



CALLISTO⁺

PLATFORM

CONFIGURATION OF CISCO UCM



Table Of Contents

Configuration of Cisco UCM	3
SIP Profile configuration.....	3
SIP Trunk configuration.....	5
Configuration of route pattern	7
Configuration of Callisto services	8
Configuration of Voice Mail Pilot number.....	9
Configuration of MWI numbers	10
Add application user	11
Activating services.....	14
Activating CDRs.....	15
Configure recording.....	16
Configure External Call Control.....	20
Enable Transport Layer Security (TLS)	24
Copyright Information, Disclaimer.....	26

SIP Profile configuration

SIP is the VoIP protocol of the Callisto Platform. Via a SIP Profile, general SIP settings can be configured.

1. Add a new SIP profile or copy the Standard SIP Profile via Device > Device Settings > SIP Profile.

SIP Profile Information

Name*	Callisto SIP Profile
Description	Callisto SIP Profile
Default MTP Telephony Event Payload Type*	101
Resource Priority	< None >
Namespace List	
Early Offer for G.Clear Calls*	Disabled
SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	TIAS and AS
User-Agent and Server header information*	Send Unified CM Version Information as User-Agen
☒ Redirect by Application	
☐ Disable Early Media on 180	
☐ Outgoing T.38 INVITE include audio mline	
☐ Enable ANAT	
☐ Require SDP Inactive Exchange for Mid-Call Media Change	
☐ Use Fully Qualified Domain Name in SIP Requests	

Check Redirect by Application.

2. Add a new SIP Trunk Security Profile via System > Security > SIP Trunk Security Profile.
For non-secure communication: For encrypted communication:

SIP Trunk Security Profile Information

Name* Callisto SIP Trunk Security Profile

Description Non Secure SIP Trunk Profile authenticated by null String

Device Security Mode Non Secure

Incoming Transport Type* TCP+UDP

Outgoing Transport Type UDP

☐ 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

☐ Allow charging header

SIP V.150 Outbound SDP Offer Filtering* Use Default Filter

SIP Trunk Security Profile Information

Name* Secure Callisto SIP Profile

Description Secure SIP Trunk Profile

Device Security Mode Encrypted

Incoming Transport Type* TLS

Outgoing Transport Type TLS

☐ Enable Digest Authentication

Nonce Validity Time (mins)* 600

X.509 Subject Name callisto

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* Standardfilter verwenden

You can use the settings as seen as on the screenshot.

It is crucial to set Outgoing Transport Type to UDP.

SIP Trunk configuration

Via a Cisco Unified Communications Manager SIP Trunk, incoming calls are forwarded to Callisto, where outgoing calls will be set up.

Add a new SIP Trunk via Device > Trunk

Trunk Information	
Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

Check Transmit UTF-8 for Calling Party Name

Device Information	
Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	Callisto_SIP_Trunk
Description	Callisto_SIP_Trunk
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	< None >
Location*	Hub_None
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	

For Encrypted Communication: Check the SRTP option.

☒ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security.
Consider Traffic on This Trunk Secure* Bei Verwendung von sRTP und TLS

At Call Routing Information, check Remote-Party-ID and Asserted-Identity.

At Inbound Calls, check Redirecting Diversion Header Delivery – Inbound.

At Outbound Calls, check Redirecting Diversion Header Delivery – Outbound.

Outbound Calls

Called Party Transformation CSS < None >

☒ Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS < None >

☒ Use Device Pool Calling Party Transformation CSS

Calling Party Selection* Originator

Calling Line ID Presentation* Default

Calling Name Presentation* Default

Caller ID DN

Caller Name

☒ Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS < None >

☒ Use Device Pool Redirecting Party Transformation CSS

Via SIP Information, enter the Callisto IP address at Destination Address.

For non-secure communication, set Destination Port to 5060.

To encrypt the communication, set this port to 5061.

SIP Information

Destination

☐ Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
1* 192.168.100.90		5060	N/A	N/A	N/A

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Callisto SIP Trunk Security Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Callisto SIP Profile [View Details](#)

DTMF Signaling Method* Keine Voreinstellung

At SIP Profile, select the profile you have setup in point 1.1.

At SIP Trunk Security Profile, select the profile you have setup in point 1.2.

All Calling Search Space related settings have to be configured according the overall CUCM configuration.

Configuration of route pattern

Callisto terminated internal numbers can be defined via Route Patterns. This applies to numbers of Voice Mail, Conference and OIM applications, and others.

The screenshot shows the 'Pattern Definition' configuration form. The fields are as follows:

- Route Pattern*: 9999
- Route Partition: < None >
- Description: (empty)
- 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*: Callisto_SIP_Trunk (with an [\(Edit\)](#) link)
- Route Option:
 - ☒ Route this pattern
 - ☐ Block this pattern No Error
- Call Classification*: OffNet
- ☐ Allow Device Override ☒ Provide Outside Dial Tone ☐ Allow Overlap Sending ☐ Urgent Priority
- ☐ Require Forced Authorization Code
- Authorization Level*: 0
- ☐ Require Client Matter Code

Select Call Routing > Route > Hunt > Route Pattern and add a new route pattern

Enter the internal voice mail number in the field Route Pattern.

This number must be identical to the number entered in the Callisto system at System > System Parameter.

Select the newly configured SIP Trunk via Gateway > Route List.

Use wildcards for the route pattern number if you want to define a range of numbers.

- X: single digit (e.g., 99XX)
- !: any digit (e.g., 99!)

Configuration of Callisto services

The settings in this step activates the Callisto Phone Services at the Cisco IP phones.

1. Go to Device > Device Settings > Phone Services
2. Add a new service
3. for the service URL use: `http://<Callisto IP address>/cisco/services.asp`

Service Information	
Service Name*	Callisto
ASCII Service Name*	Callisto
Service Description	Callisto Services
Service URL*	http://192.168.100.199/Cisco/Services.asp
Secure-Service URL	
Service Category*	XML Service
Service Type*	Standard IP Phone Service
Service Vendor	
Service Version	
☒ Enable	

Subscribe this service to the phone.

You can either subscribe it directly in Device > Phones > Subscribe/Unsubscribe Services or through a profile at Device > Device Settings > Device Profile > Subscribe Services

Set the Service Provisioning to internal or both, depending on your needs. This can be done in the phone settings directly or as above in the Device Profile.

Configuration of Voice Mail Pilot number

The settings in this step define the Callisto Voice Mail number in the Cisco Unified Communications Manager. Also, the Voice Mail keys on Cisco's IP phones are configured for Callisto.

1. Open Default via Voice Mail > Voice Mail Pilot.
2. Enter the Callisto Voice Mail number.
3. Check Make this the default Voice Mail Pilot for the system

Voice Mail Pilot Information	
Voice Mail Pilot Number	9999
Calling Search Space	< None >
Description	Default
☒ Make this the default Voice Mail Pilot for the system	

This number must be identical to the Voice Mail number entered in the Callisto web menu via System > System Parameter.

Open Default via Voice Mail > Voice Mail Profile.

Select the the new configured Voice Mail Pilot at Voice Mail Pilot.

Voice Mail Profile Information	
Voice Mail Profile	Default (used by 7 devices)
Voice Mail Profile Name*	Default
Description	Default voice messaging profile
Voice Mail Pilot**	9999/< None >
Voice Mail Box Mask	
☒ Make this the default Voice Mail Profile for the System	

Configuration of MWI numbers

Add Message Waiting numbers via Voice Mail > Message Waiting. These are used by Callisto to switch the MWI lamp on and off.

Message Waiting Information	
Message Waiting Number*	9991
Partition	< None >
Description	Callisto_On
Message Waiting Indicator*	☒ On ☐ Off
Calling Search Space	< None >

1. Select Add New.
2. Enter a free internal number and set Message Waiting Indicator to On.
3. Enter another number and set Message Waiting Indicator to Off.

These two numbers must be entered in the Callisto system at System > System Parameter.

Add application user

Callisto needs an application user to access the Cisco Unified Communications Manager.

Callisto uses three main access modes.

- AXL access
- Phone Web Access
- CTI with JTAPI (COC proxy option)

Within the Callisto appliance system, there is no need to distinguish between those connection methods. Therefore, the following description is simplified by exemplifying the configuration of one application user with one user group and the corresponding roles.

This user is used in Callisto for both accessing CUCM and for phone authentication. The COC proxy user is applied automatically. Please refer to the [Callisto](#) and [COC](#) administration manuals.

Add user group

Go to User Management > User Group and add a new group.



The screenshot shows a web form titled "User Group Information". It contains a single text input field labeled "Name*" with the value "Callisto" entered.

Assign roles

The following roles can be assigned to the user group:

Role	Description
Standard AXL API Access	Grants access to the AXL database API.
Standard CCM Admin Users	Needed to get extended information from phones.
Standard EM Authentication Proxy Rights	Grant access to extension mobility logon information.
Standard RealtimeAndTraceCollection	Grants access to the phone status.
Standard CTI Enabled*	Enables CTI application control.
Standard CTI Allow Control of Phones supporting Connected Xfer and conf*	Allows control of all CTI devices that support connected transfer and conferencing.
Standard CTI Allow Call Park Monitoring*	This role is needed for the parking feature of COC. It should be added even if the parking feature is not used.

*Those roles are available if the COC Proxy option is active on Callisto.

Add application user

1. Go to User Management > Application User to add a new user.

Application User Information

User ID*

Password

Confirm Password

Digest Credentials

Confirm Digest Credentials

Presence Group*

☐ Accept Presence Subscription

☐ Accept Out-of-dialog REFER

☐ Accept Unsolicited Notification

☐ Accept Replaces Header

2. Assign all devices and profiles to this user.

Device Information

Available Devices

Controlled Devices

Available Profiles

CTI Controlled Device Profiles

To select all entries, click on the first entry and then press *shift-end* on your keyboard to extend the selection to the last entry.

3. Add the group you configured above.

Permissions Information

Groups	Callisto	Add to User Group Remove from User Group
	View	
	Details	
Roles	Standard AXL API Access Standard CCM Admin Users Standard CTI Allow Call Park Monitoring Standard CTI Allow Control of Phones supporting Conn Standard CTI Enabled	View
	Details	

The roles will be visible after adding the group.

Activating services

Change to Cisco Unified CallManager Serviceability.

1. Open Tools > Service Activation.
2. Activate both Services Cisco IP Voice Media Streaming App and Cisco AXL Web Service.

CM Services	
	Service Name
☒	Cisco CallManager
☒	Cisco Tftp
☐	Cisco Messaging Interface
☒	Cisco IP Voice Media Streaming App
☐	Cisco CTIManager

Database and Admin Services	
	Service Name
☒	Cisco AXL Web Service
☐	Cisco Bulk Provisioning Service

Activating CDRs

Stay at Cisco Unified CallManager Serviceability.

1. Go to Tools and choose CDR Management.
2. Create a new entry as following:

Billing Application Server Parameters

Host Name / IP Address*	192.168.100.90
User Name*	UcmCDR
Password*	
Protocol*	SFTP ▾
Directory Path*	CDR/
Resend on Failure	☒

The reports should be enabled and configured in Callisto before you make these settings.

3. Enter the Callisto IP address and configure the credentials, which you have already entered in Callisto Reports > Settings.
4. The protocol must be set to SFTP and Resend on Failure can be left set.

Go to Cisco Unified CM Administration.

1. In System / Service Parameters, choose your CUCM Server and select Cisco CallManager.
2. Enable the flag CDR Enabled Flag.

System	
CDR Enabled Flag *	True ▾
CDR Log Calls with Zero Duration Flag *	False ▾
Digit Analysis Complexity *	StandardAnalysis ▾
Database Debounce Timer *	0
Maximum Phone Fallback Queue Depth *	10
Maximum Number of Registered Devices *	5000
System Initialization Timer *	60
There are hidden parameters in this group. Click on Advanced button to see hidden parameters.	

Configure recording

Following steps are necessary if you want to use the Callisto Recording feature.

On Cisco Unified Communications Manager V10.x or later mobility and off-network conversations can be captured using Network-recording. Please refer to the [Cisco Recording documentation](#).

Turn on IP phone BIB to allow recording

The Built In Bridge of the agent phone must be set to On to allow its calls to be recorded.

Location	Hub_None
AAR Group	< None >
User Locale	< None >
Network Locale	< None >
Built In Bridge*	On
Privacy*	Default
Device Mobility Mode*	Default
	Device Mobility Settings
Owner User ID	< None >
Phone Personalization*	Default
Services Provisioning	Default

Alternatively, you can set the Built-in Bridge Enable service parameter to On and leave the Built In Bridge in the Phone Configuration window set to Default. Use the Device > Phone menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

Configure tones for Recording

Set the service parameters for playing a notification tone to True to allow playing it either to agent only, to customer only, or to both.

Go to System > Services (Cisco Callmanager) and set the parameters to your needs.

Clusterwide Parameters (Feature - Call Recording)		
Play Recording Notification Tone To Observed Target *	False	False
Play Recording Notification Tone To Observed Connected Parties *	True	False

Configure codec for recording

Set the service parameters for the used codecs.

Recording is only supporting the G.711 codec.

Set G.711 A-law and μ -law to Enabled for All Devices.

All other codecs must be set to Enabled for All Devices Except Recording-Enabled Dev.

Clusterwide Parameters (System - Location and Region)	
Enforce Millisecond Packet Size *	True
Locations Trace Details Enabled *	False
Preferred G.711 Millisecond Packet Size *	20
Preferred G.722 Millisecond Packet Size *	20
Preferred G.723.1 Millisecond Packet Size *	30
Preferred G.729 Millisecond Packet Size *	20
Always Use Preferred G.729 Packet Size For SIP Trunk Answers *	False
Preferred GSM EFR Bytes Packet Size *	31
G.711 A-law Codec Enabled *	Enabled for All Devices
G.711 μ-law Codec Enabled *	Enabled for All Devices
G.722 Codec Enabled *	Enabled for All Devices Except Recording-Enabled Dev
iLBC Codec Enabled *	Enabled for All Devices Except Recording-Enabled Dev
iSAC Codec Enabled *	Enabled for All Devices Except Recording-Enabled Dev

Create recording profile

1. Go to Device > Device Settings > Recording Profile menu in Cisco Unified Communications Manager Administration to conduct the necessary configuration.
2. Enter the recording profile name, recording calling search space, and recording destination address.
3. Add a [route pattern](#) to Callisto for this recording destination number.

This destination number must be configured in Callisto Recording Option. Refer to the [Callisto Administration Manual](#).

Recording Profile Configuration		Related Links:
		Back To Find/List Go
 Save  Delete  Copy  Add New		
Status		
 Status: Ready		
Recording Profile Information		
Name *	CallistoRecording	
Recording Calling Search Space	< None >	
Recording Destination Address *	9199	

Enable recording for a line appearance

To enable recording of an agent, set the Recording Option in the line appearance of the agent.

Go to Call Routing > Directory Number in Cisco Unified Communications Manager Administration to conduct the necessary configuration.

Line 1 on Device SEP00169D597D09

Display (Internal Caller ID)		displaying text such as a name instead of a directory number for i receiving a call may not see the proper identity of the caller.
ASCII Display (Internal Caller ID)		
Line Text Label		
ASCII Line Text Label		
External Phone Number Mask		
Visual Message Waiting Indicator Policy*	Use System Policy	
Audible Message Waiting Indicator Policy *	Default	
Ring Setting (Phone Idle)*	Ring	
Ring Setting (Phone Active)	Use System Default	Applies to progress.
Call Pickup Group Audio Alert Setting(Phone Idle)	Use System Default	
Call Pickup Group Audio Alert Setting(Phone Active)	Use System Default	
Recording Option *	Automatic Call Recording Enabled	
Recording Profile	CallistoRecording	
Monitoring Calling Search Space	< None >	
☒ Log Missed Calls		

To enable the automatic and manual recording during and at the end of a call, set the *Recording Option* parameter to Automatic Call Recording Enabled.

This setting can cause massive traffic to Callisto and might be very demanding on computing capacity. Also, each recording will use a line license.

To save a record during or at the end of the call, Callisto Services are used for this. Refer to the [Callisto Administration Manual](#).

Set the recording Profile to the profile you created before.

Only for Cisco Unified Communications Manager v9.x and higher

If you want to start a record manually only, set the parameter to Selective Call Recording Enabled.

With this setting, the recording is starting at the actual point of the call. This is invoked by a softkey configuration on the Cisco Unified Communications Manager as described in the next chapter.

Add the record softkey or programmable line key to the device template

This configuration is optional and only available with Cisco UCM v9.x and higher.

To allow a user to start and stop recording from a Cisco IP device, add a record softkey or programmable line key to the device template. This function can only be used if the phone line Recording Option in the chapter above is set to Selective Call Recording.

Softkey Layout Configuration

Softkey Template: Standard User 2

Select a call state to configure **Connected**

Unselected Softkeys		Selected Softkeys (ordered by position)**
HLog (HLog)		Hold (Hold)
Immediate Divert (iDivert)		End Call (EndCall)
Mobility (Mobility)		Transfer (Trnsfer)
Quality Report Tool (QRT)		Park (Park)
Record (Record)	➤	Conference (Confrn)
Toggle Do Not Disturb (DND)	➤	Conference List (ConfList)
Undefined (Undefined)		Select (Select)
		Join (Join)
		Direct Transfer (DirTrfr)
		Video Mode Command (VidMode)
		Toggle Malicious Call Trace (MCID)
		Remove Last Conference Party (RmLstC)

To add a softkey, go to Device > Device Settings > Softkey Template in Cisco Unified Communications Manager Administration to create or modify a non-standard softkey template. Configure the softkey layout for the call state connected to have the Record softkey in the selected softkeys list.

To add the Record programmable line key, go to Device > Device Settings > Phone Button Template in the Cisco Unified Communications Manager administration. Enter the button Template Name, Feature, and Label.

Configure External Call Control

To use External Call Control in Callisto, External Call Control must first be configured in CUCM.

Configure External Call Control Profile

Go to Call Routing > External Call Control Profile and add a new External Call Control Profile.

The screenshot shows the 'External Call Control Profile Configuration' page. At the top, there is a header bar with the title and a toolbar containing 'Save', 'Delete' (with a red X icon), 'Copy', and 'Add New' (with a blue plus icon). Below the header, the 'Status' section shows 'Status: Ready' with an information icon. The main section is 'External Call Control Information', which contains several fields: 'Name*' (text box with 'Callisto'), 'Primary Web Service*' (text box with 'http://callisto:80/curri/curri.asp'), 'Secondary Web Service' (empty text box), 'Enable Load Balancing' (unchecked checkbox), 'Routing Request Timer' (text box with '2000'), 'Diversion Rerouting Calling Search Space' (dropdown menu with '< None >'), and 'Call Treatment on Failures*' (dropdown menu with 'Allow Calls'). At the bottom of the form, there are buttons for 'Save', 'Delete', 'Copy', and 'Add New'. Below the buttons, there is an information icon and a note: '*- indicates required item.'

In the field Primary Web Service put the URL of the Callisto CURRI web service: `http://callisto:80/curri/curri.asp`.

Replace *callisto* with the respective IP address or domain name.

After setting up the External Call Control Profile, the trigger point needs to be set. At the trigger point, the UCM's routing logic decides which route request is chosen.

In UCM versions 8.x and 9.x, the trigger point can only be set to the *translation pattern*. In version 10.0x and higher, two new trigger points are added: *Route pattern* and *directory number*.

Translation pattern as trigger point

Go to Call Routing > Translation Pattern and add a new translation pattern or configure an existing one.

In the External Call Control Profile field set the External Call Control Profile that is configured as described above.

Translation Pattern Configuration
Related Links: Back To Find/List Go

Save

Status: Ready

Pattern Definition

Translation Pattern	5XXXX
Partition	partition4TPGlobalize
Description	
Numbering Plan	< None >
Route Filter	< None >
MLPP Precedence*	Default
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Calling Search Space	CSS4AllEP
External Call Control Profile	ECC profile to RS1 and RS2
Route Option	☒ Route this pattern ☐ Block this pattern

Route pattern as trigger point

Go to Call Routing > Route/Hunt > Route Pattern and add a new route pattern or configure an existing one.

Set External Call Control Profile to the one that you created, as described above.

Route Pattern Configuration

 Save
  Delete
  Copy
  Add New

Pattern Definition

Route Pattern*	11XXX
Route Partition	< None >
Description	
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*	Route List Test
Route Option	☒ Route this pattern ☐ Block this pattern No Error
Call Classification*	OffNet
External Call Control Profile	ECCP Test
☐ Allow Device Override ☒ Provide Outside Dial Tone ☐ Allow Overlap Sending ☐ Urgency	

Directory number as trigger point

To use a directory number as a trigger point, go to Call Routing > Directory Number and set External Call Control Profile field to the one that you created, as described above.

Directory Number Configuration

 Save
  Delete
  Reset
  Apply Config
  Add New

Status

 Status: Ready

Directory Number Information

Directory Number*	100000
Route Partition	< None >
Description	Joe's phone
Alerting Name	
ASCII Alerting Name	
External Call Control Profile	ECCP Test
☒ Allow Control of Device from CTI	

It's enough to set External Call Control Profile to the called number for External Call Control to work.

Announcement over External Call Control

To be able to play an announcement over the External Call Control, before a call gets put through, you have to modify the SIP Trunk profile from the SIP Trunk, which is connected to the PSTN.

Go to your Cisco Administration web interface, then Device > Device Settings... > SIP Profile and choose the profile which is used by the Trunk connected to the PSTN. Head down to the paragraph Trunk Specific Configuration and set the parameter SIP Rel1XX Options to Send PRACK, if 1xx contains 'SDP'.

Trunk Specific Configuration	
Reroute Incoming Request to new Trunk based on*	Nie
Resource Priority Namespace List	< None >
SIP Rel1XX Options*	PRACK senden, wenn 1xx 'SDP' enthält
Video Call Traffic Class*	Gemischt
Calling Line Identification Presentation*	Standard
Session Refresh Method*	Einladen
Early Offer support for voice and video calls*	Deaktiviert (Standardwert)

Enable Transport Layer Security (TLS)

Enable TLS between Callisto UCM and Cisco UCM to encrypt their connection and achieve a high security level.

Download certificate from Callisto

In the Callisto web interface, go to System > System Parameters > SSL Configuration (Top right corner) > Download PEM.

If there are no certificates yet, create a new self signed certificate... and download it.

Head back to System Parameters and make sure that the box under Miscellaneous > Secure SIP (TLS, SRTP) is checked.

Upload certificate to Cisco UCM

Open the Cisco UCM interface in your web browser and select Cisco Unified OS Administration in the Navigation in the top right corner.

Go to Security > Certificate Management > Upload Certificate and upload the certificate that you previously downloaded from Callisto.

Choose CallManager-trust as the certificate purpose and provide a user friendly description like Callisto.

The screenshot shows a web interface for uploading a certificate. At the top, there's a title bar 'Upload Certificate/Certificate chain' with 'Upload' and 'Close' buttons. Below this is a 'Status' section with an information icon and a warning: 'Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster'. The main section is titled 'Upload Certificate/Certificate chain' and contains three fields: 'Certificate Purpose*' with a dropdown menu showing 'CallManager-trust', 'Description(friendly name)' with a text box containing 'Callisto', and 'Upload File' with a 'Durchsuchen...' button and the filename 'Callisto.pem'. At the bottom, there are 'Upload' and 'Close' buttons. A footer note with an information icon states '*- indicates required item.'

Device security profile

Select now the Cisco Unified CM Administration in the Navigation in the top right corner and head to System > Security > SIP Trunk Security Profile and then Add New.

Fill in the profile information as following:

SIP Trunk Security Profile Information	
Name*	Secure Callisto SIP Profile
Description	Secure SIP Trunk Profile
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
☐ Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	callisto
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*	Standardfilter verwenden

(Name and description are examples)

If you are not already using secure connections it might be that the LBM Security Mode is set to insecure. To change this, head to System > Enterprise Parameters > Security Parameters > LBM Security Mode and change it to at least Mixed.

Create trunk

Create a new Trunk under Device > Trunk as described above under [SIP tunk configuration](#).

Use the previously created Device Security Profile, set the Destinationport to 5061 and use the Callisto IP as Destination Address.

Now the Trunk is ready to be used as a secure connection, to do so [define a new route pattern](#) and use the created trunk as the Gateway / Route List to route the desired calls trough this trunk.

Copyright

Copyright © 2026 CTModule AG; All Rights Reserved

This document contains proprietary information of CTModule AG. No part of the work described herein may be reproduced. Reverse engineering of the hardware or software is prohibited and is protected by patent law.

This material or any portion of it may not be copied in any form or by any means, stored in a retrieval system, adopted or transmitted in any form or by any means (electronic, mechanical, photographic, graphic, optic or otherwise), or translated to any language or computer language without the prior written permission of CTModule AG.

The information in this document is subject to change without notice. CTModule AG makes no representation or warranties with respect to the contents herein and shall not be responsible for any loss or damage caused to users either by direct or indirect use of this information. This document may contain information about third party products or processes. This third party information is out of the sphere of influence of CTModule AG. Therefore CTModule AG shall not be responsible for the correctness or legitimacy of this information.

While due care has been taken to deliver accurate documentation, CTModule AG does not warrant that this document is error-free. If you find any errors, inconsistencies, omissions or other problems related to this document, please report this in writing by email to box@ctmodule.com at CTModule AG.

CTMaker, VAS, Callisto, Callisto Express, Callisto ISDN, Callisto One, Callisto UCM, Callisto Cruise, Callisto Hospitality, Callisto X Mobile, COC Express , COC UCM and CTModule AG are trademarks and the CTModule logo is a service mark of CTModule AG.

All other products or company names mentioned herein are used for identification purposes only, and may be trademarks or registered trademarks of their respective owners.

The following description of software, hardware or process of CTModule AG or other third party provider may be included with your product and will be subject to the software, hardware or other license agreement.

Disclaimer

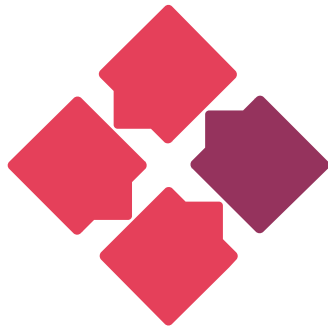
Changes are possible without notice.

The General Terms and Conditions (GTC) of CTModule AG, Switzerland apply.

All rights reserved.

For more information about CTModule AG, visit the CTModule web site at

www.ctmodule.com



CTMODULE⁺

COMMUNICATION TECHNOLOGY MODULES

CTMODULE AG

Lehnweg 1

CH-3123 Belp/Berne

Switzerland

T: +41 (0)31 531 11 11

F: +41 (0)31 531 11 12

sales@ctmodule.com

OFFICE GERMANY

Frankfurter Straße 92

D-65760 Eschborn/Frankfurt

Germany

T: +49 6196 2049173-0

F: +49 6196 2049173-9

sales-d@ctmodule.com

OFFICE SERBIA

Gospodara Vučića 145

RS-11000 Belgrade

Serbia

T: +381 18 308076

sales@ctmodule.com