sec < None > efix at the next level h case there is no Clear Prefix Calling S	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number - Incoming Called Party If the administrator se Otherwise, the value or Number Type Incoming Number - Connected Party Setti	y Setting ets the preterministry of the set ings	Prefix Default Tix to Default this int is used as the prefix Default TSS < None >	dicates call proc	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Set Contact of the set of the s	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number	y Setting ets the preterministry of the set ings	Prefix Default Tix to Default this int is used as the prefix Default TSS < None >	dicates call proc	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Set Contact of the set of the s	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number	y Setting: tts the prel configured ings ormation C	Prefix Default fix to Default this int is used as the prefix Prefix Default CSS < None > rty Transformation (dicates call proc	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Se	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number	y Setting: tts the prel configured ings ormation C	Prefix Default Tix to Default this int is used as the prefix Default TSS < None >	dicates call proc	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Set Contact of the set of the s	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator se Otherwise, the value o Number Type Incoming Number Connected Party Setti Connected Party Setti Connected Party Setti Use Device Pool Called Called Party Transformati Galled Party Transformati	y Setting: ings ormation C innected Pa	Prefix Default Tix to Default this int is used as the prefix Default CSS < None > try Transformation CSS	dicates call proc	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Set V	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator se Otherwise, the value of Number Type Incoming Number Connected Party Transfor Outbound Calls Outbound Calls Outbound Calls Outbound Calls O'l ye Device Pool Called Called Party Transformatio Oil ye Device Pool Called	y Setting: tts the pretionfigured ings ormation C nnected Pa ion CSS d Party Tra- ion CSS	Prefix Default Default ix to Default this int is used as the prefix Default SSS < None > CNONE > SSS < None > CNONE > SSS < None > CSS	dicates call proc	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Se	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator se Otherwise, the value or Number Type Incoming Number Connected Party Setti Connected Party Setti Connected Party Setti Outso Device Pool Calle Ø Use Device Pool Callis Ø Use Device Pool Callis Ø Use Device Pool Callis	y Setting: tts the pretionfigured ings ormation C nnected Pa ion CSS d Party Tra- ion CSS	Prefix Default Trix to Default this inti is used as the prefix Default Default CSS < None > rty Transformation (CSS < None > ansformation CSS	dicates call proc	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Se Calling S	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number - Incoming Called Party If the administrator se Otherwise, the value or Number Type Incoming Number - Connected Party Setti Connected Party Setti Connected Party Setti Outbound Calls Called Party Transformati I use Device Pool Callin Calling Party Transformati I use Device Pool Callin Calling Party Selection [↑]	y Setting ets the pref ings ormation C innected Pa ion CSS d Party Tra- ion CSS ng Party Tr	Prefix Default Tix to Default this in is used as the prefix Default SSS < None > Try Transformation CS < None > ansformation CSS Originator	dicates call proc	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Ser Calli	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator se Otherwise, the value of Number Type Incoming Number Connected Party Transfor Use Device Pool Calle Called Party Transformati Use Device Pool Calle Calling Party Transformati Use Device Pool Calle Calling Party Transformati Use Device Pool Calle Calling Party Calling Party Calling Party Calling Party Calling Party Calling Party Calling Party Device Pool Calle	y Setting: ings ormation C innected Pa ion CSS d Party Tra ion CSS ig Party Tr on *	Prefix Default Default Tix to Default this int is used as the prefix Default SSS < None > Try Transformation CS < None > ansformation CSS < None > ansformation CSS	dicates call proc	trip Digits essing will use provide the provided the prov	Clear Prefix Calling Set (None > Clear Prefix Calling 5 (None > Clear Prefix (None >	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator set Otherwise, the value of Number Type Incoming Number Connected Party Settit Connected Party Settit Connected Party Transfor Outbound Calls Outbound Calls Outbound Calls Outbound Calls Outbound Calls Obse Device Pool Calles Called Party Transformati Ø use Device Pool Calles Calling Into ID Presentation Calling Name Presentation	y Setting the prelimination of the prelimination of	Prefix Default Default Tix to Default this int s used as the prefix Default Default SSS < None > Try Transformation CSS < None > ansformation CSS < None > Default Default Default Default Default Default Default	iicates call proceeding of the field	trip Digits essing will use pro- is empty in whic Strip Digits	Clear Prefix Calling Ser Calli	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator se Otherwise, the value of Number Type Incoming Number Connected Party Setti Connected Party Setti Outbound Calls Called Party Transformati Ø Use Device Pool Callin Calling Party Transformati Ø Use Device Pool Callin Calling Party Transformati Calling Into IP presentatio Calling Into IP presentatio Calling and Connected Pa	y Setting the previous of the	Prefix Default Trix to Default this inti is used as the prefix Default Default CNORe > rty Transformation (CSS < None > ansformation CSS < None > ansformation CSS 	iicates call proceeding of the field	trip Digits essing will use pro- is empty in whic Strip Digits	Clear Prefix Calling Set (None > Clear Prefix Calling 5 (None > Clear Prefix (None >	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator se Otherwise, the value or Number Type Incoming Number Connected Party Setti Connected Party Setti Ouse Device Pool Calle Outbound Calls Outbound Calls Outbound Calls Outbound Calling Party Transformati Ouse Device Pool Calle Calling Party Selection* Calling Party Selection* Calling narty Selection* Calling Connected Pa	y Settling the the pretion on Figure d monofigure d monor constraints of the setting on CSS for the setting d Party Tr on * n* n*	Prefix Default Trix to Default this init is used as the prefix Default SSS < None > Try Transformation CS < None > ansformation CSS < None > ansformation CSS Originator Default Default Default Default Default Default Default Default	iicates call proceeding of the field	trip Digits essing will use pro- is empty in whic Strip Digits	Clear Prefix Calling Ser <	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator se Otherwise, the value o Number Type Incoming Number Connected Party Stett Connected Party Stett Outbound Calls Use Device Pool Con Outbound Calls Outbound Calls Use Device Pool Callet Calling Party Transformati Use Device Pool Callet Calling Party Selection* Calling In ID Presentatii Calling In ID Presentatii Calling Connected Pa Bredirecting Diversion 1 Redirecting Party Transfor	y Setting: ings momentation of a set of the	Prefix Default	iicates call proceeding of the field of the	trip Digits essing will use pro- is empty in whic Strip Digits	Clear Prefix Calling Ser Calli	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator set Otherwise, the value of Number Type Incoming Number Connected Party Setti Connected Party Setti If Use Device Pool Called Called Party Transformati If Use Device Pool Called Calling Party Transformati Calling Into ID Presentation Calling Into ID Presentation Calling and Connected Party Transformation Redirecting Diversion I Redirecting Party Transformation Wese Device Pool Redin	y Setting: ings momentation of a set of the	Prefix Default	iicates call proceeding of the field of the	trip Digits essing will use pro- is empty in whic Strip Digits	Clear Prefix Calling Ser <	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator set Otherwise, the value of Number Type Incoming Number Connected Party Settit Connected Party Settit Connected Party Settit Connected Party Transformativ W use Device Pool Callen Called Party Transformativ W use Device Pool Callen Calling Party Transformativ W use Device Pool Callen Calling Name Presentation Calling and Connected Party Calling Party Transformativ Wase Device Pool Callen Calling Name Presentation Caller Information	y Setting: ings momentation of a set of the	Prefix Default	iicates call proceeding of the field of the	trip Digits essing will use pro- is empty in whic Strip Digits	Clear Prefix Calling Ser <	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter).
Number Type Incoming Number Incoming Called Party If the administrator set Otherwise, the value or Number Type Incoming Number Connected Party Setti Connected Party Setti Outbound Calls Called Party Transformati Outbound Calls Calling Party Transformati Outbound Calling Party Transformati Outbound Calling Party Transformati Outbound Calling Party Transformati Outbound Party Transformation Calling Name Presentation Calling Name Presentation Calling Party Stelection* Use Device Pool Redire Outbound Caller In D N	y Setting. ings momentation C annected Pa momentation C d Party Trr n* n* methode Pa on * n* methode Pa on * methode Pa	Prefix Default	iicates call proceeding of the field of the	trip Digits essing will use pro- is empty in whic Strip Digits	Clear Prefix Calling Ser <	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter). Igs
Number Type Incoming Number Incoming Called Party If the administrator set Otherwise, the value of Number Type Incoming Number Connected Party Settit Connected Party Settit Connected Party Settit Connected Party Transformativ W use Device Pool Callen Called Party Transformativ W use Device Pool Callen Calling Party Transformativ W use Device Pool Callen Calling Name Presentation Calling and Connected Party Calling Party Transformativ Wase Device Pool Callen Calling Name Presentation Caller Information	y Setting. ings momentation C annected Pa momentation C d Party Trr n* n* methode Pa on * n* methode Pa on * methode Pa	Prefix Default	iicates call proceeding of the field of the	trip Digits essing will use pro- is empty in whic Strip Digits	Clear Prefix Calling Ser <	el setting (De prefix assigne Settings	Use Device Pool CSS vicePool/Service Parar d. Default Prefix Settim Use Device Pool CSS	neter). Igs



In this example the **Destination Address** is set to the host name xcapi.te-systems.de. The SIP Trunk Security Profile as mentioned in the chapter from page 8, is set to XCAPI Non Secure SIP Trunk Profile. The parameters Destination Address is an SRV, Destination Port, MTP Preferred Originating Codec and Presence Group of the SIP Information section are used with their defaults.

If required the Rerouting, Out-Of-Dialog Refer and SUBSCRIBE Calling Search Space parameters has to be set.

The DTMF Signaling Method is used with RFC 2833.

Note that it is not necessary to reset the newly created SIP trunk when the Route Pattern will be added afterwards.

Trunk Configuration						
SIP Information						
_ Destination						
Destination Address is an SRV						
Destination Address	Destination Ad	dress IPv6	Destination Port	Status	Status Reason	Duration
1* xcapi.te-systems.de			5060	N/A	N/A	N/A
MTP Preferred Originating Codec*	711ulaw		V			
BLF Presence Group*	Standard Presence gr	oup	~			
SIP Trunk Security Profile*	XCAPI Non Secure SI	P Trunk Profile	×			
Rerouting Calling Search Space	< None >		~			
Out-Of-Dialog Refer Calling Search Space	< None >		~			
SUBSCRIBE Calling Search Space	< None >		~			
SIP Profile*	Standard SIP Profile		~	View Details		
DTMF Signaling Method*	RFC 2833		~			
Normalization Script < None >		~				
Enable Trace		+				
Parameter Nan	ie .		Parameter Value			
1					± =	
Recording Information						
None						
O This trunk connects to a recording-e	nabled gateway					
O This trunk connects to other clusters	with recording-enable	d gateways				
-Geolocation Configuration						
Geolocation < None >		~				
Geolocation Filter < None >		~				
Send Geolocation Information						

Please note that the **Rerouting, Out-Of-Dialog Refer and SUBSCRIBE Calling Search Space** parameters must be assigned for appropriate SIP trunk rights. Wrong calling search space relations will cause call and/or call transfer failures. A good indicator for of incorrect routing would be **404 Not Found** notifications in reply of a SIP Invite or SIP Refer from the Cisco Unified Communications Manager.







VOICEOVERIP

Creating SIP Trunks with Digest Authentication is similar to the ones without any authentication as previously described in the chapter SIP Trunks on page 10. Please note that the SIP Trunk Security profile for Digest Authentication must be handled in a separate profile. The SIP trunk profile, named Non Secure SIP Trunk with Digest Authentication, will be described in the chapter SIP Trunk Security Profiles starting on page 8.

SIP Information —								
-Destination								
Destination Add								
	ination Address	Destination A	ddress IPv6	Destination	Port	Status	Status Reason	Duration
1* xcapi.te-syst	ems.de			5060		N/A	N/A	N/A
MTP Preferred Origin	ating Codec*	711ulaw			/			
BLF Presence Group*	ĸ	Standard Presence g	roup		-			
SIP Trunk Security P	rofile*	Non Secure SIP Trun	k with Digest Au	thentication	-			
Rerouting Calling Sea	arch Space	< None >			~			
Out-Of-Dialog Refer	Calling Search Space	< None >			~			
SUBSCRIBE Calling S	Search Space	< None >			~			
SIP Profile*		Standard SIP Profile			View De	tails		
DTMF Signaling Meth	od*	RFC 2833			~			
-Normalization Sc	ript							
Normalization Scrip	t < None >		~					
Enable Trace								
	Parameter Nam	e		Paramete	r Value			
1						±		
-Recording Inform	lation							
None								
-	nects to a recording-er							
O This trunk conn	nects to other clusters	with recording-enable	ed gateways					
Geolocation Config	·							
	None >		¥					
_	None >		¥					
Send Geolocation	Information							



Page 15

3.2.2.1 User Management

An **Application User** must be created for allowing **Digest Authentication**. For this please select the **Application User's** configuration in the Cisco's **[User Management ▼]** tab.



For the **Application User Information** configuration, the required authentication information has to be defined. In this example, the **User ID** is set to **xcapi** and used with an arbitrary password. The parameters **Digest Credentials** and **Confirm Digest Credentials** are used for the **Digest Authentication** method. This is your SIP password that has to be set to the XCAPI controller as shown in the chapter **XCAPI with Digest Authentication** on page 16. The parameters **Accept Presence Subscription**, **Accept Out-of-Dialog REFER**, **Accept Unsolicited Notification** and **Accept Replaces Header** are enabled. The **Device Information** parameters aren't modified at all.

pplication User Configura	ation
Application User Informa	tion
User ID*	kcapi
Password	
Confirm Password	
Digest Credentials	
Confirm Digest Credentials	
BLF Presence Group*	Standard Presence group
	1-Default User Rank
Accept Presence Subscrip	tion
Accept Out-of-dialog REF	
Accept Unsolicited Notific	
Accept Replaces Header	
- · · ··	
Device Information	
Available Devices	Auto-registration Template SEPF8A5C5B2658B Device Association
	Sample Device Template with TAG usage examples Find more Route Points Find more Route Points
	v
	**
Controlled Devices	A
	✓
Available Profiles	
	v
	* *
CTI Controlled Device Profile	
	v
-CAPF Information	
Associated CAPF Profiles	A
	View Details
Permissions Information]
Groups	
	Add to Access Control Group
	View Details Remove from Access Control Group
Roles	
	View Details



3.2.2.2 XCAPI with Digest Authentication

voiceoverIP

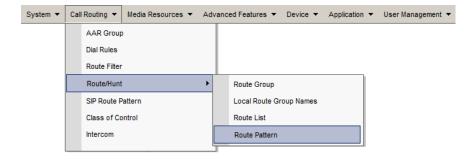
In accordance with Cisco's defined application user information, the given credentials must also be set to the XCAPI SIP controller. That ensures that the correct username and password will be used for proper authentication.

For enabling the authentication ensure that the Allow Digest Authentication is set.

XCAPI Configuration								-		×
File View Help										
Configuration	SIP	Options	Proxies	Registrations	Protocol	Timer	Overlap sending	Failover and	Overflow	
/ Information > 愛 Licenses (TE-SYSTEMS GmbH - 500 Channels + Fax) > 愛 CAPI 2.0 Options 員 Trace	The		r proxy as	well. The "con			nd are used to auth sed to provide a sp			ct
✓ ■ Controller	Use	rname			хсарі					
✓ ■ Cisco Unified Communications Manager ■ SIP	Use	rname (Aut	horizatio	n)						
TLS	Pas	sword			•••••	••••				
	Dis	olay Name								
Audio	Org	anization								
> III Network	Cor	itact								
>	SIP	Domain and	l Registra	tion						
Telephone-number-filter	The "Default SIP Domain" will be appended to any SIP address with a missing domain-part. The SIP Domain" will be appended to any local SIP address (i.e. in a FROM header) instead of the "De Domain".									
> 🍓 H.323 Tweaks	Def	ault SIP Dor	nain		172.18.0.1	24				
		ocal SIP Do	main							
	Aut	hentication								
	Please select the allowed authentication scheme. Since the username and password won't be en in the basic authentication scheme, it is not recommended to use the basic authentication scher							e encrypte cheme.	2d	
		Allow Basic	Authenti	cation						
	\bigtriangledown	Allow Diges	t Authent	ication						
	Ma	Authentic	ation Atte	empts	8]			

3.3 Route Pattern

Define XCAPI's SIP trunk required **Route Pattern** through the [Call Routing ▼] menu.





Page 17

In this example the route pattern **75.!** is used for XCAPI's SIP trunk **xcapi.te-systems.de**.

Route Pattern Configuration			
Pattern Definition			
Route Pattern*	75.!		
Route Partition	< None >	~	
Description	XCAPI route pattern	,	
Numbering Plan	Not Selected	~	
Route Filter	< None >	~	
MLPP Precedence*	Default	~	
Apply Call Blocking Percentage	L		
Resource Priority Namespace Network Doma	n < None >	~	
Route Class*	Default	~	
Gateway/Route List*	xcapi.te-systems.de		(Edit)
Route Option	 Route this pattern 		
	O Block this pattern No Error	~	
Call Classification* OffNet		7	
External Call Control Profile < None >		- 	
Allow Device Override Provide Outside		Urgant Briarity	
Require Forced Authorization Code			
Authorization Level*			
Require Client Matter Code			
Calling Party Transformations			
Use Calling Party's External Phone Number	r Mask		
Calling Party Transform Mask			
Prefix Digits (Outgoing Calls)			
Calling Line ID Presentation* Default		√	
Calling Name Presentation* Default			
Calling Party Number Type* Cisco CallMa	nager		
Calling Party Numbering Plan* Cisco CallMa	nager	~	
	-		
Connected Party Transformations			
Connected Line ID Presentation* Default		v	
Connected Name Presentation* Default		¥	
Called Party Transformations			
Discard Digits <pre></pre>		×	
Called Party Transform Mask			
Prefix Digits (Outgoing Calls)			
Called Party Number Type* Cisco CallMar			
Called Party Numbering Plan* Cisco CallMar	-		
Cisco Calimar	iayoi V	1	
ISDN Network-Specific Facilities Inform	ation Element		
Network Service Protocol Not Selected -	· · · · · · · · · · · · · · · · · · ·		
Carrier Identification Code			
Network Service	Service Parameter Name	Service Parameter Valu	e
Not Selected	✓ < Not Exist >		

Please ensure that the appropriate **Route Partition** is assigned to the SIP trunk's Calling Search Space for proper basic call and call transfer behavior.



Page 18

3.4 SIP Profile

A SIP profile can be configured through Cisco's **[Device ▼] [Device Settings ▶]** menu. You can specify a set of SIP attributes (timings, ports etc.) to the appropriate SIP trunks and SIP endpoints.

System 🔻	Call Routing 🔻	Media Resources 🔻	Advanced Features 💌	Dev	rice 🔻	Application •	User Manag	ement	■ Bulk Administration ■ Help ■
					CTI Ro	ute Point			
					Gateke	eeper			
					Gatew	ay			
					Phone				
					Trunk				
					Remot	e Destination			
					Device	e Settings	I	·	Device Defaults
									Firmware Load Information
									Default Device Profile
									Device Profile
									Phone Button Template
									Softkey Template
									Phone Services
									SIP Profile

In this example the **Standard SIP Profile** is used and assigned to XCAPI's SIP trunk as shown in the SIP trunking chapter on page 10.

SIP Profile Configuration							
_ Status							
(i) Status: Ready	(i) Status: Ready						
All SIP devices using this profile must be	e restarted before any cha	nges will take affect.					
•	,,						
SIP Profile Information							
Name*	Standard SIP Profile]				
Description	Default SIP Profile						
Default MTP Telephony Event Payload Type*	101						
Early Offer for G.Clear Calls*	Disabled	×					
User-Agent and Server header information*	Send Unified CM Version	Information as User-Agen' 🗸					
Version in User Agent and Server Header*	Major And Minor	v					
Dial String Interpretation*	Phone number consists o	f characters 0-9, *, #, anc ∨					
Confidential Access Level Headers*	Disabled	¥					
Redirect by Application							
Disable Early Media on 180							
Outgoing T.38 INVITE include audio mline							
Offer valid IP and Send/Receive mode on							
Use Fully Qualified Domain Name in SIP F	Requests						
Assured Services SIP conformance							
Enable External QoS**							
SDP Information	SDP Information						
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites * TIAS and AS \checkmark							
SDP Transparency Profile < None > v							
Accept Audio Codec Preferences in Received Offer* Default v							
Require SDP Inactive Exchange for Mid-	Call Media Change						
Allow RR/RS bandwidth modifier (RFC 3	556)						



Page 19

The following SIP profile parameters are used with their defaults.

SIP Profile Configuration						
Parameters used in Phone		Trunk Specific Configuration				
Timer Invite Expires (seconds)*	180	Reroute Incoming Request to new Trunk based on*	Never			
Timer Register Delta (seconds)*	5	Resource Priority Namespace List	< None > v			
Timer Register Expires (seconds)*	3600	SIP Rel1XX Options*	Disabled v			
Timer T1 (msec)*	500	Video Call Traffic Class*	Mixed v			
Timer T2 (msec)*	4000	Calling Line Identification Presentation*	Default v			
Retry INVITE*	6	Session Refresh Method*	Invite v			
Retry Non-INVITE*	10	Early Offer support for voice and video calls*	Disabled (Default value)			
Media Port Ranges	Common Port Range for Audio and Video	Enable ANAT				
incula i orcitaligea	Common Port Range for Audio and Video Separate Port Ranges for Audio and Video	Deliver Conference Bridge Identifier				
Start Media Port*	Separate Port Ranges for Audio and Video	Allow Passthrough of Configured Line Device Ca	ller Information			
Stop Media Port*	32766	Reject Anonymous Incoming Calls				
DSCP for Audio Calls	Use System Default	Reject Anonymous Outgoing Calls				
DSCP for Video Calls	Use System Default	Send ILS Learned Destination Route String				
DSCP for Audio Portion of Video Calls	Use System Default	Connect Inbound Call before Playing Queuing A	nnouncement			
DSCP for TelePresence Calls	Use System Default	SIP OPTIONS Ping				
DSCP for Audio Portion of TelePresence Calls		Enable OPTIONS Ping to monitor destination st	atus for Trunks with Service Type "None (Default)"			
Call Pickup URI*	x-cisco-serviceuri-pickup	Ping Interval for In-service and Partially In-service	e Trunks (seconds)* 60			
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup	Ping Interval for Out-of-service Trunks (seconds)	120			
Call Pickup Group URI*		Ping Retry Timer (milliseconds)*	500			
Meet Me Service URI*	x-cisco-serviceuri-gpickup	Ping Retry Count*	6			
User Info*	x-cisco-serviceuri-meetme					
DTMF DB Level*	None v	SDP Information				
Call Hold Ring Back*	Off v	Send send-receive SDP in mid-call INVITE				
Anonymous Call Block*	Off v	Allow Presentation Sharing using BFCP				
Caller ID Blocking*	Off Y	Allow iX Application Media				
Do Not Disturb Control*	User v	Allow multiple codecs in answer SDP				
Telnet Level for 7940 and 7960*	Disabled V					
Resource Priority Namespace	< None >					
Timer Keep Alive Expires (seconds)*	120					
Timer Subscribe Expires (seconds)*	120					
Timer Subscribe Delta (seconds)*	5					
Maximum Redirections*	70					
Off Hook To First Digit Timer (milliseconds)*	15000					
Call Forward URI*						
Speed Dial (Abbreviated Dial) URI*	x-cisco-serviceuri-cfwdall x-cisco-serviceuri-abbrdial					
	x-cisco-serviceuri-abbrdial					
Conference Join Enabled						
Semi Attended Transfer						
Enable VAD						
Stutter Message Waiting						
Stutter message waiting MLPP User Authorization						
Normalization Script						
Normalization Script < None >	×					
Enable Trace	Parameter Value					
1						
Incoming Requests FROM URI Settings						
Caller ID DN						
Caller Name						



Transport Layer Security

The requirements and configuration procedure for TLS (Transport Layer Security) will be described in the following sections.

4.1 XCAPI SIP Security Additions

To enable **XCAPI SIP Security Additions (XSSA)**, it is necessary to run the **XSSA installer**, on the application/XCAPI server. The current version is **1.8.3**. Please note that a server reboot is required after the XSSA installation.

It is possible to use the **XCAPI SIP Security Additions (XSSA)** application (the xssa-ldr executable) for generating RSA keys, self-signed certificates and certificate signing requests. Please note that those **RSA** keys will be generated within the folder where the **xssa-ldr** executable is called.

4.1.1 RSA Keys & Self-Signed Certificates

The Cisco UCM can handle RSA keys with an encryption level up to **2048 bit**. For this example the XSSA-loader (xssa-ldr.exe) is used to generate a 2048 bit RSA key via the command line using the hostname of the XCAPI server. The private key is stored as **xcapi-private-key.pem** while the **xcapi-public-key.pem** filename is used for the public key. The corresponding command line for this is used as shown below:

```
C\>xssa-ldr crytool generate rsa --bits=2048
--private=xcapi-private-key.pem
--public=xcapi-public-key.pem
```

Next, this RSA key is used for generating a self-signed certificate. This **xcapi-certificate.pem** is valid for 365 days.

```
C:\>xssa-ldr crytool generate certificate --private=xcapi-private-key.pem
--cn=xcapi.te-systems.de
--idn=xcapi.te-systems.de
--certificate=xcapi-certificate.pem
--days=365
```

4.1.2 CA-Signed Certificate

You can use the private key can to generate a **CSR (Certificate Signing Request)** file for requesting a CA-signed certificate. The next example shows how to create the **xcapi-csr.pem** file which is used for requesting a CA-signed certificate.

```
C:>xssa-ldr crytool generate csr --private=xcapi-private-key.pem
--cn=xcapi.te-systems.de
--idn=xcapi.te-systems.de
--csr=xcapi-csr.pem
```



4.2 Certificate Management

The **Certificate Management** is handled through the **[Security ▼]** menu of the **Cisco Unified Operating System Administration**.



The CUCMs generated **CallManager.pem** certificate, which is used for this example, is shown in the certificates list.

Show - Settings -	Show ▼ Settings ▼ Security ▼ Software Upgrades ▼ Services ▼ Help ▼						
Certificate List	ertificate List						
Generate Self-sign	Generate Self-signed 🕒 Upload Certificate/Certificate chain 📵 Generate CSR						
Status	Status 1 records found						
Certificate List	(1 - 1 of 1)						
Find Certificate List v	vhere Certificate v	is exactly	anager Find (Clear Filter 🔂 📼			
Certificate	Certificate Common Name Type Key Type Distribution Issued By Expiration Description						
CallManager <u>cucm12.testlab.te-systems.de</u> Self-signed RSA cucm12.wob.te-systems.de cucm12.testlab.te-systems.de 04/24/2023 Self-signed certificate generated by system							
Generate Self-sign	Upload Certificate/C	Certificate chain Ge	nerate CSR				

The **CallManager.pem** will be locally stored and has to be imported as **Trusted Certificate** to the XCAPI controller, which is described in detail in the chapter **Configuring the XCAPI SIP Security Additions** on page 28.

Certificate Details for	cucm12.testlab.te-systems.de, CallManager
Regenerate 💽 Ger	nerate CSR 🔋 Download .PEM File 🔋 Download .DER File
Certificate Settings	
File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly nan	ne) Self-signed certificate generated by system
SignatureAlgorithm: S Issuer Name: L=WolfS O=TE-SYSTEMS GmbH, Validity From: Wed Ap To: Mon Apr 2 Subject Name: L=Wol O=TE-SYSTEMS GmbH, Key: RSA (1.2.840.11 Key value:	pr 25 14:24:12 CEST 2018 4 14:24:11 CEST 2023 fsburg, ST=Niedersachsen, CN=cucm12.testlab.te-systems.de, OU=Testlab, C=DE



The generated XSSA certificate **xcapi-certificate.pem** has to be imported to the CallManager.

Show - Settings - Security - Software Upgrades - Services - Help -
Certificate List
Conerate Self-signed 🎒 Upload Certificate Certificate chain 🔃 Generate CSR
Certificate List
Find Certificate List where Certificate V begins with V Find Clear Filter
Generate Self-signed Upload Certificate/Certificate chain Generate CSR
Upload Certificate / Certificate chain Upload Certificate / Certificate chain Upload Certificate / Uploading a cluster-wide certificate will distribute it to all servers in this cluster Upload Certificate / Certificate chain Certificate Purpose* Description(finedy SetSigned CAE) cortificate Upload fined Upload fined Upload fined Cises

Afterwards, the XCAPI certificate will be shown in the certificate list.

		Rows per Page 250 🗸
Filter 🕂 🛥		
Issued By	Expiration	Description
xcapi.te-systems.de	08/31/2019	Self-signed XCAPI certificate
F	Issued By	Issued By Expiration

Please ensure that the **Subject** line, in this example **Subject: CN=xcapi.te-systems.de**, displays the correct host name. This must be correct for the **SIP Trunk Security Profile**, as shown in the next chapter on page 23.

Certificate Details		
🗙 Delete 🔋 Download	.PEM File Download .DER File	
Status		
(i) Status: Ready		
-Certificate Settings		
File Name	xcapi.te-systems.de.pem	
Certificate Purpose	CallManager-trust	
Certificate Type	trust-certs	
Certificate Group	product-cm	
Description(friendly name) Self-signed XCAPI certificate	
Certificate File Data		
Version: V3		^
Serial Number: 01	A1withRSA (1.2.840.113549.1.1.5)	
Issuer Name: CN=xcap		
Validity From: Fri Aug 3		
To: Sat Aug 31 Subject Name: CN=xcar	13:47:14 CEST 2019	
Key: RSA (1.2.840.113)		
Key value:		
	49b50e43565078bc58dd1b2cd164e15ab5bb3e1a5c731	
	d561618b2247f1f25b845b282cffad5dfaf14d458f5482f 7749028489e34952415a5ef919e3181894102e47df3a9	
	bba8ecac05707d69c543932770f6d389827bf8fdeac412	~
2866999f2c765c5e6d89f	b3619d749f1e012b2b6a2e531d867583cdd16b3eceaf3d	



4.3 SIP Trunk Security Profile for TLS

Enabling TLS requires a properly configured SIP Trunk Security Profile.



In this example the profile is used as follows:

- The Device Security Mode must be set to Encrypted.
- The Incoming and Outgoing Transport Type must be set to TLS.
- The X.509 Subject Name must be equivalent to the one of the XCAPI certificates, here xcapi.te-systems.de.
- The **Incoming Port** is set to **5061** which is also used as default TLS port by the XCAPI controller.
- The Accept out-of-dialog refer, Accept unsolicited notification and accept replaces header are used enabled.

System 👻	
SIP Trunk Security Profile Configurat	tion
🔜 Save 🗙 Delete 🗋 Copy 蠀	Reset 🥒 Apply Config 🕂 Add New
SIP Trunk Security Profile Informatio	n
Name*	XCAPI Security Profile
Description	SIP Trunk Security Profile for TLS
Device Security Mode	Encrypted V
Incoming Transport Type*	TLS V
Outgoing Transport Type	TLS V
Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	xcapi.te-systems.de
	\sim
Incoming Port*	5061
Enable Application level authorization	
Accept presence subscription	
✓ Accept out-of-dialog refer**	
Accept unsolicited notification	
Accept replaces header	
Transmit security status	
Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter



Page 24

4.4 SIP Trunking with TLS

The SIP trunk for TLS has to be created as a standard SIP trunk (see chapter **SIP Trunking** on page 10). Additionally the TLS secured SIP trunk must be used with an enabled **SRTP Allowed** parameter. In detail this trunk will be used as follows:

System - Call Routing - Media Resources - Advanced Features - Devic	e 🕶	
Trunk Configuration		
🔚 Save 🗙 Delete 😭 Reset 🕂 Add New		
_ Status		
(i) Status: Ready		
SIP Trunk Status		
Service Status: Full Service Duration: Time In Full Service: 2 days 19 hours 47 minutes		
Device Information		
Product:	SIP Trunk	
Device Protocol:	SIP	
Trunk Service Type	None(Default)	
Device Name*	xcapi.te-systems.de	
Description	XCAPI SIP Trunk for TLS	
Device Pool*	Default 🗸	
Common Device Configuration	< None >	
Call Classification*	Use System Default	
Media Resource Group List	< None >	
Location*	Hub_None V	
AAR Group	< None >	
Tunneled Protocol*	None 🗸	
QSIG Variant*	No Changes 🗸	
ASN.1 ROSE OID Encoding*	No Changes 🗸	
Packet Capture Mode*	None 🗸	
Packet Capture Duration	0	
Media Termination Point Required		
Retry Video Call as Audio		
Path Replacement Support		
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 co	nfigured in the network to provide end to end security. Fa	ilure 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		



Please ensure that the parameters for standard SIP trunking, **Redirecting Diversion Header Delivery - Inbound** and **Redirecting Diversion Header Delivery - Outbound** are enabled for redirection numbering support.

system 👻 Call Routing 👻 Media R	Resources - Advanced Feature	es 🔻 Device 👻				
runk Configuration						
🗐 Save 🗙 Delete 🏻 🎦 Rese	t 🕂 Add New					
Intercompany Media Engine (I	ME)					
E.164 Transformation Profile < No	one >	~				
MLPP and Confidential Access	Level Information					
MLPP Domain < None		~				
Confidential Access Mode < None	>	~				
Confidential Access Level < None	>	\sim				
Call Routing Information						
Remote-Party-Id						
Asserted-Identity						
Asserted-Type* Default		~				
SIP Privacy* Default		~				
Trust Received Identity* Trust All	l (Default)	~				
-Inbound Calls						
Significant Digits*	All		~			
Connected Line ID Presentation*			~			
Connected Name Presentation*	Default		~			
Calling Search Space AAR Calling Search Space	< None >		~			
Prefix DN	< None >					
Redirecting Diversion Header	Delivery - Inhound					
- Incoming Calling Party Setti						
If the administrator sets the used as the prefix unless the	prefix to Default this indicates field is empty in which case t	there is no prefix assign	ned.	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Otherwise, the value configured is
		Clear Prei	ix settings Dera	uit Prenx Settings		
		C1-1- D1-11-		c		Use Desides Deal con
Number Type	Prefix	Strip Digits	< None >	Calling Search Space	×	Use Device Pool CSS
	Prefix efault	Strip Digits	< None >	Calling Search Space	~	Use Device Pool CSS
	efault		< None >	Calling Search Space	V	
Incoming Number	efault	0				Ø
Incoming Number	efault ngs	o s call processing will us there is no prefix assign	e prefix at the next ined.	evel setting (DevicePool/Servi		
Incoming Number	sfault ngs prefix to Default this indicates field is empty in which case t	o s call processing will us there is no prefix assign Clear Pref	e prefix at the next ined.	evel setting (DevicePool/Servi ult Prefix Settings		Dtherwise, the value configured is
Incoming Number	efault	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next ined.	evel setting (DevicePool/Servi	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault ngs prefix to Default this indicates field is empty in which case t	o s call processing will us there is no prefix assign Clear Pref	e prefix at the next ined.	evel setting (DevicePool/Servi ult Prefix Settings		Dtherwise, the value configured is
Incoming Number	efault	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next ined.	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	efault ngs Frefix to Default this indicates field is empty in which case t Prefix efault	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next i ned. fix Settings Defa	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault ngs prefix to Default this indicates field is empty in which case t Prefix sfault n CSS < None >	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next ined.	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault ngs prefix to Default this indicates field is empty in which case t Prefix sfault n CSS < None >	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next i ned. fix Settings Defa	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault ngs prefix to Default this indicates field is empty in which case t Prefix sfault n CSS < None >	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next i ned. fix Settings Defa	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	efault ngs prefix to Default this indicates field is empty in which case t Prefix efault n CSS < None > Party Transformation CSS	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next i ned. fix Settings Defa	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault ngs prefix to Default this indicates field is empty in which case t Prefix fault n CSS < None > Party Transformation CSS Transformation CSS	o s call processing will us there is no prefix assign Clear Pref Strip Digits	e prefix at the next index.	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	efault ngs prefix to Default this indicates prefix efault n CSS < None > Party Transformation CSS	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next i ned. ix Settings Defa < None >	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	efault ngs prefix to Default this indicates field is empty in which case t Prefix efault n CSS [< None > Party Transformation CSS [< None > Transformation CSS [< None > Transformation CSS]	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next i ned. ix Settings Defa < None >	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number Dr Incoming Called Party Settii If the administrator sets the jused as the prefix unless the used as the prefix unless the incoming Number Dr Number Type Incoming Number Dr Connected Party Settings Connected Party Transformation Dr Connected Party Transformation CSS I Use Device Pool Called Party Called Party Transformation CSS Outbound Calls Calling Party Transformation CSS I Use Device Pool Called Party Calling Party Selection*	sfault ngs prefix to Default this indicates field is empty in which case t Prefix afault n CSS < None > Party Transformation CSS C None > Transformation CSS C None > Transformation CSS	o s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next i nec. ix Settings Defa	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault ngs refix to Default this indicates field is empty in which case t Prefix fault n CSS < None > Party Transformation CSS	o s call processing will us there is no prefix assign Clear Pref Strip Digits	e prefix at the next index. its Settings Defa < None > V V V V V V V V V	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	efault ngs prefix to Default this indicater field is empty in which case t Prefix efault n CSS < None > Party Transformation CSS Transformation CSS Transformation CSS Transformation CSS Transformation CSS	s call processing will us there is no prefix assign Clear Pref Strip Digits	e prefix at the next i need. It is Settings Defa V V V V V V V V V V V V	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	efault prefix to Default this indicate: field is empty in which case t Prefix efault n CSS < None > Party Transformation CSS Transformation CSS Transformation CSS Transformation CSS Transformation CSS Format* Format* Default Defaul	s call processing will us there is no prefix assign Clear Pref Strip Digits	e prefix at the next index. its Settings Defa < None > V V V V V V V V V	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault ngs prefix to Default this indicates field is empty in which case t Prefix afault n CSS < None > Party Transformation CSS (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (Default Default Default Default Deliver DN only in Deliver DN only in	s call processing will us there is no prefix assign Clear Pref Strip Digits	e prefix at the next i need. It is Settings Defa V V V V V V V V V V V V	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault sfault sfault sfault prefix to Default this indicates field is empty in which case t Pefix sfault n CSS < None > Party Transformation CSS S (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S)	s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next i nec. ix Settings Defa < None > V V V V V V V V V V V V V	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault sfault sfault sfault prefix to Default this indicates field is empty in which case t Pefix sfault n CSS < None > Party Transformation CSS S (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S)	s call processing will us there is no prefix assign Clear Pref Strip Digits	ie prefix at the next i nec. ix Settings Defa < None > V V V V V V V V V V V V V	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault sfault sfault sfault prefix to Default this indicates field is empty in which case t Pefix sfault n CSS < None > Party Transformation CSS S (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S)	o o cal processing will us chere is no prefix assign Clear Pref Strip Digits o	ie prefix at the next i nec. ix Settings Defa < None > V V V V V V V V V V V V V	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	sfault sfault sfault sfault prefix to Default this indicates field is empty in which case t Pefix sfault n CSS < None > Party Transformation CSS S (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (None > Transformation CSS (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S) (S)	o o cal processing will us chere is no prefix assign Clear Pref Strip Digits o	ie prefix at the next i nec. ix Settings Defa < None > V V V V V V V V V V V V V	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS
Incoming Number	efault prefix to Default this indicate field is empty in which case t Pefix efault n CSS < None > Party Transformation CSS C < None > Transformation CSS C < None > Transformation CSS C < None > Transformation CSS Fransformation CSS Fransformatic CSS Coriginat Default Default Default Default Default Default CSS < None > Party Transformation CSS Party Transformation CSS A None > A Non		ie prefix at the next i nec. ix Settings Defa < None > V V V V V V V V V V V V V	evel setting (DevicePool/Servi ult Prefix Settings	ce Parameter). (Dtherwise, the value configured is Use Device Pool CSS



Beside of the default values within the SIP Information dialog, the Destination Address is used with the host address xcapi.te-systems.de and the default port for TLS 5061. The SIP Trunk Security Profile is associated to the XCAPI-Server-TLS security profile.

System ▼ Call Routing ▼ Media Resources ▼ Advanced Features ▼ Device ▼						
Trunk Configuration						
Save 🗙 Delete 🍟 Reset 👍	Add New			_		
SIP Information						
SIP Information						
Destination						
Destination Address is an SRV						
Destination Address		Destination Address IPv6	Destination Port	Status		
1* xcapi.te-systems.de			5061	up		
MTP Preferred Originating Codec*	711ulaw	~				
BLF Presence Group*	Standard Presence group	~				
SIP Trunk Security Profile*	XCAPI Security Profile	~				
Rerouting Calling Search Space	< None >	~				
Out-Of-Dialog Refer Calling Search Space	< None >	~				
SUBSCRIBE Calling Search Space	< None >	~				
SIP Profile*	XCAPI SIP Profile	~	View Details			
DTMF Signaling Method*	RFC 2833	~				
Normalization Script						
Normalization Script < None >						
Parameter Name		Parameter Value				
1			± =			
Recording Information						
None						
O This trunk connects to a recording-e						
O This trunk connects to other clusters	with recording-enabled ga	teways				
Geolocation Configuration						
Geolocation < None >						
Geolocation Filter < None >		V				
Send Geolocation Information						
Send Geolocation Information						



4.5 Route Pattern

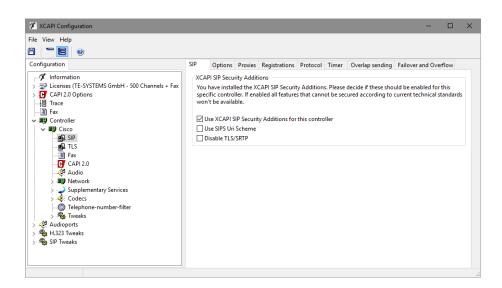
The Route Pattern for the TLS SIP trunk is used as shown:

System Call Routing					
Route Pattern Configuration					
Save 🗙 Delete 🗋 Copy 🕂 Add N	lew				
┌ Status					
i Status: Ready					
Pattern Definition					
Route Pattern *	,!				
Route Partition	XCAPIpartition 🗸				
Description	XCAPI route pattern				
Numbering Plan	Not Selected 🗸				
Route Filter	< None >				
MLPP Precedence*	Default 🗸				
Apply Call Blocking Percentage					
Resource Priority Namespace Network Domain	< None >				
Route Class*	Default 🗸				
Gateway/Route List*	xcapi.te-systems.de 🗸 (Edit)				
Route Option	Route this pattern				
	○ Block this pattern No Error ✓				
Call Classification* OffNet	×				
External Call Control Profile <pre></pre>	✓				
Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority					
Require Forced Authorization Code					
Authorization Level*					
Require Client Matter Code					



4.6 Configuring the XCAPI SIP Security Additions

For running XSSA it is necessary to enable the Use XCAPI SIP Security Additions for this controller option.



The self-generated **xcapi-certificate.pem** file, as described in the chapter **Certificate Management** on page 21 and the associated RSA key **xcapi-private-key.pem** must be uploaded through the XCAPI controllers **TLS Certificate** dialog.

🛠 XCAPI Configuration			-		\times
File View Help					
Configuration Information CAPI 2.0 Options CAPI 2.0 Options Controller Controller Controller Controller CAPI 2.0 CAPI 2.0 C	Certificate and Private Key During TLS connection establishmen and the corresponding RSA private I Certificate RSA Private Key	nt it is neccessary to authenticate with the remo	e peer using	a cettific	×



Within the **Trusted Certificates** dialog you have to import the **CallManager.pem** certificate, as shown in the chapter **Certificate Management** on page 21.

Finally you have to save the XCAPI controller changes and need to restart the CAPI application services.

XCAPI Configuration	- 0
ile View Help	Certificate Trusted Certificates Options
→ Information > 😳 Uccenses (TE-SYSTEMS GmbH - 500 Channels + Fax: > 🕞 CAPI 2.0 Options → Tarce → ■ Fax > ♥ Controller → ■ Fax → ■ Fax → ■ Fax → ■ Fax → ■ CAPI 2.0 → ■ CAPI 2.0 → ■ Autoork > → >> Supplementary Services → ■ Gets → ■ Teaks → ■ Toeks > ♦ ■ Network > → >> ■ Tweaks > ♦ H4233 Tweaks > ♦ SIP Tweaks > ♦ SIP Tweaks	Trusted Certificates During TLS connection establishment a remote peer is authenticated using the certificate presented by this peer.



Fax Services

In this chapter, we are going to describe configuring the fax services leveraging T.38 (including V.34), Softfax (G.711) and T.38 to Softfax fallback.

For faxing to function correctly it must be ensured that the Codec, Framing, Bandwidth and DTMF settings are set conform to the ones of the XCAPI controller configuration and other participating SIP instances.

Note that the XCAPI controller Fax dialog as well as T.38 (including V.34 support) to G.711 fallback support is available from XCAPI version 3.5.0. We strongly recommend using latest XCAPI versions for best results and it might be even be mandatory with latest manufacturer releases and firmware versions.



The fax related configurations for the Cisco gateway will be described in the chapter **Troubleshooting**, **Hints and Configuration Examples** from page 33. Please note that XCAPI does not support the **T.38** fax protocol through XSSA and enabled TLS.

5.1 SoftFax (G.711 Fax Pass Through)

In the **SoftFax** mode, the XCAPI simulates an analog fax device by transmitting modulated fax signals like a modem through the established G.711 audio channels. The **SoftFax (G.711 fax pass through)** fax method has to be enabled as shown below.

🛠 XCAPI Configuration		-	<
File View Help			
Configuration Configuration Configuration Configuration CAPI 2.0 Options Fax CAPI 2.0 Options T Is Fax CAPI 2.0 CAP	in the audio channel (Softfax). Selectii Fax Method V.34 Fax Support Enabled Fax Calling Tone/Fax Called Tone	sfer fax messages via T.38 signalling or via T.30 signalling encoded ng Disabled will also remove any configured fax codecs. Softfax (G.711 fax pass through) v ions start with a CED or CNG signal tone. Select whether these shall gotiation. before T.38 negotiation for V.34 only v before T.38 negotiation (in audio channel) v Default v	



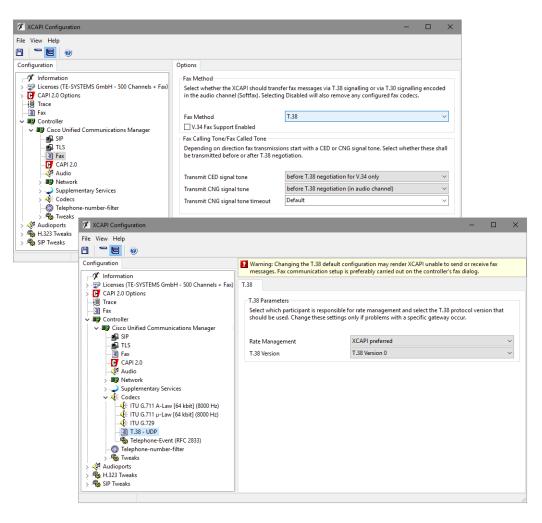
Page 31

5.2 T.38

In the case of T.38, using this fax method must also be supported and enabled for all other participating instances in between (SIP gateways, SIP provider, SBCs etc.). It is strongly recommended to avoid any kind of unnecessary transcoding (for e.g. G.711 to T.38 or vice versa) and using standard fax methods for all participating instances.

For enabling T.38 this Fax Method must be set as shown on the next screenshot.

Ensure that the **T.38** - **UDP** is available and enabled within the **Codecs** tab of the XCAPI controller configuration. One speech codec (in common G.711law or G.711 μ -law) must be enabled for the initial call establishment.







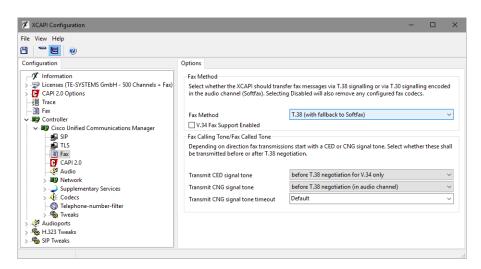
iceoverIP

T.38 with V.34 is available from XCAPI version 3.5.0 and Cisco VoIP gateways from version 15.1. To enable T.38 with V.34, **T.38** as well as **V.34 Fax Support** must be enabled within the XCAPI controllers **Fax** tab. The appropriate Cisco configurations will be described within the **Troubleshooting** section starting on page 33.

XCAPI Configuration		– 🗆 X
File View Help	Options	
Information Sevent Life SYSTEMS GmbH - 500 Channels + Fax) Gr CAPL20 Options Trace Trace Trace Sevent Life Controller Sevent Life Communications Manager Sevent Life Strate TLS	in the audio channel (Softfax). Select Fax Method ☑ V.34 Fax Support Enabled Fax Calling Tone/Fax Called Tone Depending on direction fax transmis:	nsfer fax messages via T.38 signalling or via T.30 signalling encoded ing Disabled will also remove any configured fax codecs.
Image: State	be transmitted before or after T.38 nd Transmit CED signal tone Transmit CNG signal tone Transmit CNG signal tone timeout	gotistion. before T.38 negotiation for V.34 only before T.38 negotiation (in audio channel) Default V

5.4 T.38 with G.711 Fax Fallback

The fax fallback can be enabled, also with **V.34 Fax Support**, as shown on the screenshot below. The corresponding Cisco configurations will be described within the **Troubleshooting** section starting on page 33. It is strongly recommended to check if this mode is supported by all participating VoIP instances, especially in the case of session border controller's or connected SIP providers. Depending on the VoIP environment additional configurations might be required. Incorrect configurations (not only for the ones of the XCAPI controller) will result in bad or non-working fax transmissions.





Troubleshooting, Hints and Configuration Examples

For best practice and functionality please read through the hints and examples of this section. The XCAPI related configurations for the given fax dial-peer examples can be reviewed in the chapter **Fax Services** from page 30.

6.1 Common Hints

- There are several protocols like **H.323**, **SIP** or **MGCP** that can be used for building up the connectivity between the Cisco Unified Communications Manager and a Cisco gateway. If the Cisco gateway and Cisco Unified Communications Manager connectivity is interacting via the SIP or H.323 VoIP protocol, the same protocol has to be used for the XCAPI trunk. Using different protocols for the VoIP environment commonly causes more issues (like DTMF functionality) and other side effects which require in-depth analysis.
- The dial-peer command **destination-pattern** is used for setting up the routing for the Cisco Unified Communications Manager and its connected gateway and can be used as well for the XCAPI trunk.
- You should give consideration to configuring dial-peers for routing the calls from the Cisco Unified Communications Manager to its gateway, as you cannot setup all necessary parameters within the global **voice service voip** dialog.
- The **called-number** dial-peer command can be used for utilizing its parameters for outgoing (outbound) call legs.
- In practice a wide range of matching calling numbers has to be routed which can be invoked with the **incoming called-number T** command.
- Use the dial-peer command answer-address for matching a specific calling number.

6.2 Frequent Issues

- In a case of working incoming (inbound) faxes with the outgoing (outbound) transmission always failing, it is recommended you check with the dial-peer that is used for the outbound route. In most cases it is incorrectly configured.
- If the XCAPI controller is configured to use the Softfax (G.711 Fax Pass Through) method but no outbound (outgoing) dial-peer is assigned a corresponding G.711 codec, the gateway will use the globally defined **voice service voip** code settings, which will probably be T.38. You can correct this by using commands like **incoming called-number T** or **answer-address 123456** for proper dial-peer matchings.
- If connections are rejected immediately or terminated after the call establishment, the root cause is mostly due to wrong or not conformed codec configurations. The related Cisco Unified Communications Manager dial-peer should be configured with a G.711 μ -Law codec which has to be enabled in the XCAPI controller also. However, this is normally the default setting for both instances.



Page 34

6.3 Network Clock

Wrong or faulty network clock configurations can be the reason for aborted faxes due to clocking and frame errors on the PRI. So if utilized, please check the proper PRI configurations and clocking or TX\RX errors. Example for the network:

network-clock-select 1 E1 0/0/0

6.4 MGCP

If using the **SoftFax (G.711 fax pass through)** method through an MGCP configured gateway, the dial-peer commands should be handled as follows. Do not set any of these MGCP commands:

```
mgcp modem passthrough voip mode nse
mgcp modem passthrough voip codec g711alaw (or codec g711ulaw)
mgcp fax t38 inhibit
mgcp fax t38 gateway force
```

Ensure that this MGCP command is set:

mgcp fax rate disabled

6.5 Using SoftFax (G.711 Fax Pass Through)

When running the SoftFax (G.711 fax pass through) method, you should avoid to enable commands like **fax protocol pass-through** or **fax protocol t.38**. Use the **fax rate disabled** command for disabling any gateway-sided fax detection for the related dial-peer.

SIP dial-peer example for using SoftFax (G.711 fax pass through):

```
dial-peer voice 800 voip
    destination-pattern 8...
    codec g711ulaw
    session protocol sipv2
    session target ipv4:192.168.1.100
    incoming called-number T
    dtmf-relay rtp-nte
    fax rate disable
```



6.6 Using SoftFax (G.711 Fax Pass Through) in Virtual Environments

The parameters **playout-delay nominal 250** and **playout-delay mode fixed** are used to specify a more graceful jitter buffer. So the handling of UDP/RTP packets might be handled in a more efficient way.

SIP dial-peer example, which is only used for outgoing facsimile transmissions when matching a specific prefix, for using SoftFax (G.711 fax pass through) in virtual environments:

```
translation-rule 2

Rule 1 8999990 0

dial-peer voice 8999990 voip

translate-outgoing called 2

incoming called-number 8999990

playout-delay nominal 250

playout-delay mode fixed

codec g711ulaw

fax rate disable

no vad
```

6.7 Using T.38

Using the T.38 fax protocol requires to set the **fax protocol t.38** command. It is recommended you enable **ECM** error correction mode. For this, you need to ensure that the **fax-relay ecm disable** command is NOT used.

SIP dial-peer example for using T.38:

```
dial-peer voice 800 voip
    destination-pattern 8...
    codec g711ulaw
    session protocol sipv2
    session target ipv4:192.168.1.100
    incoming called-number T
    dtmf-relay rtp-nte
    fax protocol t38 ls-redundancy 0 hs-redundancy
```



6.8 Using T.38 with V.34

Using the T.38 fax protocol requires you set up the **fax protocol t38 version 3** command. Make certain that the **fax-relay ecm disable** command has **NOT** been set because V.34 requires the error correction mode.

SIP dial-peer example for using T.38 with V.34:

```
dial-peer voice 800 voip
    destination-pattern 8...
    codec g711ulaw
    session protocol sipv2
    session target ipv4:192.168.1.100
    incoming called-number T
    dtmf-relay rtp-nte
    fax protocol t38 version 3 ls-redundancy 0 hs-redundancy 0 fallback none
```

6.9 Using T.38 with G.711 Fax Fallback

Using the T.38 fax protocol requires to set the **fax protocol t.38** command. We recommend enabling the **ECM** mode. For this, you need to be certain that the **fax-relay ecm disable** command is **NOT** used.

SIP dial-peer example for using T.38 with G.711 fallback:

```
dial-peer voice 800 voip
  destination-pattern 8...
  codec g711ulaw
  session protocol sipv2
  session target ipv4:192.168.1.100
  incoming called-number T
  dtmf-relay rtp-nte
  fax protocol t38 version 0 (or version 3 for V.34 support)
  ls-redundancy 0 hs-redundancy 0 fallback pass-through g711ulaw
```



Page 37

Call Transfer

For enabling call transfer via SIP refer, the **simulated ect by call-tromboning (line-interconnect)** parameter has to be disabled within the XCAPI controller **features** tab. Make certain the SIP Trunk Security Profile parameters **Accept Out-of-Dialog REFER** and **Accept Replaces Header** (see chapter **SIP Trunk Security Profiles** on page 8) and the **Application User Configurations** of the User Management dialog (see chapter **User Management** on page 15) are all enabled. You must also be certain that the corresponding Route Partition is assigned to the SIP trunk's calling search space for allowing proper basic calls and call transfers.

File View Help				
Configuration	ontroller	tures		
Joint Containen Joint Containen Joint CAPI 20 Options Joint CAPI 20 Joint CAPI 20	Simulate In cases : call-tran: Simul Notify Tunn Tr Hold/ DTMF Software These fe connecti	re the environment does not supp ye all-tromboning (line-inter- stination gnaling information to destination th replacement new relay ye decs	rconnect)	

Message Waiting Indications

For Message Waiting Indications via SIP Notify, the **Accept Unsolicited Notification** parameter must be enabled in the SIP Trunk Security Profile. Also check if the **SIP NOTIFY** method is enabled for XCAPI controller.

XCAPI Configuration -	×
File View Help	
Configuration MWI-Protocol Interset Options Interset State Controller Image: Signal message-waiting-indications (MWI) in your environment. Image: Signal message-waiting-indications (Signal message-waiting-indications) Image: Signal message-waiting-indications (Signal	Y



Page 38

XCAPI Outbound Failover

A XCAPI related outbound failover can be accomplished with setting up multiple gateway IP addresses within the controller **Proxies** tab. Each gateway has to be available and aware of the XCAPI SIP trunk. If required the valid **Default SIP Domain** of the Cisco environment has to be set within the XCAPI controller **Options** tab, otherwise the system may reject inbound calls from the application if XCAPI uses the wrong host part in SIP URIs. An example is given on the screenshot below.

File time Help	🖉 XCAPI Configuration								-		×
Configuration SP Option* Provies Registrations Protocol Timer Overlap sending Failover and Overflow Information Face information Face information are required to establish a connection and are used to authorize the user at the Fighter and/or provy as well. The "contact" field may be used to provide a special value for the contact hader replacing the default. Username (Authorization) Password Display Name Oganization Contact SP Domain and Registration File View Help File File File View Help File File File File File File File File	File View Help										
Information Informati											
Information Informati	Configuration	SIP	Options	Proxies	Registrations	Protocol	Timer	Overlap sendi	ing Failover a	nd Overflow	
Authentication File View Help Configuration SIP Options Proxies Registrations Protocol Timer Overlap sending Failover and Overflow Information SIP Options Proxies Registrations Protocol Timer Overlap sending Failover and Overflow Information SIP Options Proxies Place enter the hostname or IP address of your SIP Proxy below. Automatic failover is supported if the list contains multiple SIP Proxies. Fax Enable SIP Proxy Send OPTIONS Port Proxy Port Proxy Port T2.18.0.125 Default T2.18.0.126 Default T2.18.0.126 Default T2.18.0.126 Default T2.18.0.126 Default	✓ Information ✓ Licenses (TE-SYSTEMS GmbH - 500 Channels) ✓ CAPI 2.0 Options Image: Sign and S			tion are re r proxy as ng the def chorization d Registra P Domair ill be appo main	quired to estab well. The "coni ault.)) tion	lish a conn tact" field r	ection al nay be u SIP addr ress (i.e.	nd are used to a sed to provide a ess with a missi	uthorize the us special value f	er at the or the contac]]]]
Information SIP Options Proxies Registrations Prover law sending Failover and Overflow Information SIP Options Proxies Registrations Proxy Proxy Information SIP Options Proxies Registrations Proxy Proxy Information SIP Options Proxies Registrations Proxy Proxy If Trace SIP SIP Options Proxies Proxy Proxies If Trace SIP SIP Options Proxy Proxy Prox If Trace SIP SIP Options Proxy Prox Proxy If Trace SIP SIP Options Proxy Prot Proxy If Table SIP Frax SIP Default Default Proxy Prot If Table SIP Supplementary Services Supplementary Services Default Default Proxy Prot If Telephone-number-filter Sin Telephone-number-filter Sin Telephone-number filter Sin Telephone Sin Telephone-number filter Sin Te	-	L	ocal SIP Do	omain							
File View Help Configuration SIP Options Proxies Registrations Protocol Timer Overlap sending Failover and Overflow Information SIP Options Proxies Registrations Proxy below. Automatic failover is supported if the list contains multiple SIP Proxy Information SIP Configuration Please enter the hostname or IP address of your SIP Proxy below. Automatic failover is supported if the list contains multiple SIP Proxies. Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controller Image: Controll		Auth	entication								
 Information Capi 2.0 Options Fax Controller Controller	File View Help										
 Sectionses (TE-SYSTEMS GmbH - 500 Channels) CAPI 2.0 Options Fax Fax Controller Section Control of the address of your site Proxy below. Addothate tandover is supported in the list contains multiple SIP Proxy Controller Section Control of the address of your site Proxy below. Addothate tandover is supported in the list contains multiple SIP Proxy Fax Controller Section Control of the address of your site Proxy below. Addothate tandover is supported in the list contains multiple SIP Proxy Fax Fax	Configuration		SIP	Opt	ions Proxies	Registratio	ons Pro	tocol Timer	Overlap sendir	ng Failover	and Overflow
2 - TRY DIF IWEAKS	 ✓ Licenses (TE-SYSTEMS GmbH - 50) > ○ CAPI 2.0 Options → □ Taxe → □ Taxe → □ Taxe → □ Taxe → □ Tax → □ Tax → □ Tax → □ Tax → □ Controller → □ Tax → □ Tax → □ Tax → □ Tax → □ Controller → □ Tax → □ Tax → □ Tax → □ Tax → □ Controller → □ Tax → □ Tax → □ Controller → □ Tax → □ Tax → □ Controller → □ Tax →	i00 Chanr	nels list	Contains I Enable SI Send OP Proxy 172.18.0.12	P Proxy TIONS 14		s of your	SIP Proxy belov	v. Automatic fa	Port Def	D X t t ault ault



Exclusion of Liability

Copyright © 2018 TE-SYSTEMS GmbH

All rights reserved

This document, in part or in its entirety, may not be reproduced in any form without the prior consent of TE-SYSTEMS GmbH.

The information contained in this document was correct at the time of writing. TE-SYSTEMS GmbH reserves the right to make any alterations without prior notice.

The utmost care was applied during the compilation of texts and images, as well as during the creation of the software. Nevertheless, no responsibility can be taken for the content being accurate, up to date or complete, nor for the efficient or error-free operation of the software for a particular purpose. Therefore, TE-SYSTEMS GmbH cannot be held liable for any damages resulting directly or indirectly from the use of this document.

Trademarks

All names of products or services used are trademarks or registered trademarks (also without specified indication) of the respective private or legal persons and are therefore subject to legal regulations.

Third Party Disclaimer and Limitations

"OpenSSL", developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/), written by Eric Young (eay@cryptsoft.com) and written by Tim Hudson (tjh@cryptsoft.com).

"MD2, MD4 and MD5 Message Digest Algorithms" via source code derived from the RSA Data Security, Inc.

"RFC 4634 Secure Hash Algorithm", via source code derived from the RFC 4634.

Copyright-Notices

All files included in this sample are copyrighted by TE-SYSTEMS GmbH.

All samples and the SDK may only be used in combination with the XCAPI-product.

The SDK contains code from libtiff with the following copyright-notice:

Copyright (c) 1988-1997 Sam Leffler

Copyright (c) 1991-1997 Silicon Graphics, Inc.

Permission to use, copy, modify, distribute, and sell this software and its documentation for any purpose is hereby granted without fee, provided that (i) the above copyright notices and this permission notice appear in all copies of the software and related documentation, and (ii) the names of Sam Leffler and Silicon Graphics may not be used in any advertising or publicity relating to the software without the specific, prior written permission of Sam Leffler and Silicon Graphics.

THE SOFTWARE IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

IN NO EVENT SHALL SAM LEFFLER OR SILICON GRAPHICS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.