CALLISTO

PLATFORM

INSTALLATION MANUAL

Table Of Contents

Requirements

Network

- Cisco Unified Communications Manager Release 3.3 and higher
- DHCPDynamic Host Configuration Protocol Server on the LANLocal Area Network
- LAN connection via RJ45 ethernet cable with 10/100 Base-T
- LAN connection between Cisco Unified Communications Manager and the Callisto Platform
- 110–220 V at 50/60 Hz (UPS and overload protection are recommended)
- Environmental conditions (light, temperature, air humidity, EMC), similar to the Cisco Unified Communications Manager environment
- 2 rack units rack space

User side

- A Internet Explorer, Firefox , Chrome, or Safari
- Free TCP Port 80 to the Callisto Platform for web access
- Phone with DTMFDual Tone Multi Frequency – supported by most regular phones capability for remote access to the VoiceMail box
- Cisco Unified Communications Manager compatible IP phones (features may vary according to the phone model)

Cisco Unified Communications Manager settings

Callisto works with Cisco Unified Communications Manager's standard settings. Only a few settings specifically related to the Callisto Platform are needed to be modified. Communication between Callisto and the Cisco Unified Communications Manager needs to be configured according to the Cisco UCM configuration manual and the appendix. If optional fax services are required, a fax dial peer needs to be configured on the appropriate PSTNPublic Switched Telephony Network gateway according to Cisco's documenation at www.cisco.com.

Quick start

Installation of a virtual appliance for VMware ESXi 4.1

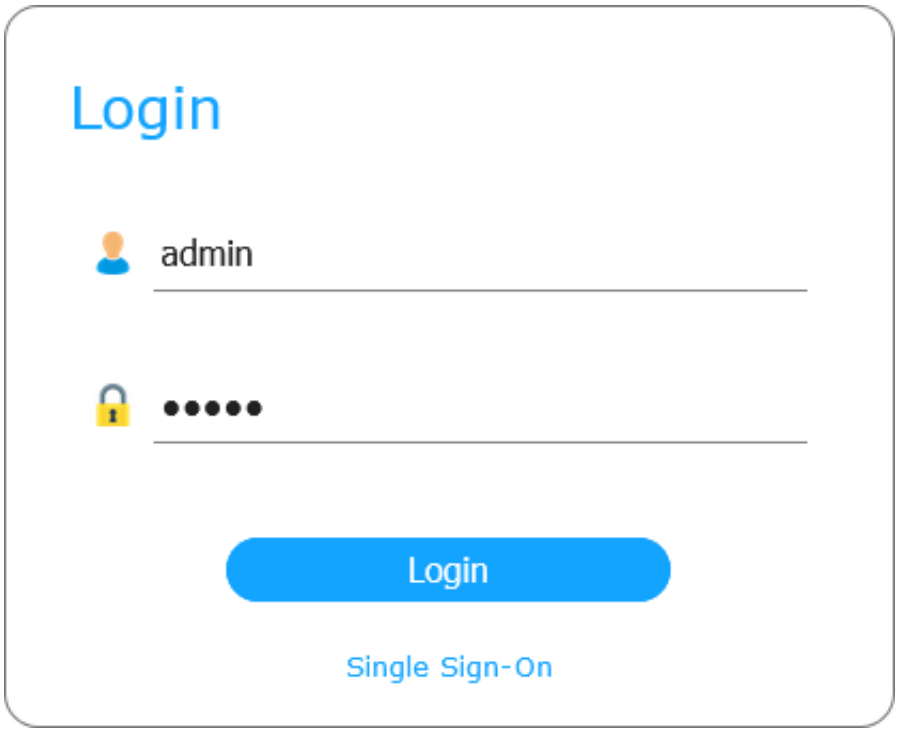
Information regarding the virtual deployment of the Callisto Platform can be found within the virtual deployment manual.

Callisto UCM web configuration

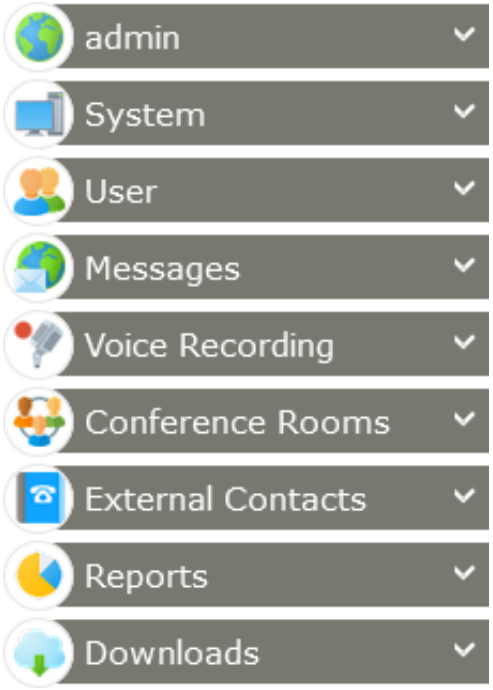
Admin account parameters

1. Type http://callisto into the address bar of a regular web browser to access Callisto from a client PC (see Requirements – User side)

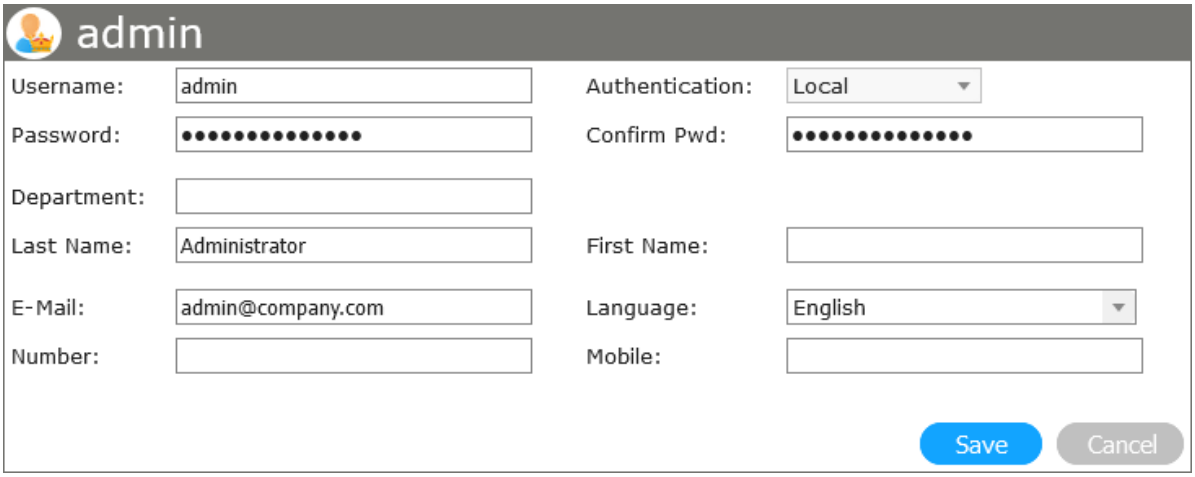
2. Type username admin and password admin for the first logon.



The following menu appears.

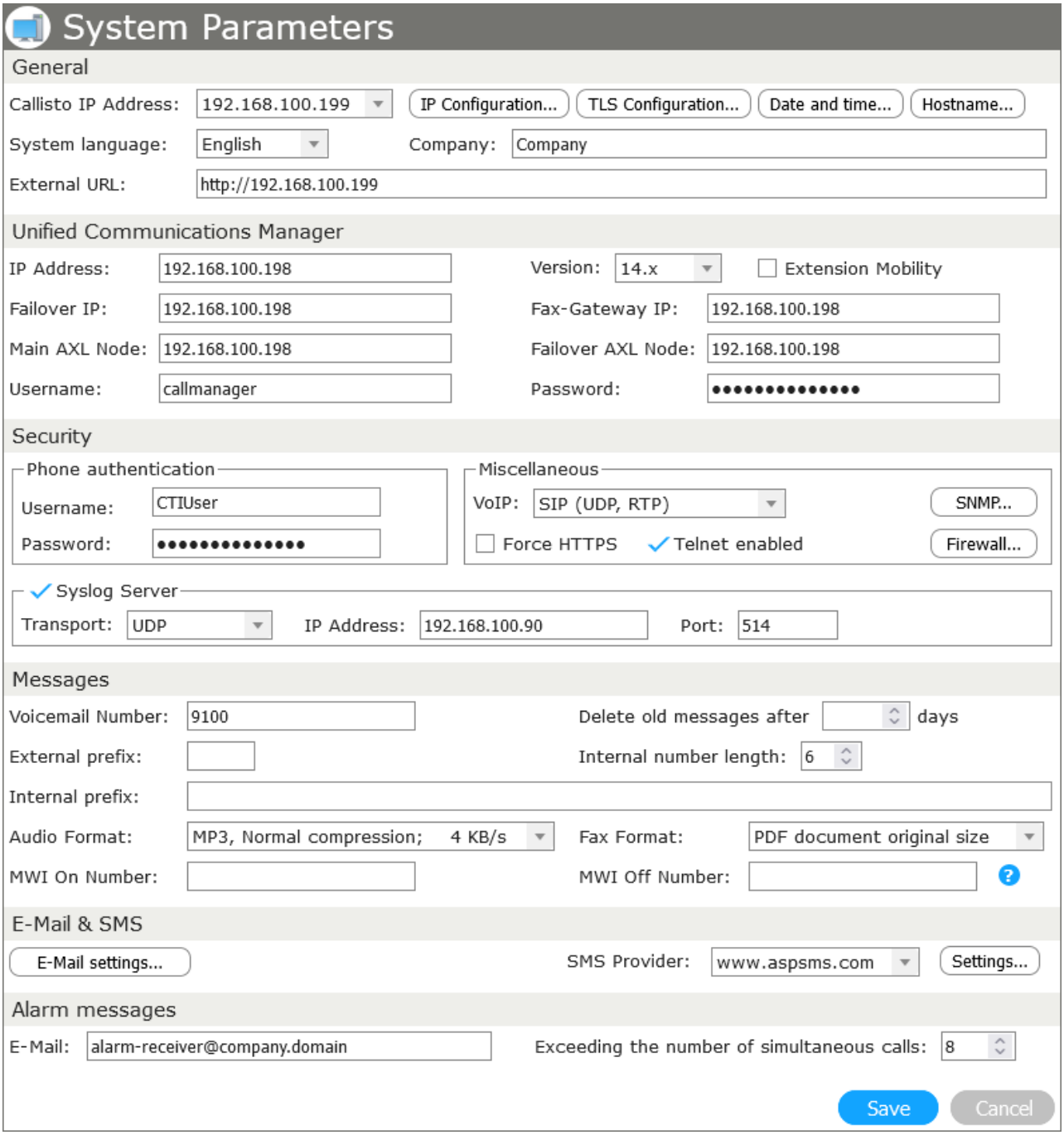


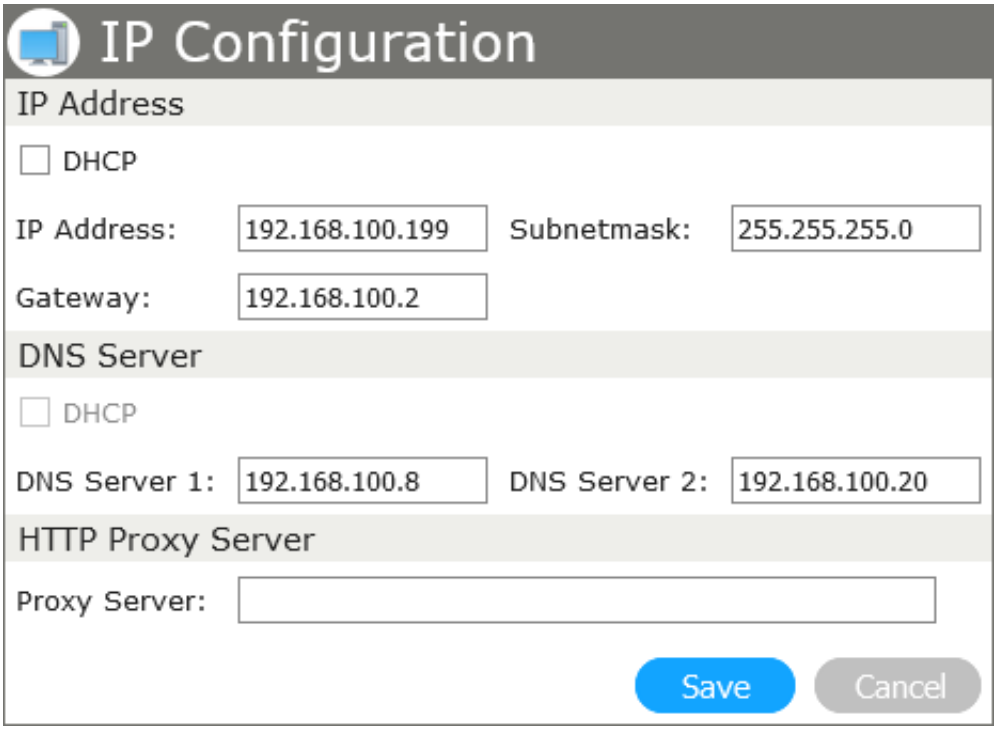
3. On the menu, choose Admin > Account to change the Username and Password. Supply the required data and select the preferred language.



Save the new settings.

System parameters


System Parameters
General
Callisto IP Address: 192.168.100.199
IP Configuration...
TLS Configuration...
Date and time...
Hostname...
System language: English
Company: Company
External URL: http://192.168.100.199
Unified Communications Manager
IP Address: 192.168.100.198
Version: 14.x
Extension Mobility
Failover IP: 192.168.100.198
Fax-Gateway IP: 192.168.100.198
Main AXL Node: 192.168.100.198
Failover AXL Node: 192.168.100.198
Username: callmanager
Password:
Security
Phone authentication
Username: CTIUser
Password:
Miscellaneous
VoIP: SIP (UDP, RTP)
SNMP...
Force HTTPS
Telnet enabled
Firewall...
Syslog Server
Transport: UDP
IP Address: 192.168.100.90
Port: 514
Messages
Voicemail Number: 9100
Delete old messages after
days
External prefix:
Internal number length: 6
Internal prefix:
Audio Format: MP3, Normal compression; 4 KB/s
Fax Format: PDF document original size
MWI On Number:
MWI Off Number:
E-Mail & SMS
E-Mail settings...
SMS Provider: www.aspsms.com
Settings...
Alarm messages
E-Mail: alarm-receiver@company.domain
Exceeding the number of simultaneous calls: 8
Save
Cancel



On the System menu, click System Parameters and enter the relevant system parameters:

For static IP address configuration parameters, click IP Configuration. After assigning a new IP address, reboot Callisto.
An IP Address for the Cisco Unified Communications Manager
A Username for the Cisco Unified Communications Manager administrator
A Password for the Cisco Unified Communications Manager administrator
The Gateway IP Address (for fax termination)
A Subnet mask
The System Language (system generic language that is used when external users call Callisto without first logging on)
A Voice Mail Number and the number of days the old messages are stored (0 = no deletion)
An External Prefix (the prefix required to be entered by users to facilitate external calls during normal operation)
The MWI On and MWI Off numbers that correspond to the MWI numbers configured on the Cisco Unified Communications Manager as described in the Cisco UCM Configuration Manual and the Appendix.

- Selection of SMS Provider:

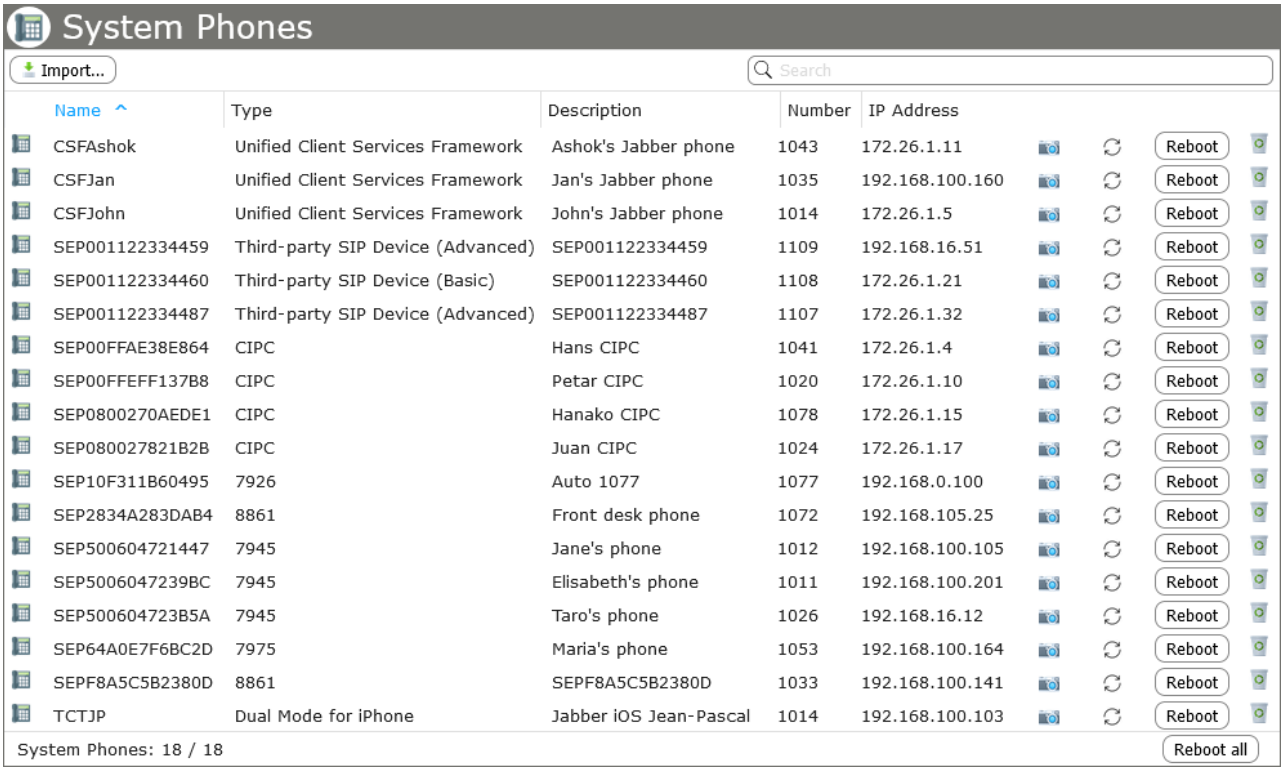
  a. *aspsms.com*: Click Settings, then type Username and Password corresponding to an active aspsms.com account.
  b. *E-Mail to SMS*: Enter a Receiver address (Please note: change expression SMSNumber to the target phone number), an Addressor address and the subject in Settings. For correct settings refer to the relevant provider. You can find a detailed description in the Administration Manual.
- SMTP-Server and Addressor. Optionally, a Username and Password can be set for SMTP Auth (RFC 2821) authentication.

Save the new settings.

To listen to voice mail by phone, users call an internal voice mail number. For external access, an external number on the public telephone network must point to the internal number.

System > Cisco phones & services

On the System menu, click System and then Cisco Phones, and all IP phones connected to the system are listed. By clicking Reboot or Reboot all, the IP phones can be rebooted individually or simultaneously.

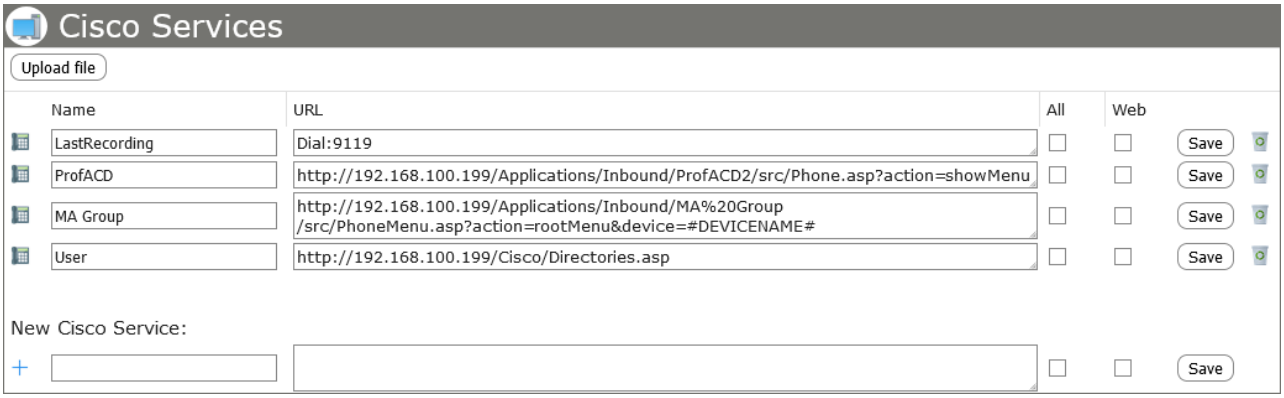


Generating a complete list of all phones can sometimes take a long time.

Cisco services

Services button

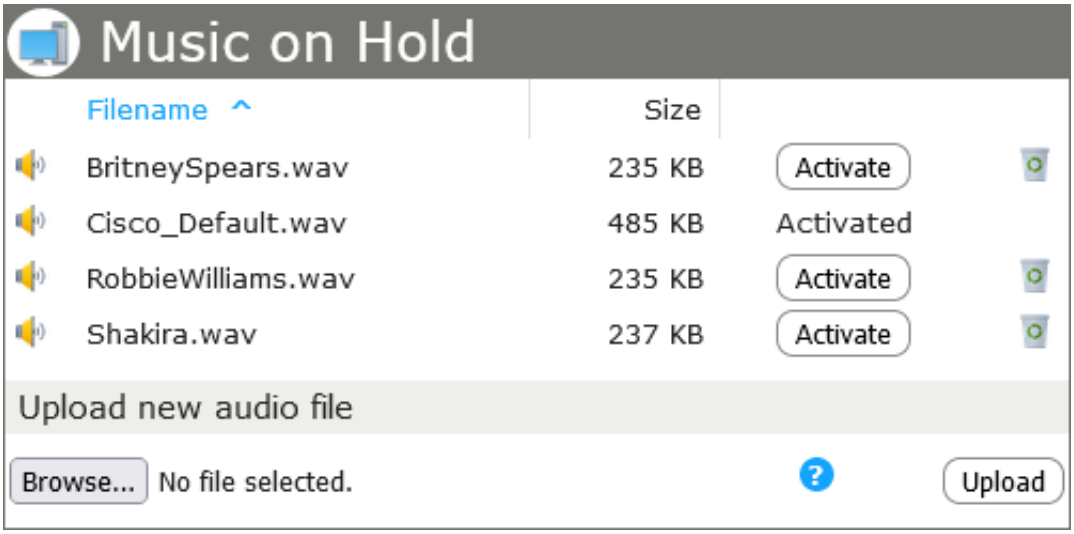
Add custom services from the System menu by clicking Cisco Services; users can select these by pressing the *Services* button on their Cisco IP phone. Administrators can add custom services or services from third parties to this menu. For further details consult the Callisto Administration Manual.



Music on hold

You can change the music that plays when a phone user is put on hold by uploading a custom *.wav* file to Callisto. To do so, navigate to Music on hold > Browse > Upload.

After uploading, select the file and click Activate.



Recycle icon

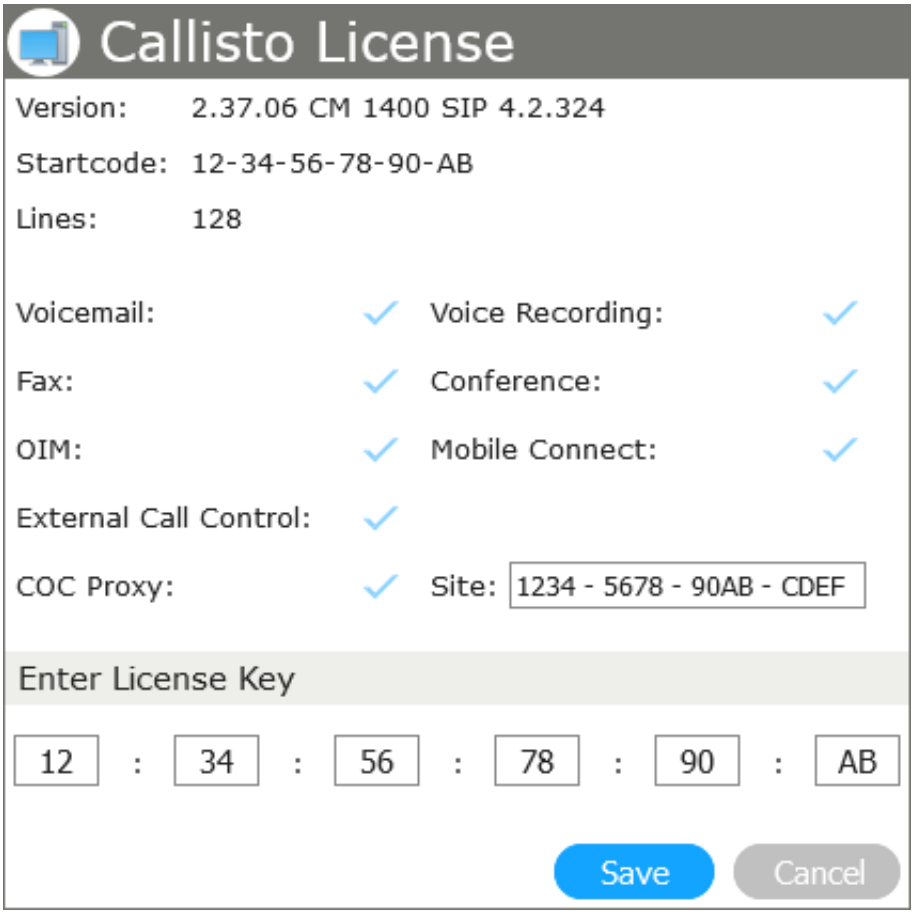
Files can be deleted by clicking the *recycle* icon.

The *.wav* files need to be of the following format: CCITT A-Law 8 kHz; 8 Bit; Mono.

Per default, a Cisco music file (*Cisco_default.wav*) is activated.

Callisto License

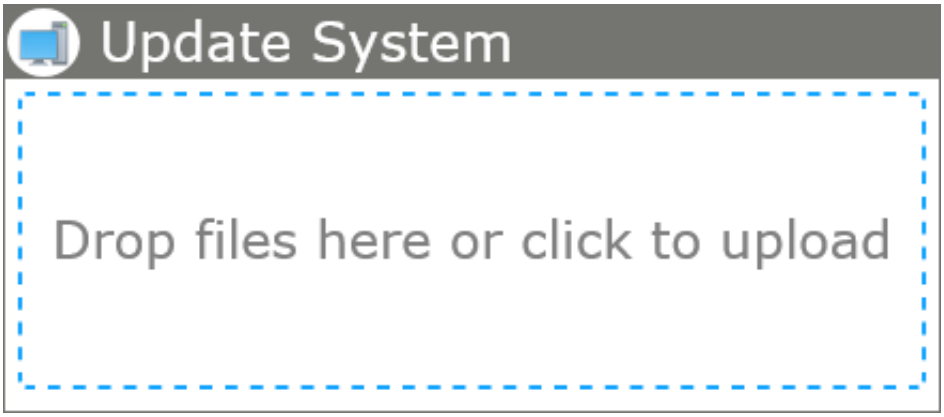
Standard Callisto appliances are normally delivered with four lines (*Callisto for UCM, HCS, Webex*) or two lines (*Callisto for UCME*) and excluding any options. To upgrade Callisto with additional features, enter a valid license key under System > Callisto License. Contact support@ctmodule.com for a new upgrade license key; the Callisto General Terms and Conditions (GTC) apply.



The optional modules *Virtual Conference Room* and *Mobile Connect* are only available with the Callisto SIP version (Callisto UCM version 1.5x or higher).

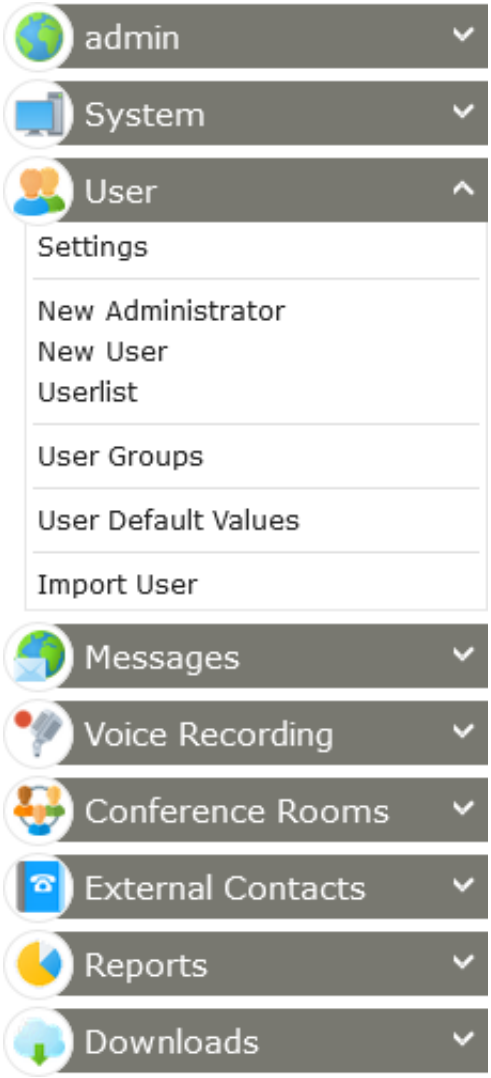
Update System

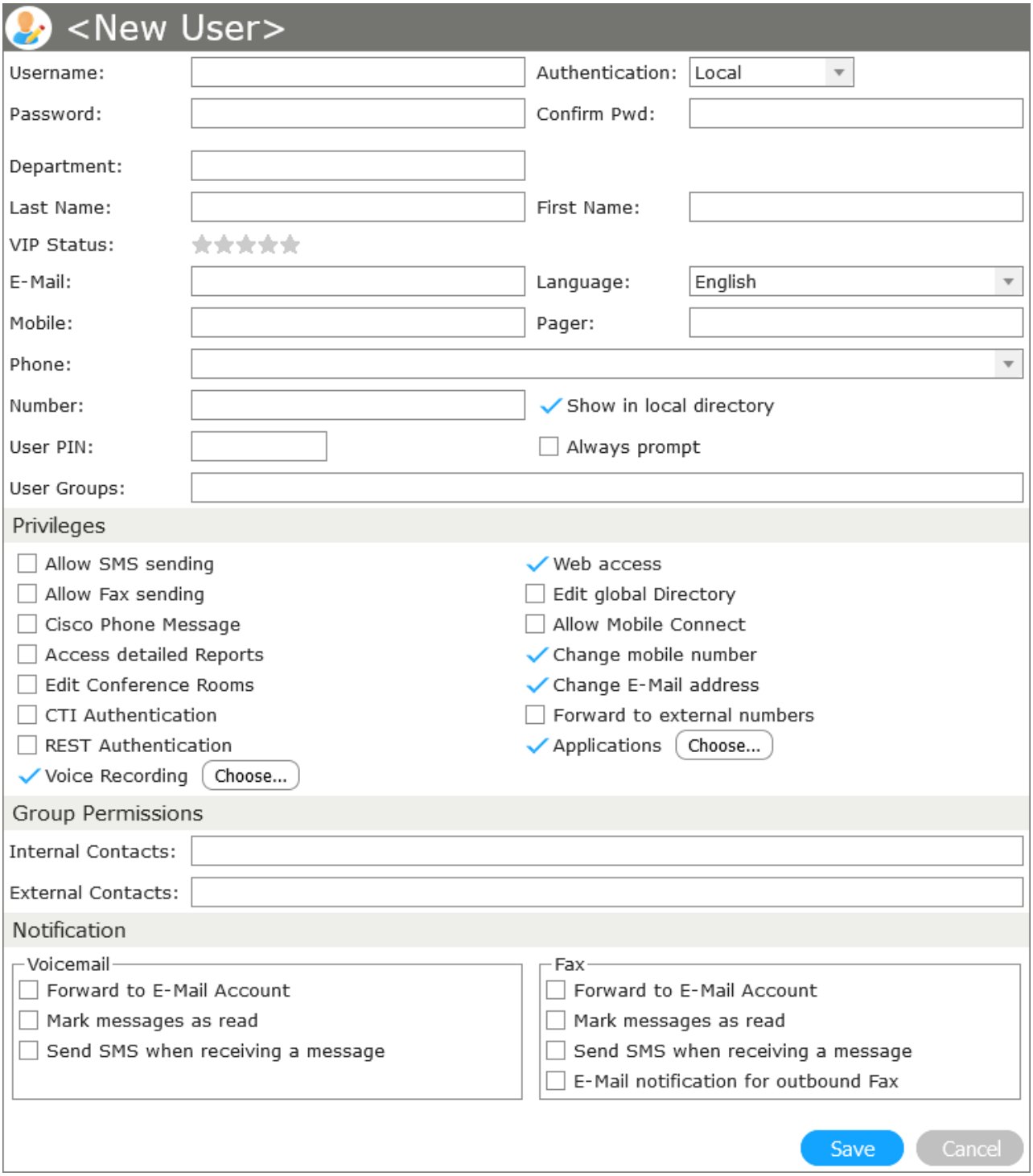
You will find the most recent updates at www.ctmodule.com. Verify under Callisto License that the latest Callisto software version is installed. Upload an update (executable file) to Callisto UCM from the System menu by clicking System Menu > Install.



User

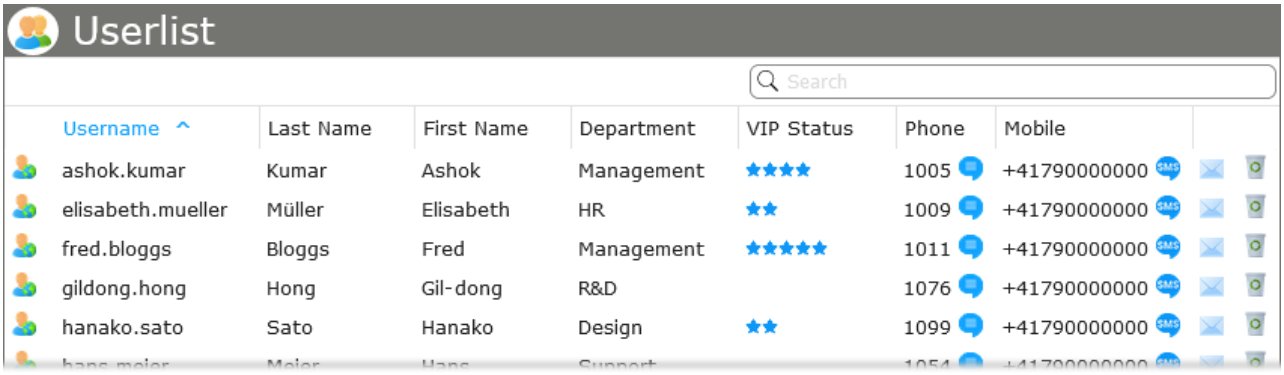
To add new users, go to User >New User, select the appropriate IP phone from the Phone list (all IP phones connected and active), enter all the other parameters and assign Privileges (for example, allow: SMS sending and notification, editing of the Global Directory, optional Fax sending, etc.)


admin
System
User
Settings
New Administrator
New User
Userlist
User Groups
User Default Values
Import User
Messages
Voice Recording
Conference Rooms
External Contacts
Reports
Downloads



Save the new settings.

Choose User > Edit User to access the user list. Here, new users can be verified, changed or deleted.



Use the Search box to find any user or selection of users. For details on available search operators, refer to the search operators quick reference.

All users from the Cisco Unified Communications Manager can be imported into Callisto UCM. Under User > User Import, verify that the system is operating correctly and then create a backup.

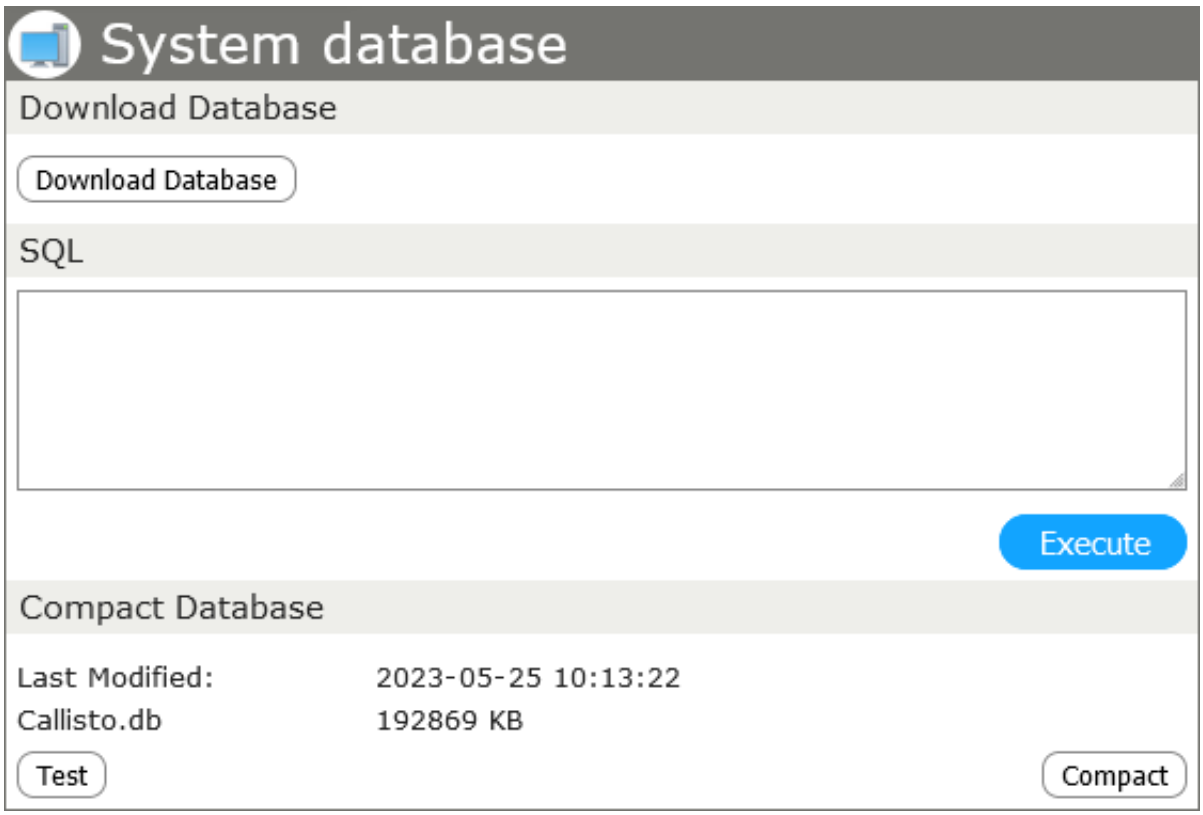
Should you encounter unexpected difficulties, check the Callisto FAQ, call your Callisto service and sales partner, or follow the instructions according to Callisto's General Terms and Conditions (GTC) and/or Service Level Agreement (SLA).

Maintenance and service

The Callisto concept ensures a maintenance free system over years. This is achieved through modern, efficient, integrated technology design.

In the unlikely event of a system failure we differentiate between services within a defined warranty period and those outside a defined warranty period.

The warranty duration is defined as per the relevant GTC document, valid at date of purchase. After warranty expiration, CTModule endeavors to facilitate replacements quickly and efficiently in order to keep down-time at a minimum.



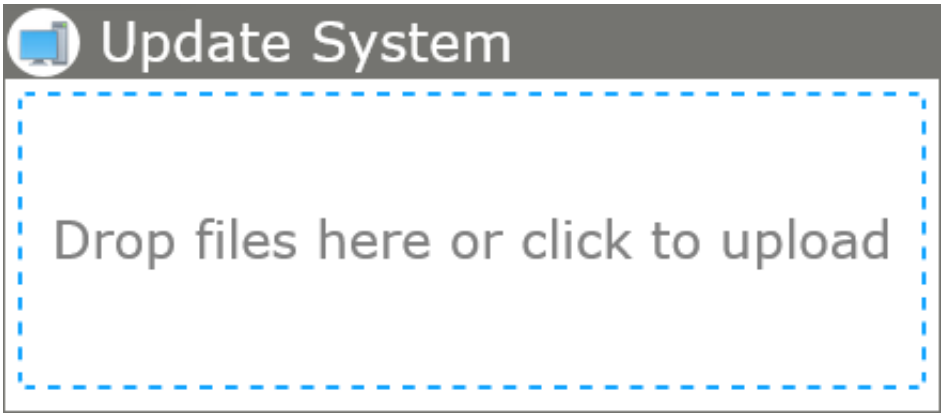
It is highly recommended to backup system parameters and user settings periodically, especially immediately before and after larger changes. Additionally, the system database should be cleaned from time to time.

To backup the database, go to the System menu, and click Backup. The downloaded and archived system database contains all Callisto Platform configurations and settings.

When restoring a database, ensure that the file name is *Callisto.mdb*.

Restoring a system database requires a backup originating from a system with an identical Callisto version.

CTModule provides occasional Callisto Platform updates and upgrades, which can be downloaded from www.ctmodule.com. They can be uploaded and installed by choosing System > Update System. A system restart may or may not be required.



After a system update, it is essential to generate a new backup. Earlier backups may possibly not be compatible any longer.

Before reporting an error, check the following:

- Are the LEDs at the front of the Callisto appliance on? Or, do they flash from time to time?
- Is the power cable plugged in firmly and properly?
- Is the correct power supply in use?
- Can the fan and/or the hard disk be heard in the Callisto appliance?
- Do the LEDs flash on the RJ45 LAN plug socket at the back of the Callisto appliance?
- Does DHCPDynamic Host Configuration Protocol function correctly in the LAN?
- Do you get the login screen on a Client PC's browser if you type http://callisto/ into the browser's address bar?
- Is the Cisco Unified Communications Manager configured correctly according the Cisco UCM Configuration Guide and the Appendix? Is the communication link between the Cisco Unified Communications Manager and Callisto working?

Should there be any unexpected malfunctions, please consult the Callisto FAQ list, call your Callisto dealer or follow the instructions according to the Callisto GTC and/or SLA.

In case of software or configuration problems, our technicians might need to activate trace logging on your Callisto Platform. Further information about this can be found on the page Telnet access of the Administration Guide (see also Additional administration).

Additional administration

Additional system administration tasks are described in the Callisto platform administration manual. An administrator defines a range of parameters, with validity for either single users or for all users; for security reasons, only an administrator may edit these values. To take full advantage of both systems, Cisco Unified Communications Manager and Callisto, your customers might consider reading the Administration Guide.

Appendix

Configuration of Cisco Unified Communications Manager 5.x to 12.x

The dedicated guide for establishing the communication link between Callisto UCM and versions 5.x to 12.x of the Cisco Unified Communications Manager can be found here.

Example dial-peer for T.38 fax on a Cisco gateway

Because the Cisco Unified Communications Manager older than version 5.x does not support SIP/T.38 reliable, Callisto uses SIP/T.38 on the PSTN gateway directly.

Example of a VoIP Callisto dial-peer:

```
voice class uri Callisto sip
 host CALLISTO

dial-peer voice 100 voip
description CALLISTO_FAX
destination-pattern <Internal Callisto fax number>;
session target ipv4:<Callisto IP address>;
fax protocol t38 ls-redundancy 0 hs-redundancy 0
ip qos dscp cs5 media
no vad
codec g711alaw
session protocol sipv2
incoming uri from Callisto
dtmf-relay sip-notify
```

The settings t38 (support of real time Fax over IP) and no vad (disable “Voice Activity Detection”) are crucial.

In case of problems like incompletely transmitted documents, refer to chapter Network Clock Timing in the Cisco High Density Voice/Fax Network Modules documentation.

Activating T.38 and pass-through on a Cisco gateway

To transport T.38 and still able to use analog pass-through devices use the following settings on the gateway:

```
voice service voip
  fax protocol t38 fallback pass-through g711alaw
```

Used TCP/UDP Ports

Source	Destination	Protocol	Port	Description
Client	CALLISTO	http/https	TCP/80, TCP/8080,	Web Frontend, Fax

Source	Destination	Protocol	Port	Description
			TCP/443	Service
Client (admin)	CALLISTO	telnet	TCP/23	CLI
Client (COC)	CALLISTO	TCP	TCP/27864	COC encrypted
Client (COC)	CALLISTO	TCP	TCP/27866	COC unencrypted
Phone	CALLISTO	http/https	TCP/80, TCP/16002, TCP/443	Phone Services
CALLISTO	CUCM	https	TCP/443	AXL
CALLISTO	CUCM	SIP/SIPS	TCP&UDP/5060, TCP/5061	SIP Trunk
CALLISTO	CUCM	RTP/SRTP	UDP 49152-65535	SIP Trunk
CALLISTO	CUCM	CTI/QBE	TCP/2748	JTAPI
CALLISTO	CUPS	REST	TCP/8082, TCP/8083	Presence Server
CALLISTO	Phone	http/https	TCP/80, TCP/443	XML Message
CALLISTO	Phone	RTP/SRTP	UDP 49152-65535	SIP RTP
CALLISTO	Mail Server	SMTP	TCP/25	E-Mail delivery
CALLISTO	Time Server	NTP	UDP/123	TimeSync
CALLISTO	Backup Server	FTP	TCP/21	FTP Backup
CALLISTO	Backup Server	FTP	TCP/(depends on server)	FTP Backup passive range
CALLISTO	Syslog Server	Syslog	UDP/514, TCP/6514	Syslog
CUCM	CALLISTO	SIP/SIPS	TCP&UDP/5060, TCP/5061	SIP Trunk
CUCM	CALLISTO	RTP/SRTP	UDP 49152-65535	SIP Trunk
CUCM	CALLISTO	CTI/QBE	TCP/2789	JTAPI
CUCM	CALLISTO	SFTP	TCP/22	SFTP CDRs
CUPS	CALLISTO	REST	TCP/8843	Presence Server
CUPS	CALLISTO	SIP	TCP/27865	SIP SIMPLE Presence Server
SNMP Client	CALLISTO	SNMP	UDP/161, UDP/162	SNMP

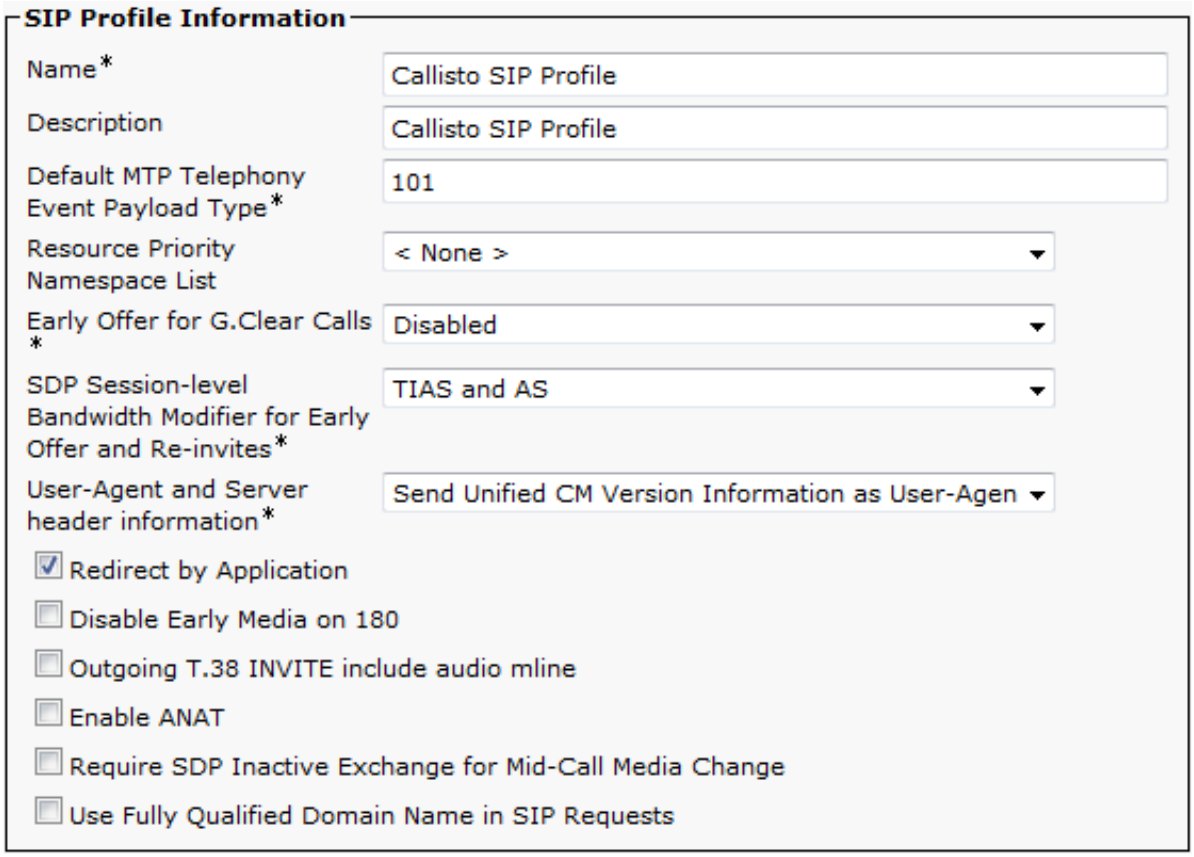
PLATFORM

CONFIGURATION OF CISCO UCM

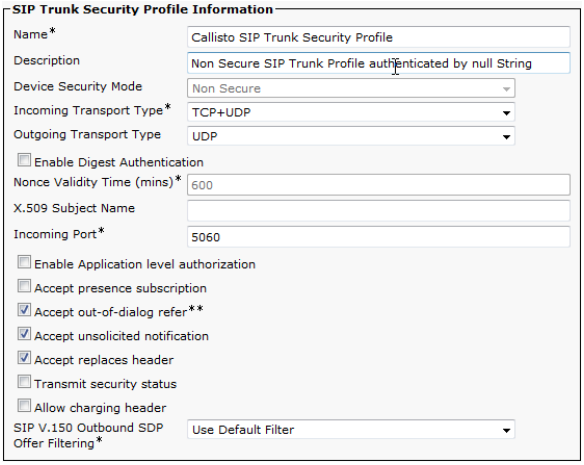
SIP Profile configuration

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

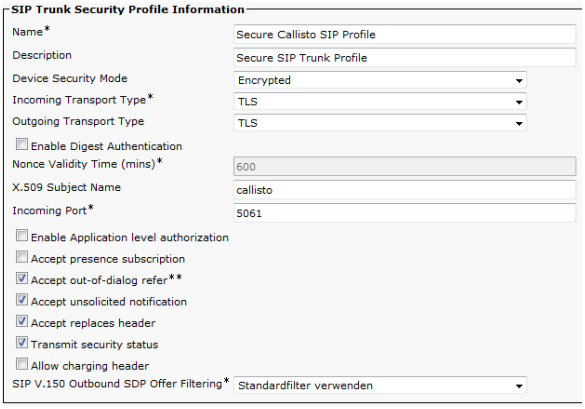
1. Add a new SIP profile or copy the Standard SIP Profile via Device > Device Settings > SIP Profile.



   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:



It is crucial to set Outgoing Transport Type to UDP.

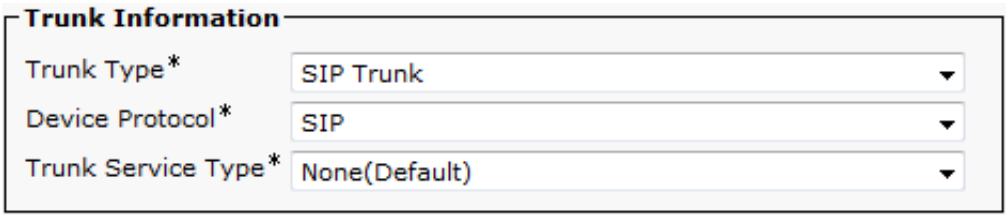


You can use the settings as seen as on the screenshot.

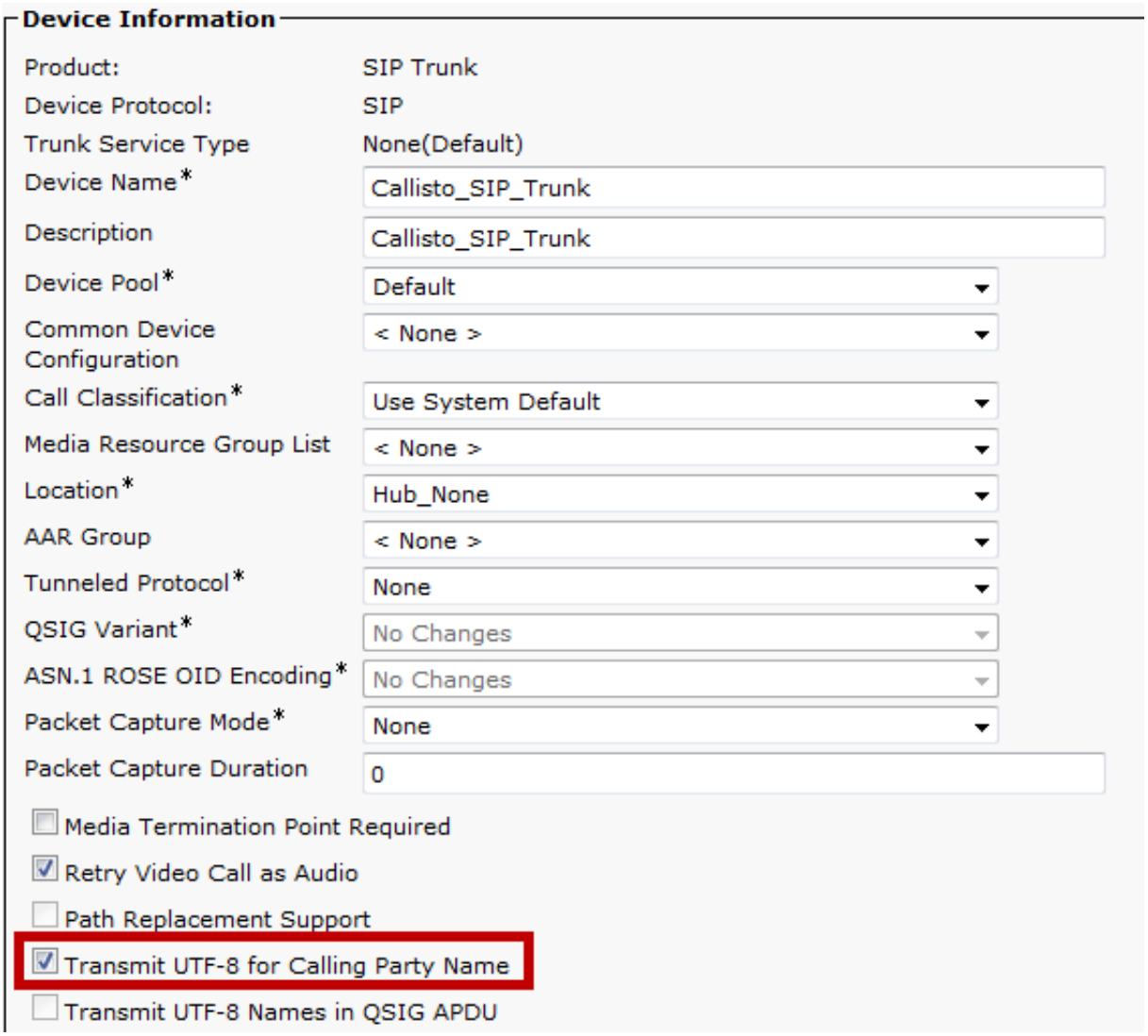
SIP Trunk configuration

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

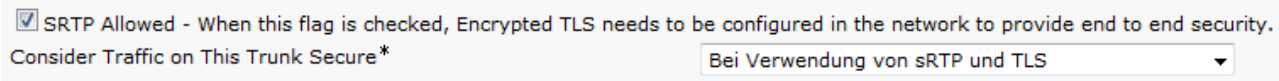
Add a new SIP Trunk via Device > Trunk



Check Transmit UTF-8 for Calling Party Name



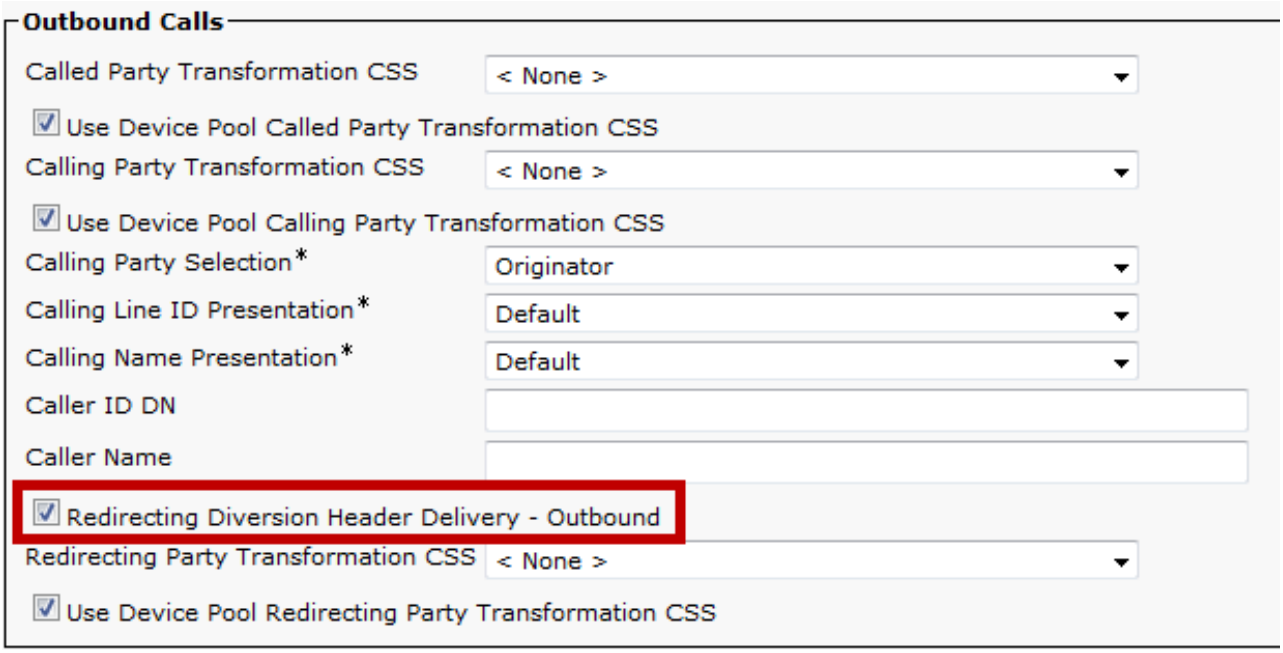
For Encrypted Communication: Check the SRTP option.



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.



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.

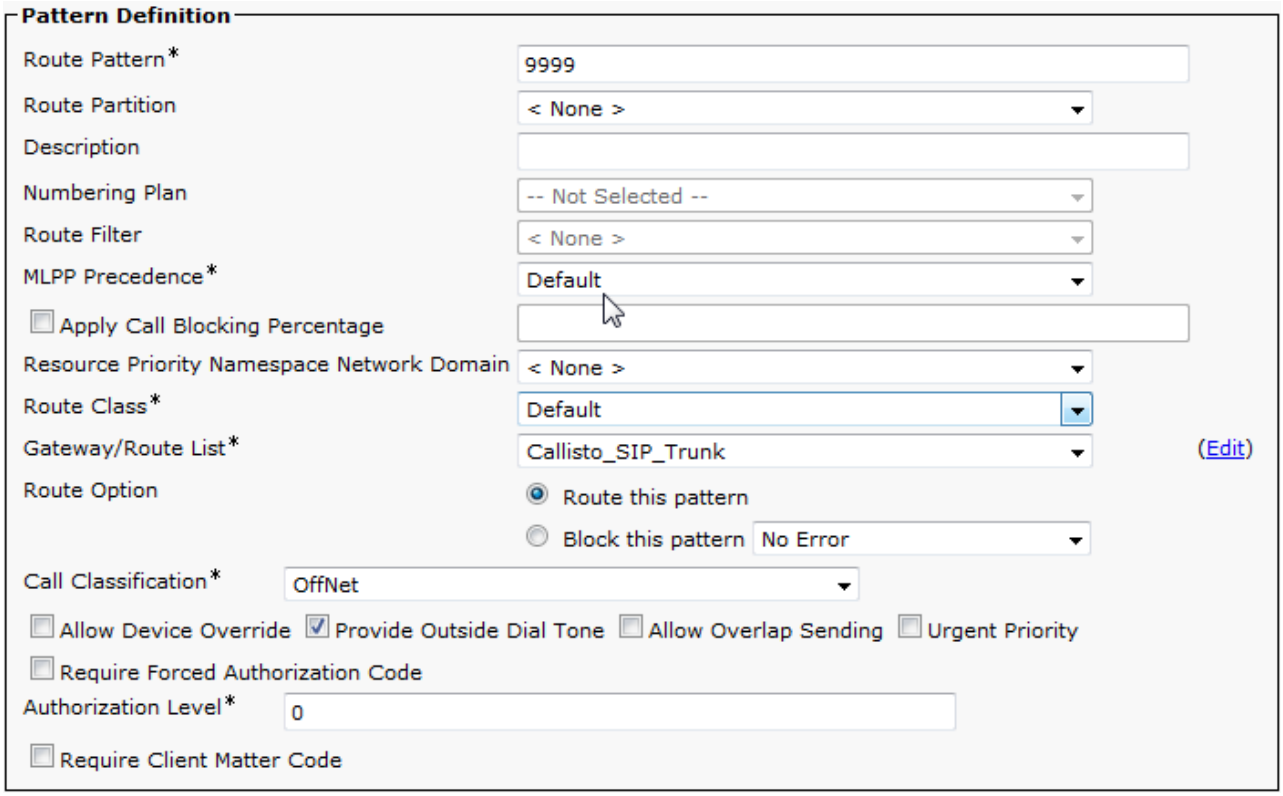
At SIP Profile, select the profile you have setup in point 1.1.

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.



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.

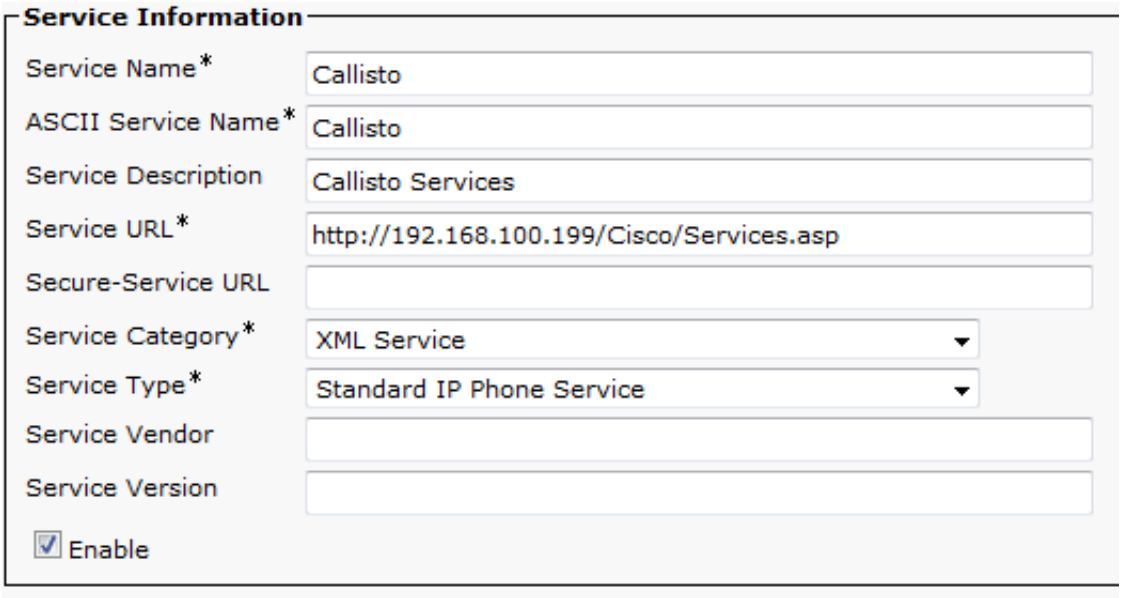
Use wildcards for the route pattern number if you want to define a range of numbers.

- 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



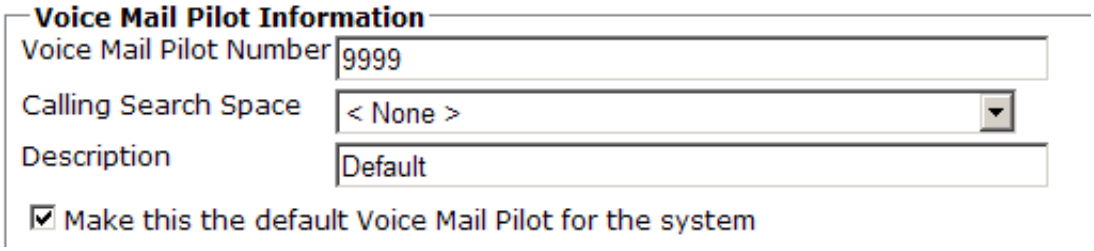
Subscribe this service to the phone.
You can either subscribe it directly in Device > Phones > Subscribe/Unsubscribe Services or trough a profile at Device > Device Settings > Device Profile > Subscribe Services

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.

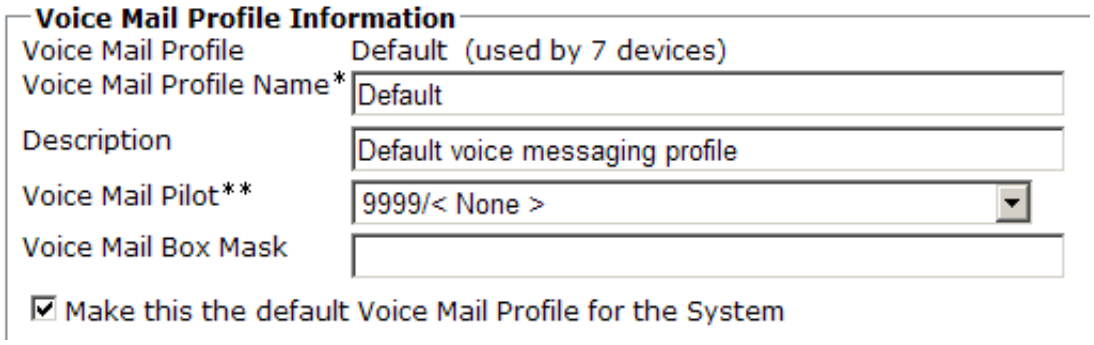
1. Open Default via Voice Mail > Voice Mail Pilot.
2. Enter the Callisto Voice Mail number.
3. Check Make this the default Voice Mail Pilot for the system



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

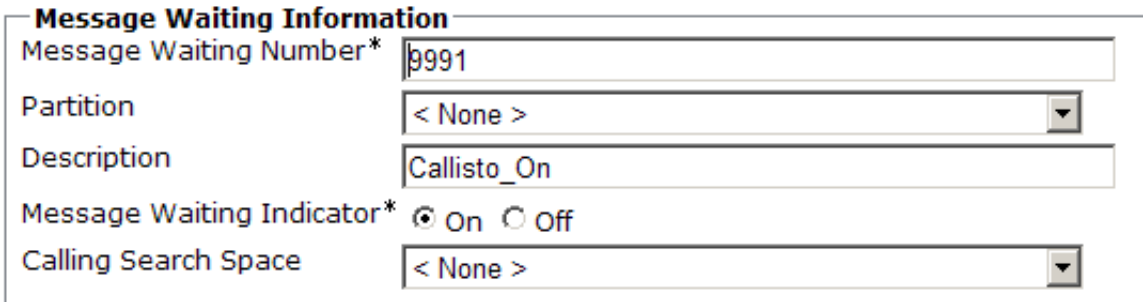
Open Default via Voice Mail > Voice Mail Profile.

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



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.



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.

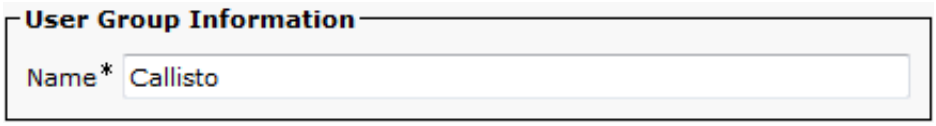
- AXL access
- Phone Web Access
- CTI with JTAPI (COC proxy option)

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.



Assign roles

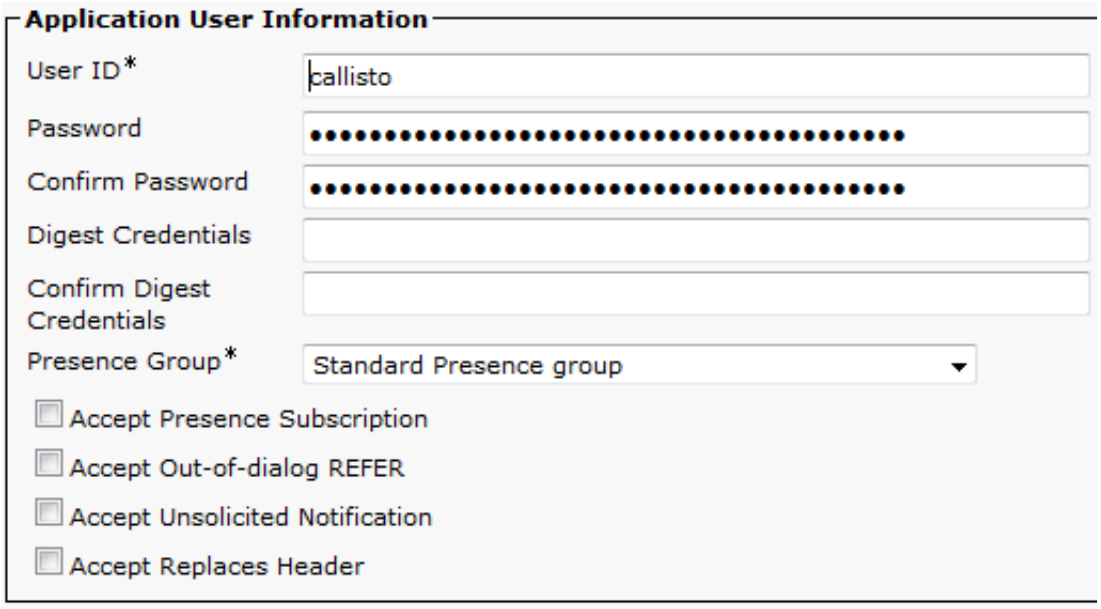
The following roles can be assigned to the user group:

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.

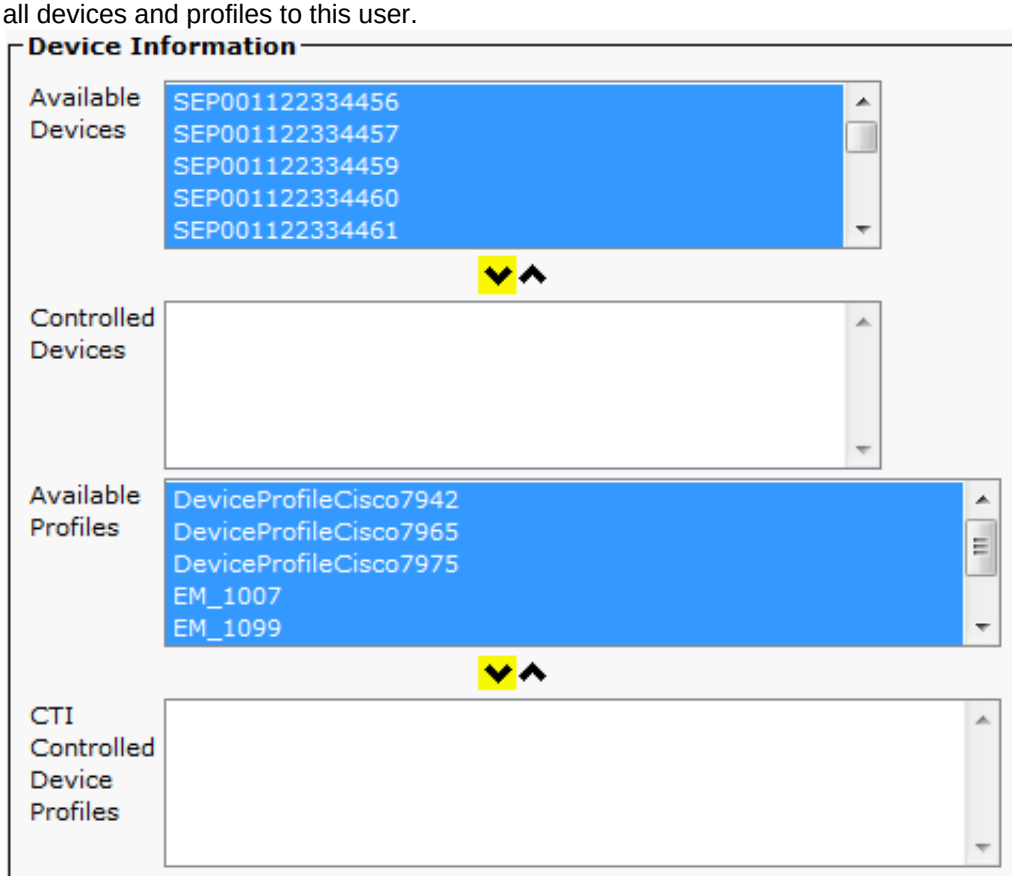
*Those roles are available if the COC Proxy option is active on Callisto.

Add application user

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

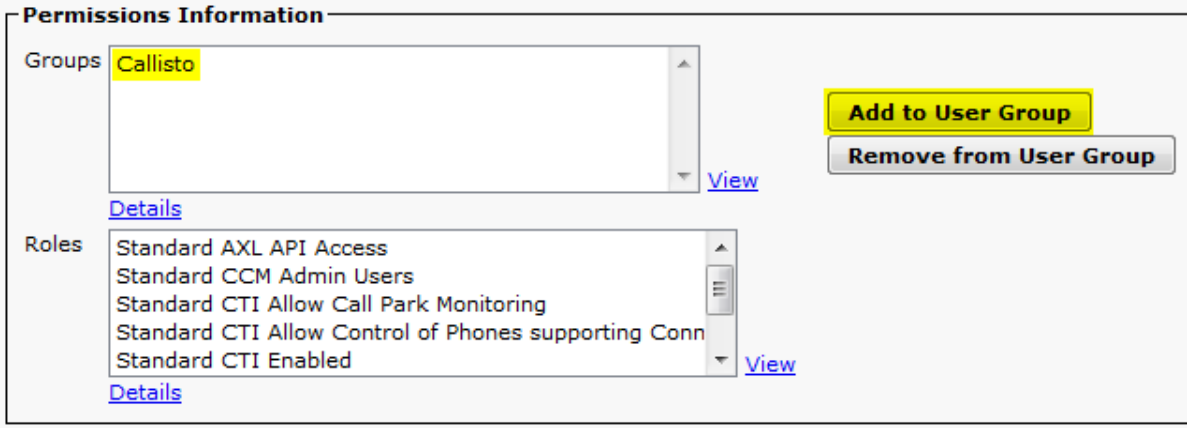


2. Assign all devices and profiles to this user.



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.

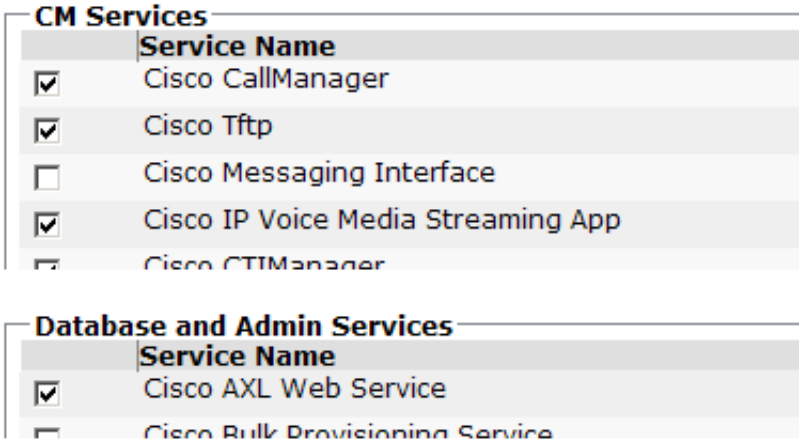


The roles will be visible after adding the group.

Activating services

Change to Cisco Unified CallManager Serviceability.

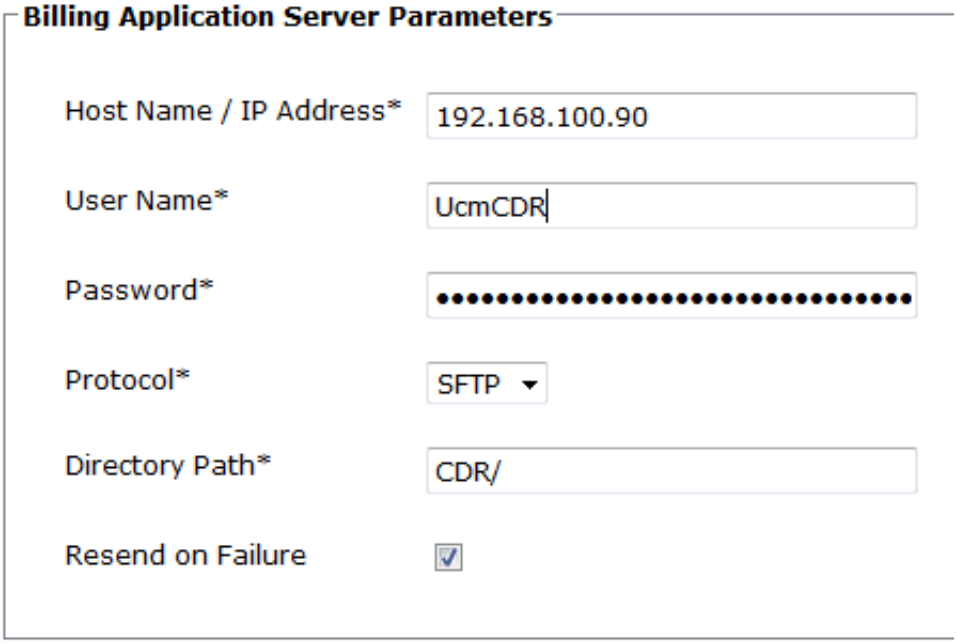
1. Open Tools > Service Activation.
2. Activate both Services Cisco IP Voice Media Streaming App and Cisco AXL Web Service.



Activating CDRs

Stay at Cisco Unified CallManager Serviceability.

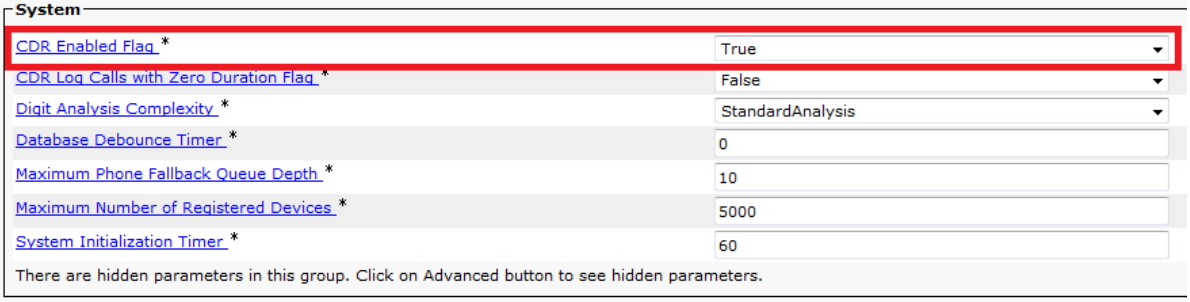
1. Go to Tools and choose CDR Management.
2. Create a new entry as following:



   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.



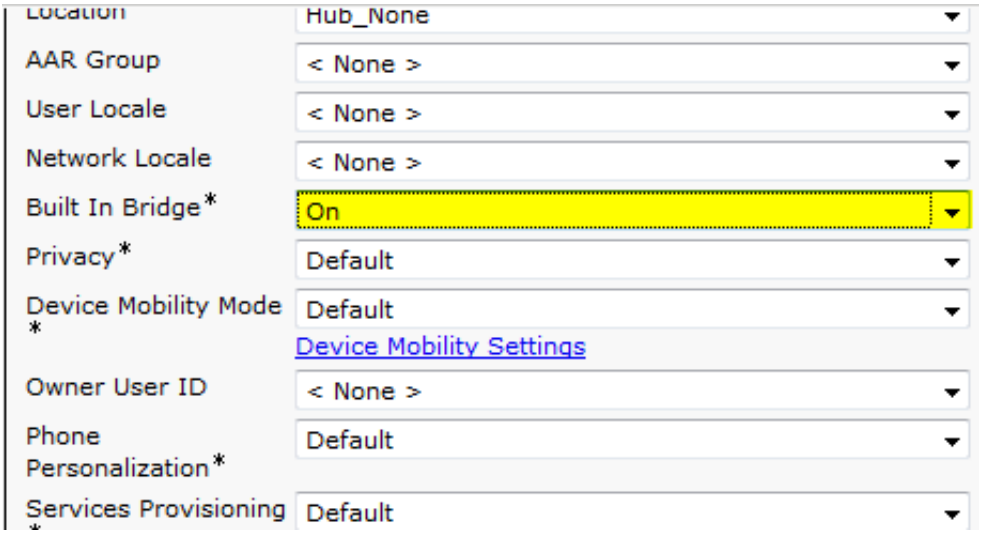
Configure recording

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

On Cisco Unified Communictions 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.

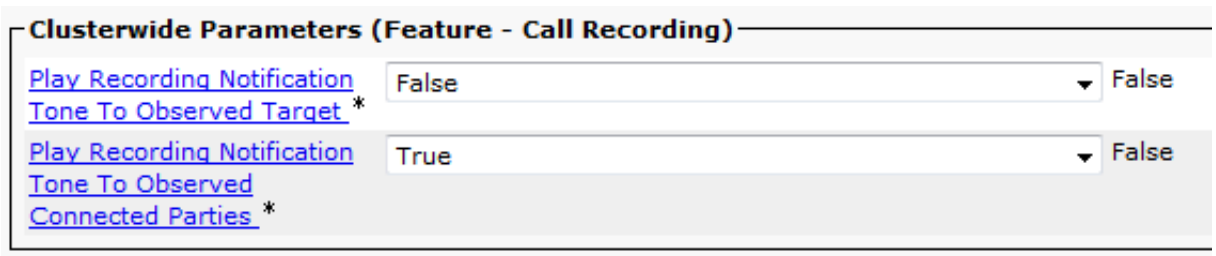


Alternatively, you can set the Built-in Bridge Enable service parameter to On and leave the Built In Bridge in the Phone Configuration window set to Default. Use the Device > Phone menu option in Cisco Unified Communications Manager Administration to perform the necessary configuration.

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.



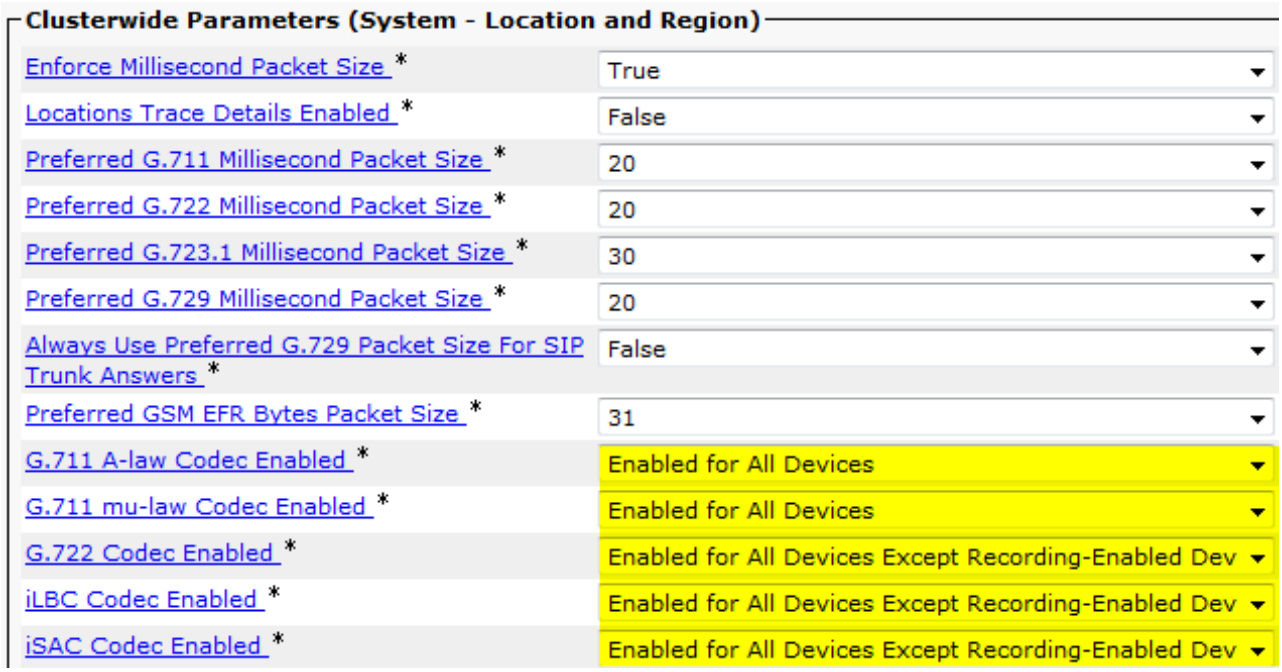
Configure codec for recording

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.

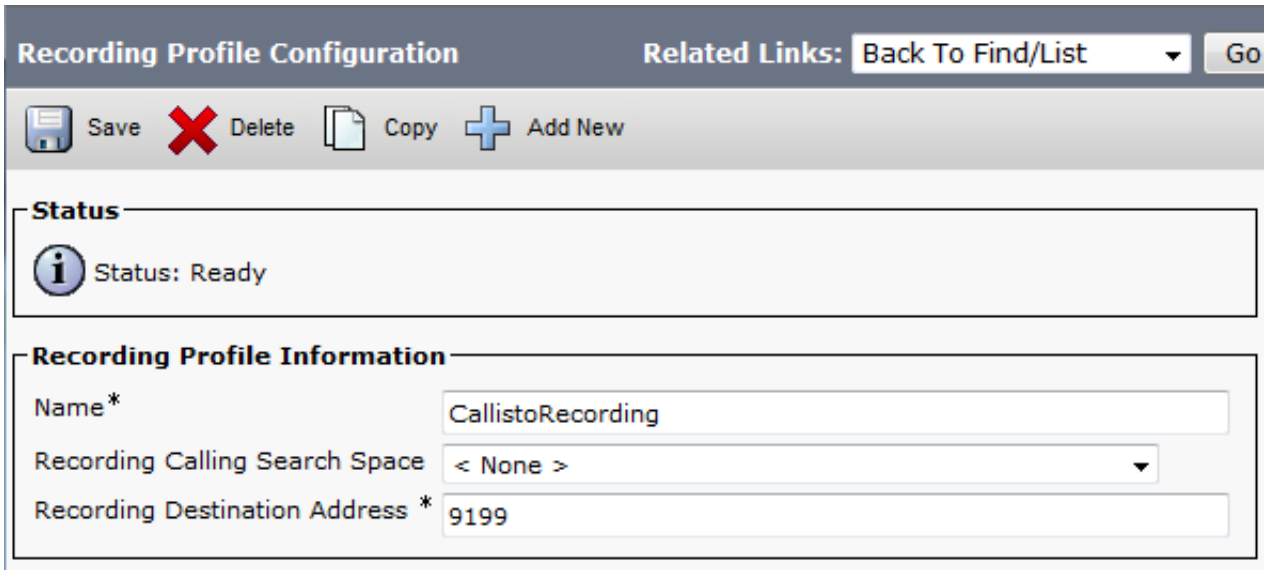
All other codecs must be set to Enabled for All Devices Except Recording-Enabled Dev.



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.

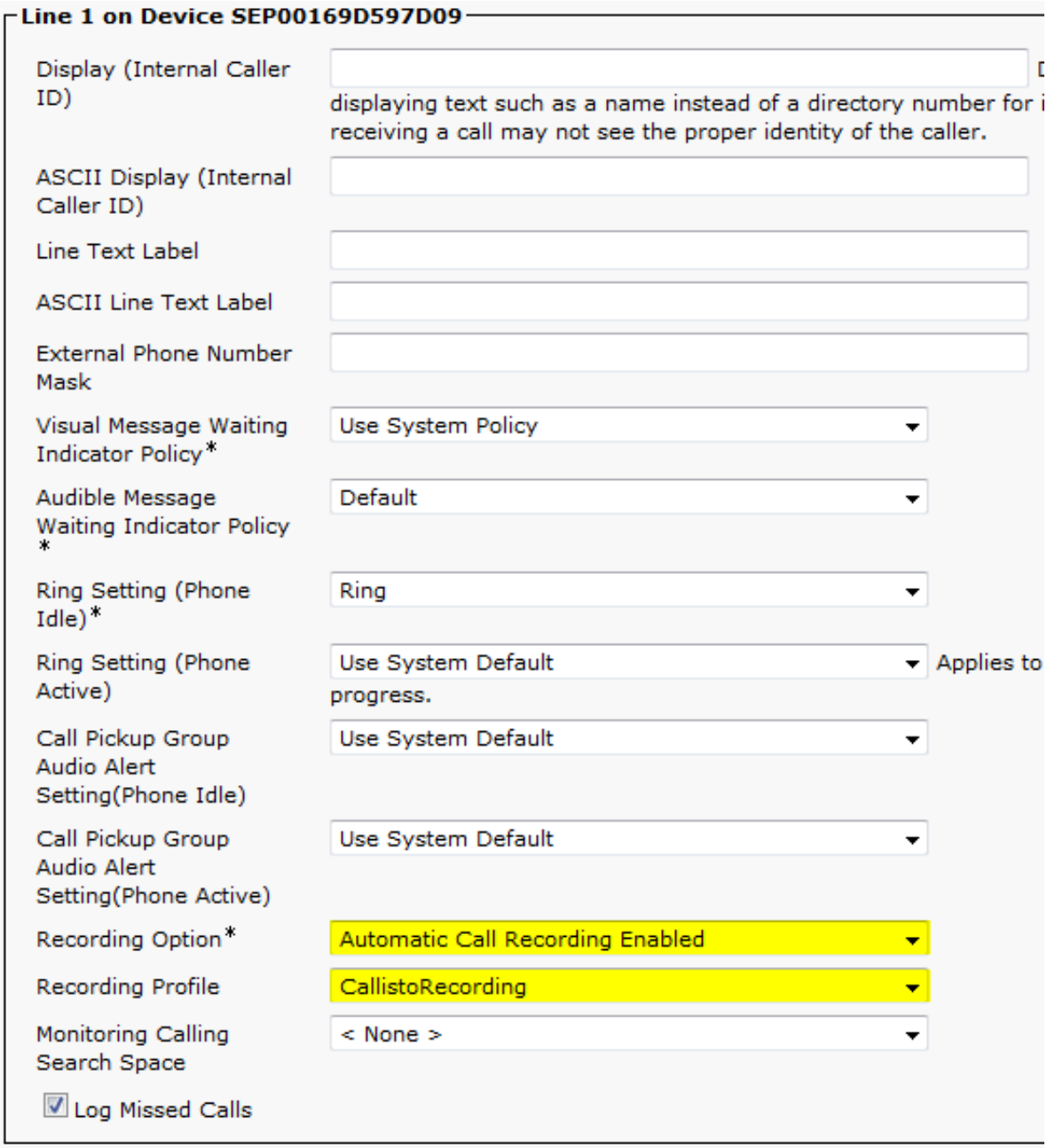
This destination number must be configured in Callisto Recording Option. Refer to the Callisto Administration Manual.



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.



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

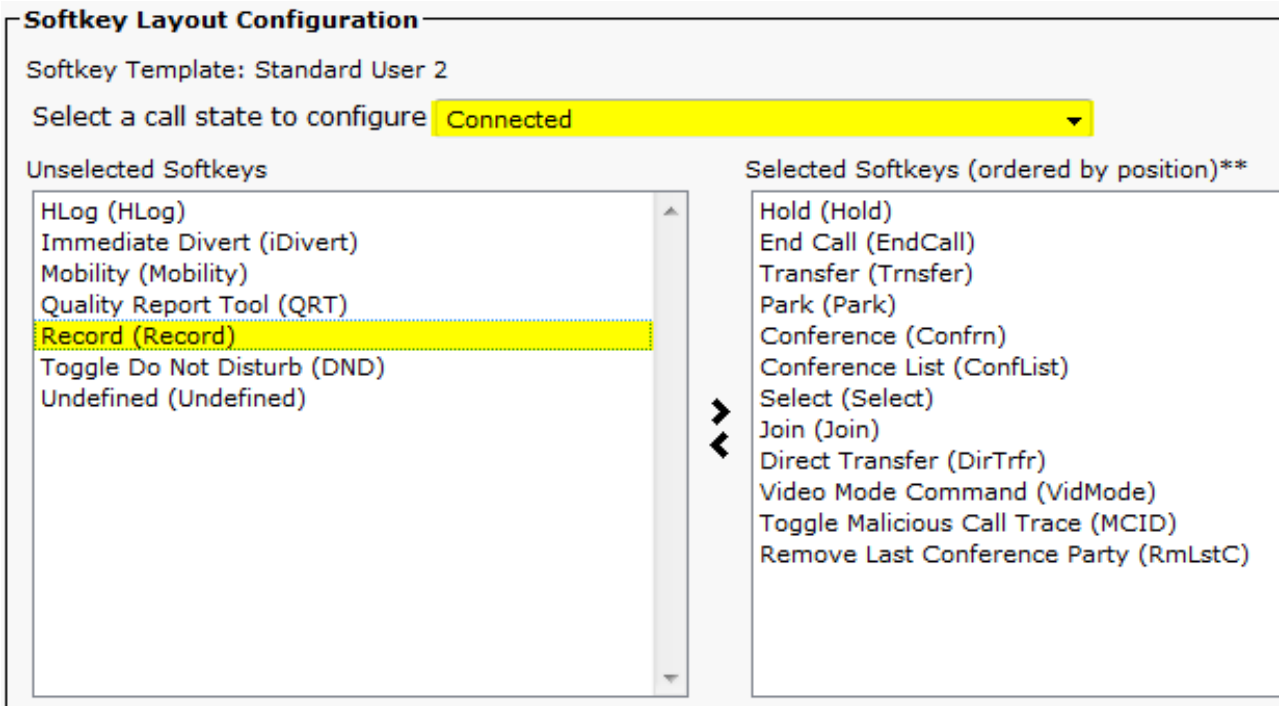
If you want to start a record manually only, set the parameter to Selective Call Recording Enabled.

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.



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.

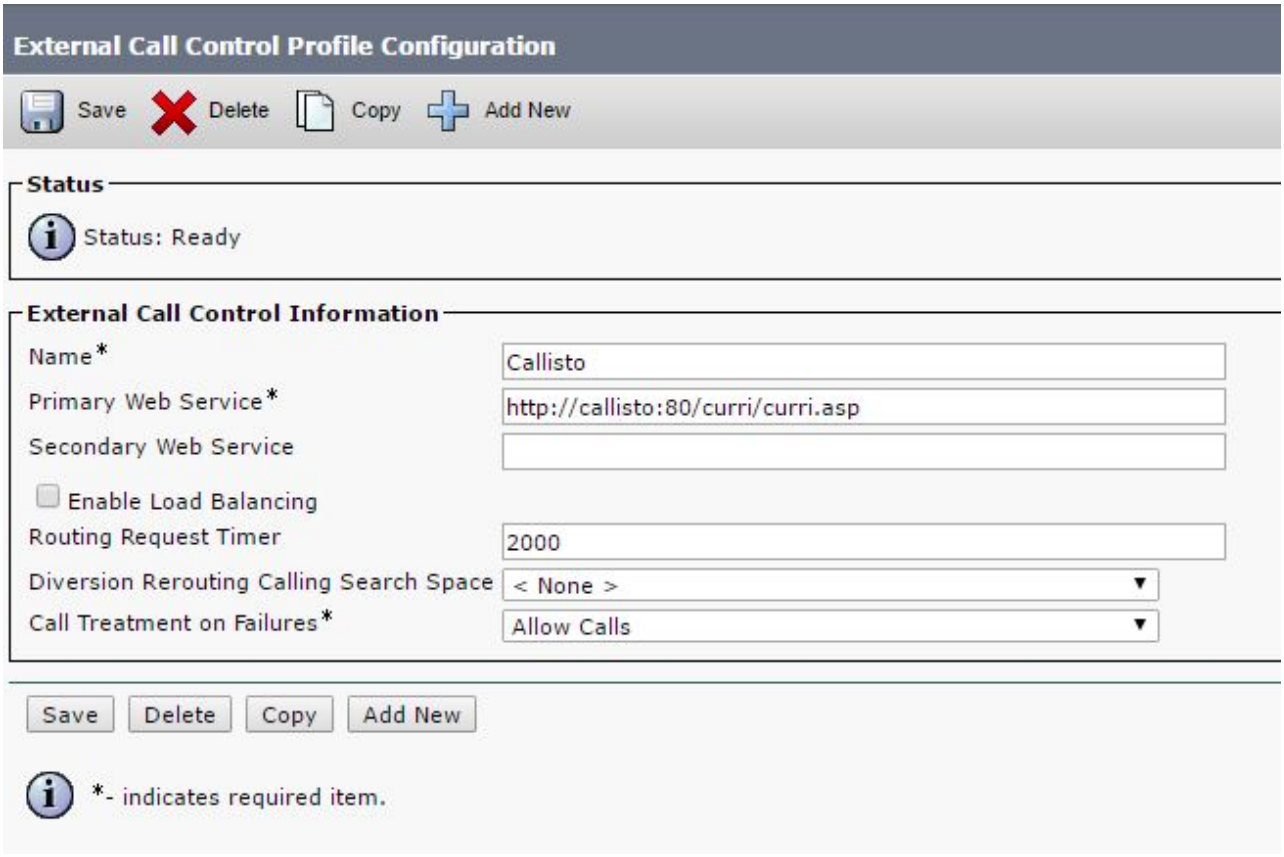
To add the Record programmable line key, go to Device > Device Settings > Phone Button Template in the Cisco Unified Communications Manager administration. Enter the button Template Name, Feature, and Label.

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.



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.

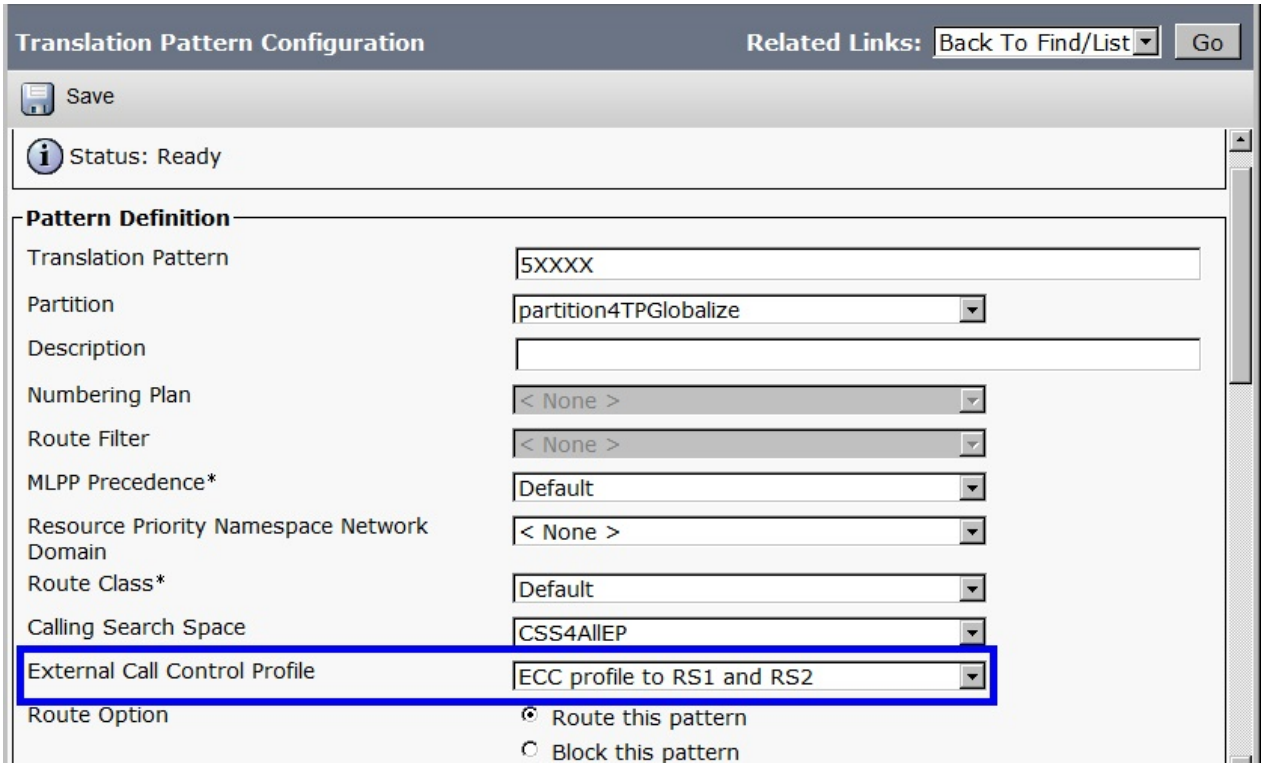
After setting up the External Call Control Profile, the trigger point needs to be set. At the trigger point, the UCM's routing logic decides which route request is chosen.

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.

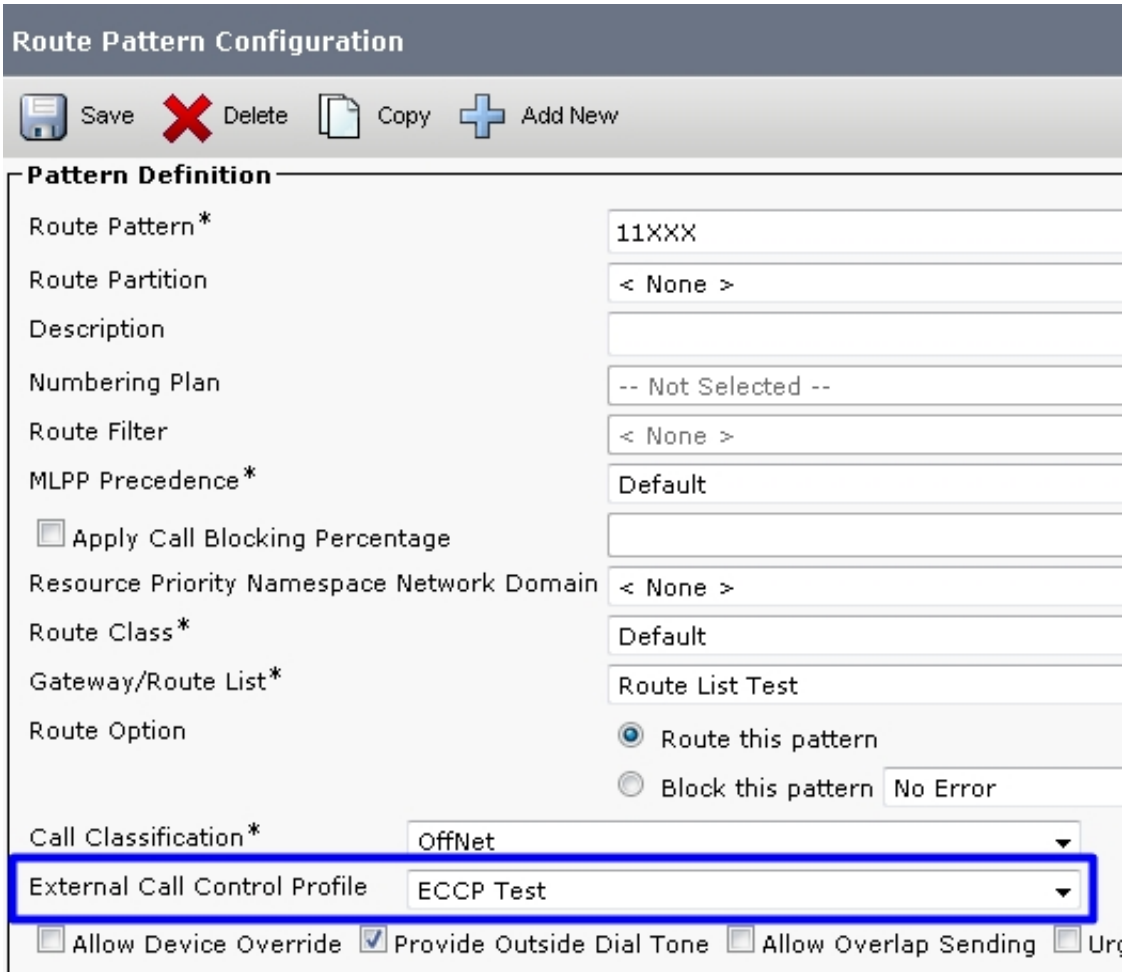
In the External Call Control Profile field set the External Call Control Profile that is configured as described above.



Route pattern as trigger point

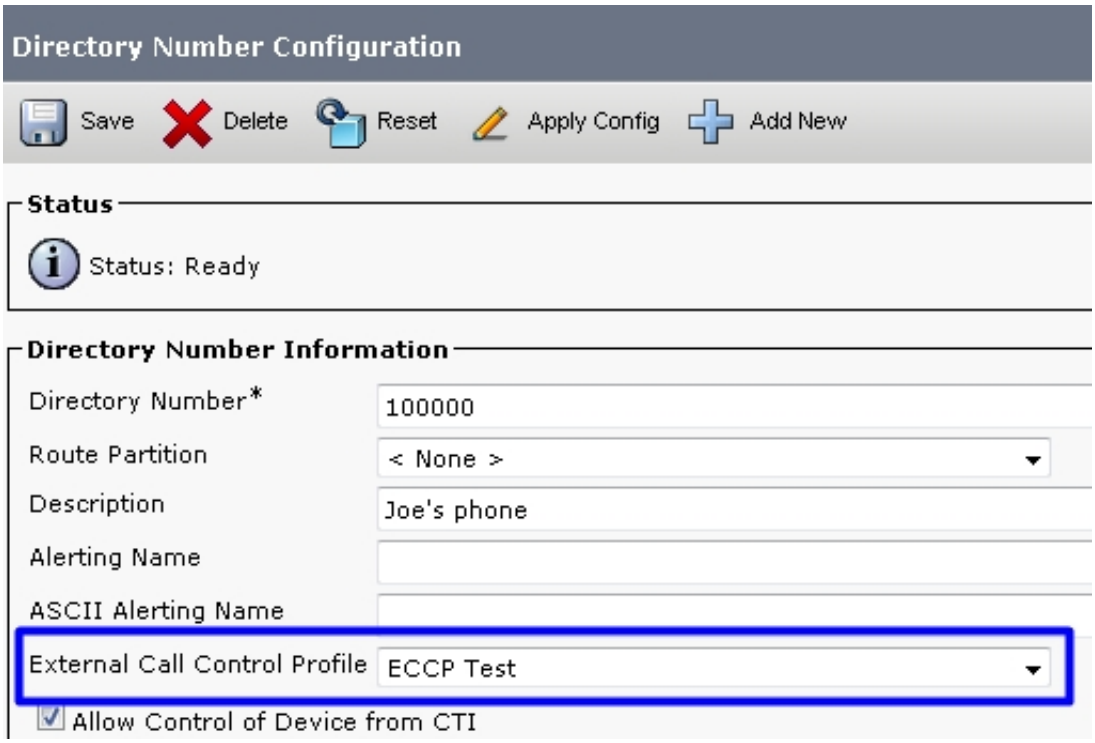
Go to Call Routing > Route/Hunt > Route Pattern and add a new route pattern or configure an existing one.

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



Directory number as trigger point

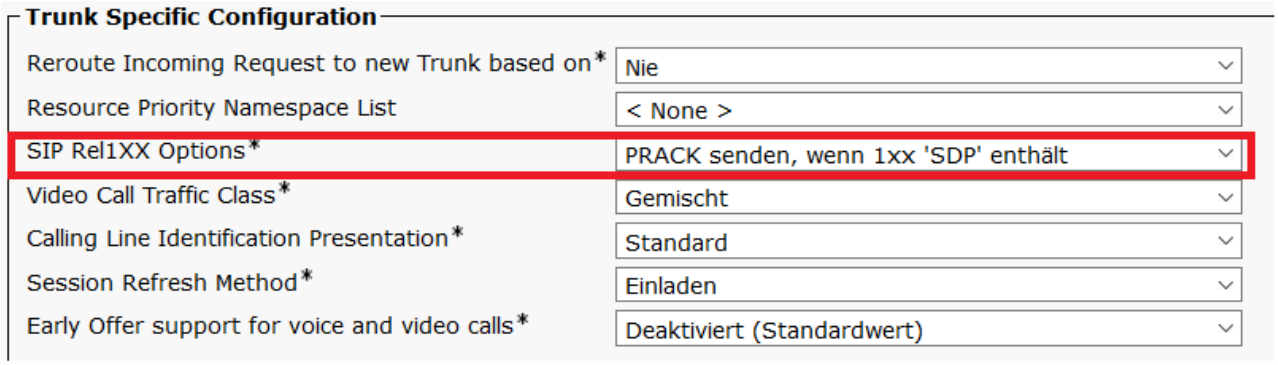
To use a directory number as a trigger point, go to Call Routing > Directory Number and set External Call Control Profile field to the one that you created, as described above.



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 trough, 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’.



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

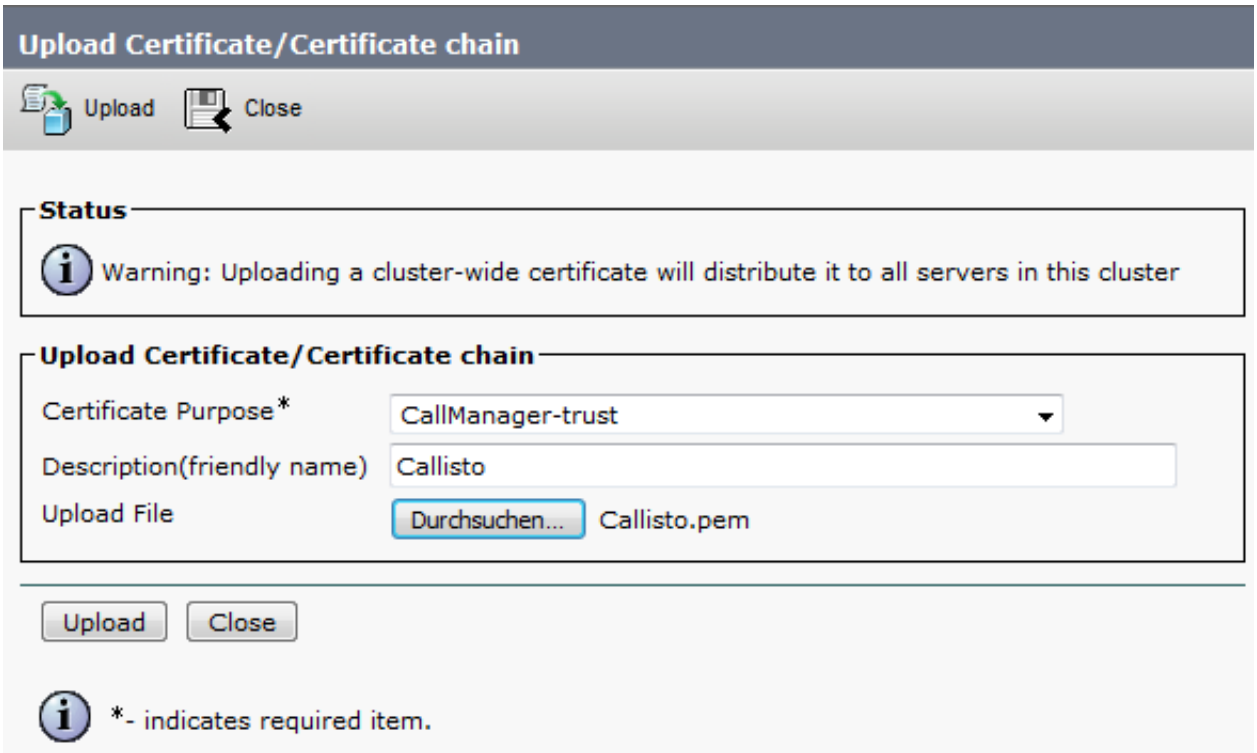
In the Callisto web interface, go to System > System Parameters > SSL Configuration (Top right corner) > Downlad PEM.
If there are no certificates yet, create a new self signed certificate… and download it.

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.

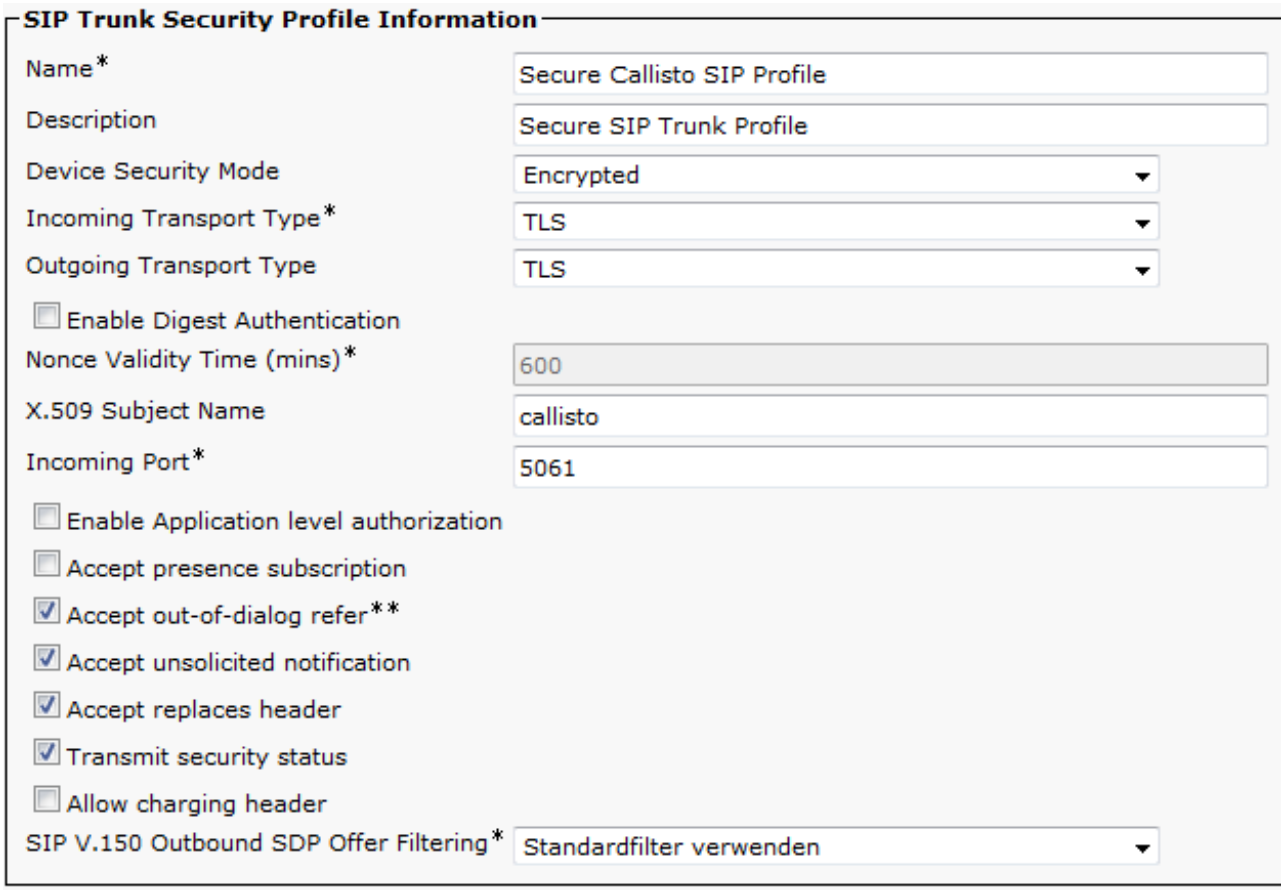
Go to Security > Certificate Management > Upload Certificate and upload the certificate that you previously downloaded from Callisto.
Choose CallManager-trust as the certificate purpose and provide a user friendly description like Callisto.



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 Profle and then Add New.

Fill in the profile information as following:



(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.

PLATFORM

CALLISTO VIRTUAL DEPLOYMENT MANUAL

Virtual deployment

Callisto systems can be deployed in a virtual environment. This page denotes the required information to deploy Callisto in a VMware ESX(i) environment.

Deployment package

The deployment package contains:

- This manual
- Single file appliance (*Callisto.ova*)

Minimal requirements

Environment (General)

- VMware ESX(i) 7

Environment (Callisto VM)

- 2 GB RAM
- 2 CPUs (c. 2 GHz)
- 80 GB hard disk space
- 1 Network adapter

Execute the deployment

1. Connect to the respective hypervisor using vSphere Client.
2. Start the deployment wizard (File > Deploy OVF Template…).
3. Browse for the appliance (*Callisto.ova*).
4. Check the OVF Template details.
5. Provide a name for the virtual machine.
6. Choose the designated datastore.
7. Select the preferred disk format (Thin provisioned format and Thick provisioned format are supported).
8. Select the network mapping.
9. Confirm the settings and start the deployment process by pressing Finish.
10. Wait for the import process to complete.
11. Right-click onto the newly deployed virtual machine and select Edit. Go to Hardware and select Video card. Change the setting to Auto-detect video settings.
12. Go to Hardware and select Network adapter 1. Set the MAC Address to Manual and enter the mac address provided by the licensing information you received by email.
13. Power-on the virtual machine.
14. After booting up (login screen available), upgrade the VMware Tools. To do so, right-click onto the respective virtual machine and select Guest > Install/Upgrade VMware Tools. Choose Automatic Tools Upgrade.

PLATFORM

ADMINISTRATION MANUAL

Documentation reference, requirements

In order to perform the tasks in this manual, a Cisco Unified Communications Manager (Express) or UC500 with an operational Callisto system is required. Detailed descriptions on setting up the Callisto system can be found in the relevant manuals.

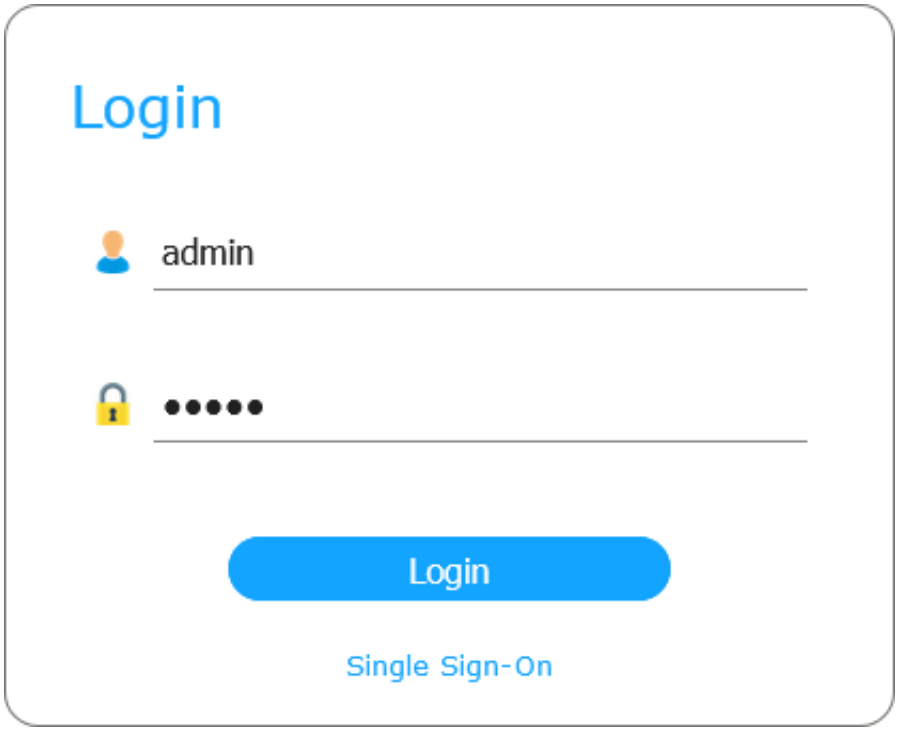
For administration tasks, a browser is required:

- Microsoft Internet Explorer: version 8.0 or higher
- Mozilla Firefox: version 2.0
- Safari and Chrome: current versions

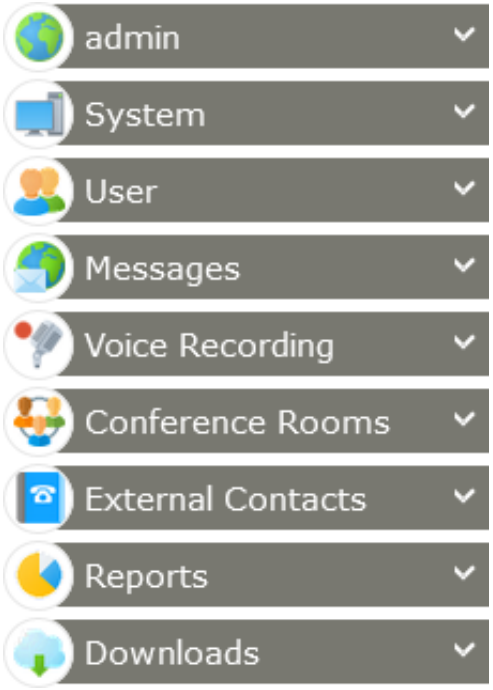
Administration management

Access Callisto with a browser from a client PC:

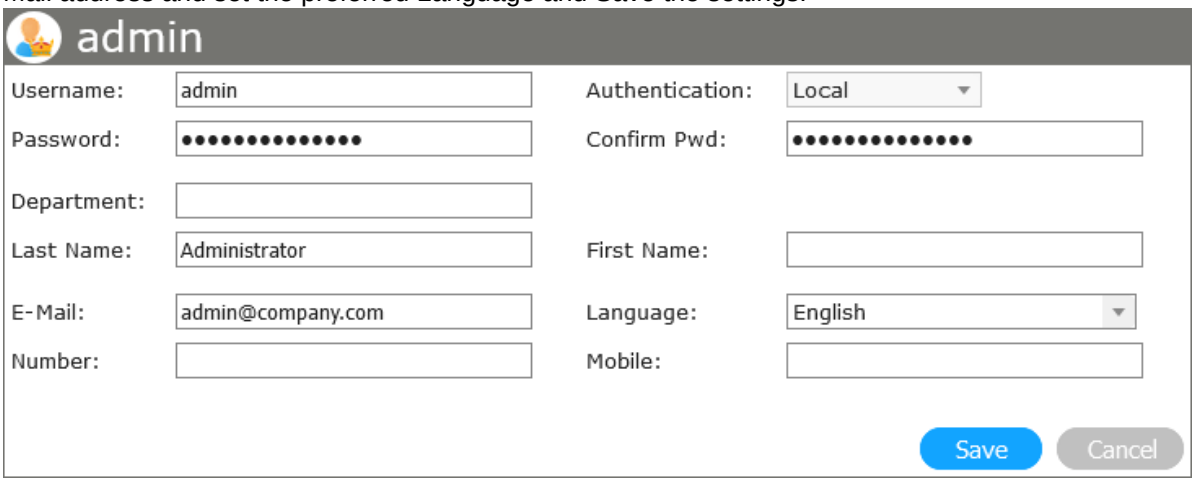
1. Connect to: http://<*callisto*>/, where <*callisto*> is the domain or IP address of your Callisto installation.
2. To logon, type the user name admin and default password admin. It is possible that the default administrator password was changed during installation. In this case, consult with the Cisco partner who performed the Callisto installation.



3. After successful logon, the administration navigation menu is shown.



4. After logging on for the first time, it is highly recommended to change the default user name and password for security reasons. From the navigation bar, choose admin > Account. Type a valid E-Mail address and set the preferred Language and Save the settings.

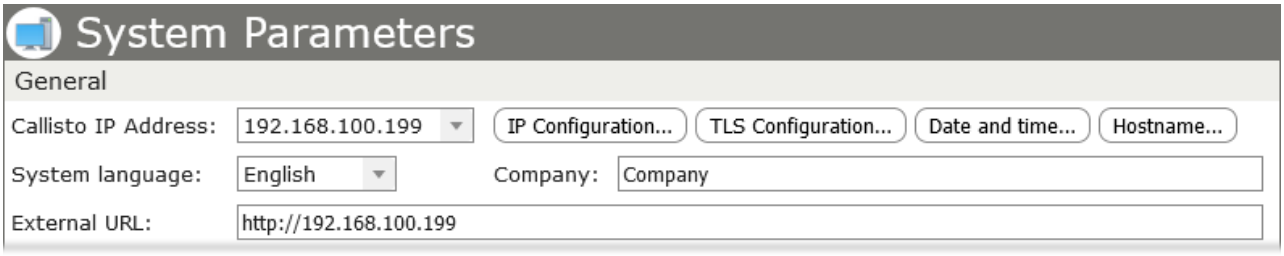


5. Administrator accounts cannot be used concurrently. Only one administrator at a time can be logged on to the appliance.
6. If the administrator's logon details should get lost, they can be retrieved from the backup system file. Therefore it is important to ensure that no unauthorized user has access to the backup file.

System

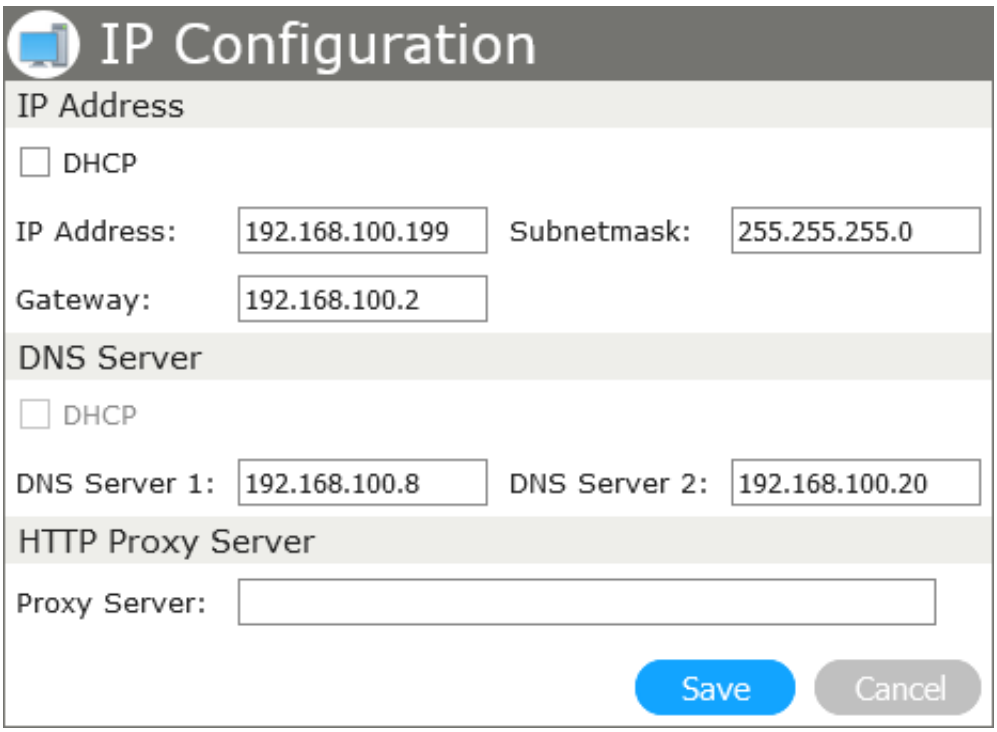
System parameters

On the navigation bar, click on System > System Parameter. Here, a multitude of settings and parameters can be examined and changed by the administrator.



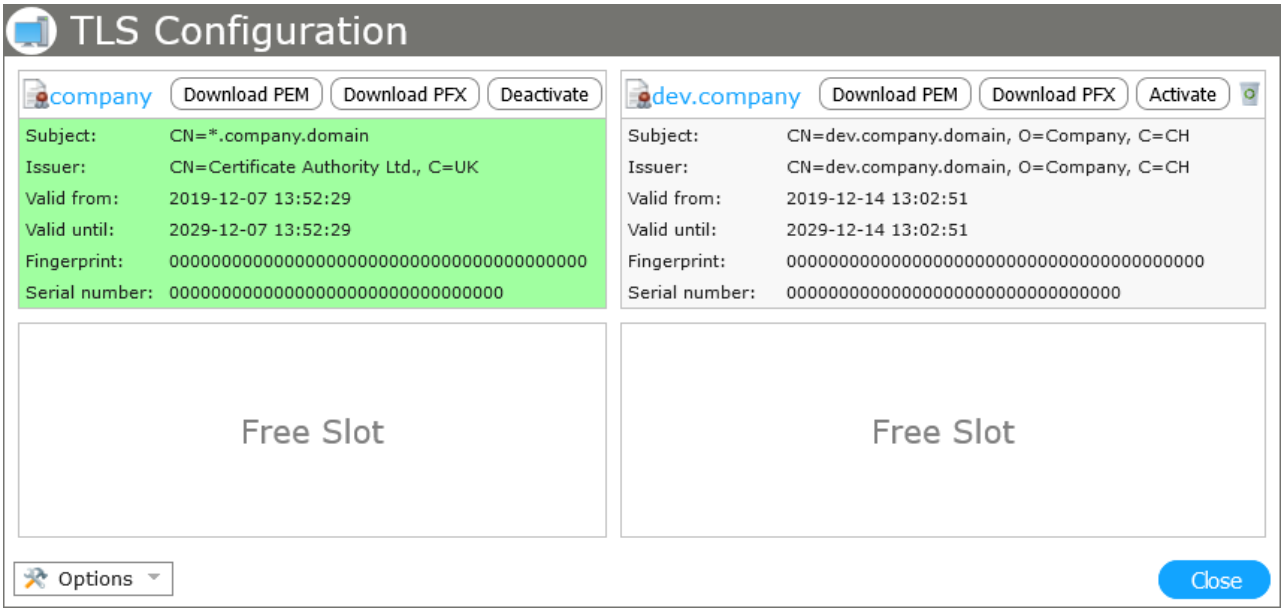
Callisto IP address(DHCP or static)

To set the parameters for a static IP configuration, click IP Configuration….



Secure web access

To set the parameters for a SSL web access, click TLS Configuration.



In the Options drop-down list, you can generate a new self signed certificate or import an existing one. The Import Certificate function only supports PFX files with a set password.

Next to the certificate name, buttons to export to PEM (i.e. for CUCM trusted certificates) and PFX formats are available for moving the certificate to another installation. PFX files will have the password callisto. Click Activate on the certificate to use this certificate and activate secure web access.

Other system parameters

In the Company text field, you can enter a custom text to identify your company. This text is displayed on the header of the web frontend and on the Cisco IP Phones if a system notification is sent (e.g. voicemails or fax information).

The parameter External URL is used to synchronize the “email marked as read” tag between the user’s email application and Callisto. If a user opens a voicemail or a fax message in their email application, the message will also be set to “read” on the Callisto system. This URL must be accessible from the outside web and point to the internal Callisto IP (port forward). You can also use HTTPS if activated on Callisto. The user must allow the download of external images for the Callisto email sender address (see Subsection “E-Mail”).

Subsection “Unified Communications Manager Express”

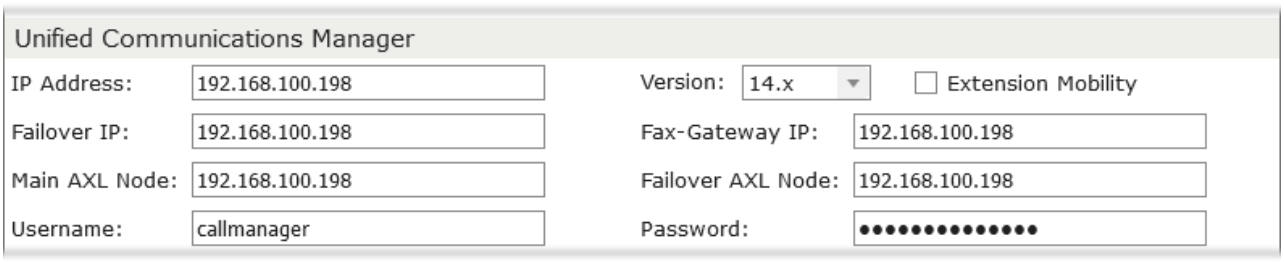
This section is only available on Callisto for CUCM Express.

Type the Cisco Unified Communications Manager Express’ Router IP Address and Subnetmask, including Router Password and Router Enable Password. Entering a Router User is optional.

Check Extension Mobility if you have users with EM enabled. Otherwise, leave this parameter unchecked to prevent unnecessary system load.

Subsection “Unified Communications Manager”

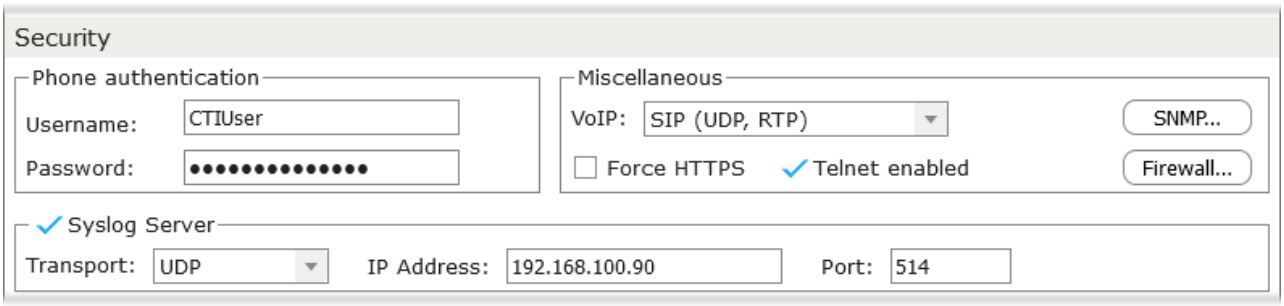
This section is only available on Callisto for Cisco UCM, HCS, Webex.



- In the field IP Address, type the address of the Cisco Unified Communications Manager *publisher*.
- In the field Failover IP, type the address of the Cisco Unified Communications Manager *subscriber*. The subscriber IP is used if the publisher cannot be reached. Callisto will then use the subscriber for all calls until the publisher is reconnecting to Callisto.
- Select the Version of your Cisco Unified Communications Manager.
- Check Extension Mobility if you have users with EM enabled. Otherwise leave this parameter unchecked to prevent unnecessary system load.
- Type the Username and Password for the Cisco Unified Communications Manager access user.
- Type the Fax Gateway IP Address (only for fax termination). Leave it empty to use the Cisco Unified Communications Manager’s IP for fax sending.

For the router and phone user configuration on the Cisco Unified Communications Manager, refer to the Callisto installation manual.

Subsection “Security”



Phone authentication

Type the Username and Password for phone authentication (XML-Push).

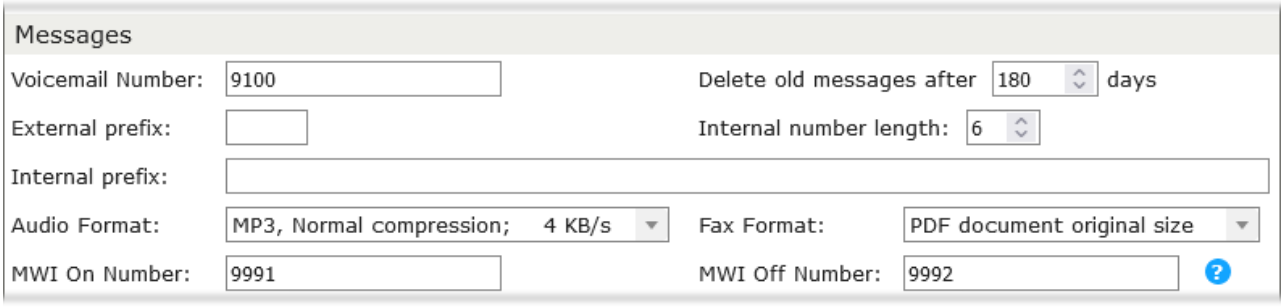
Miscellaneous

- Check the Secure SIP (TLS, SRTP) box to enable secured traffic to and from Callisto.
- Check the Telnet enabled box to monitor Callisto actions.

Syslog Server

If you want to use a syslog server, you can enter the connection details here.

Subsection “Messages”



- In the field Voicemail Number, type in the Voice Mail Pilot Number as configured in the Cisco UCM(see Cisco UCM configuration manual).
- Type the number of days after which old messages should be deleted in the Delete old messages after field. (0 = never)
- The External prefix is the prefix required to be entered by users to facilitate external calls during normal operation in the box. Applying the prefix depends on the following two parameters. Leaving the field empty will disable the external prefix.
  In order to use the external prefix, either one of the two parameters Internal number length or Internal prefix must be set.
- The Internal number length enables Callisto to distinguish between internal and external calls based on the length of the entered number. Setting it to 0 or leaving it empty disables this function.
- Internal prefix can be used as an alternative to the parameter above. If you have internal extensions of different length or using the e.164 number format on your trunk, use this method. This parameter is used to identify internal users and applying the external prefix on external calls. Leaving the field empty disables this function.
- The System language sets the display language that is used when a user calls Callisto from an external number before logging on.
- Audio Format determines the format in which voicemail attachments are saved.
- Using the Fax Format parameter, fax documents can be saved in either TIFF or PDF format.
- The MWI On and MWI Off Number parameters are only available with CUCM. These correspond to the MWI numbers configured in the Cisco UCM (see Cisco UCM configuration manual).

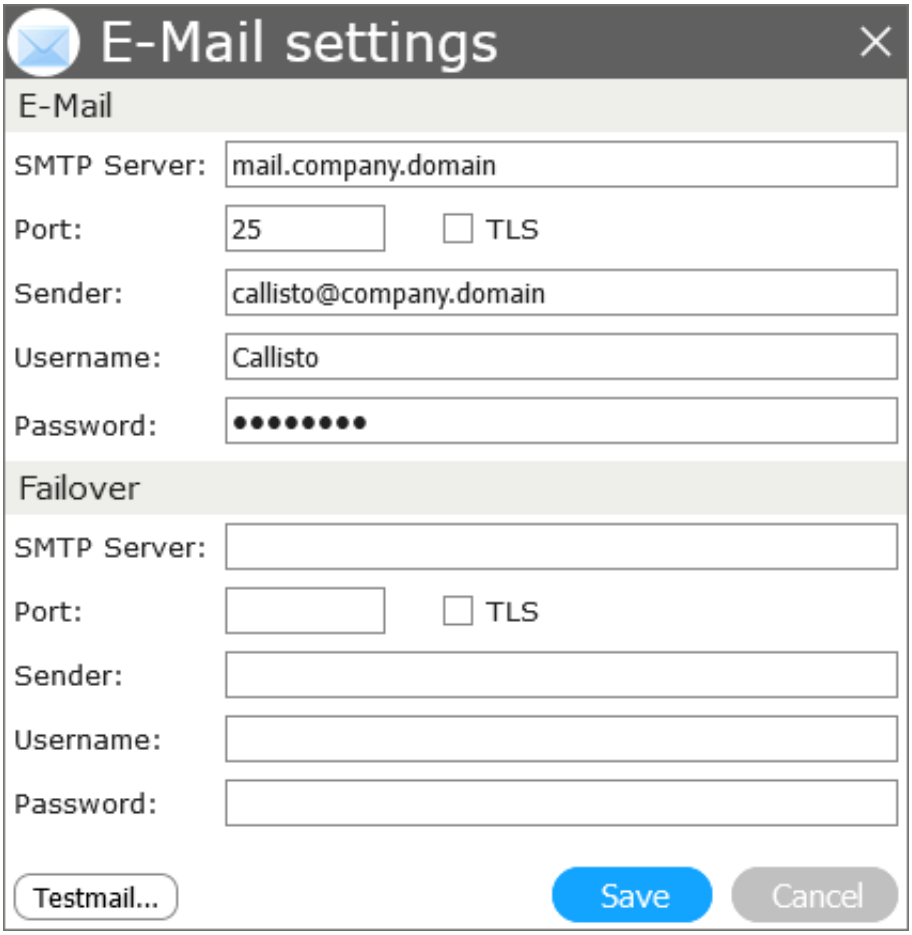
To listen to a voice mail by phone, dial the internal voice mail number. This number is dialled by users to access the voice messages for their phone. For external access an external number on the public telephone network must point to the internal number.

Subsection “E-Mail & SMS”

E-Mail settings

Enter your SMTP Server and Addressor's address as seen in the screen shot; optionally, for SMTP (RFC 2821) authentication, a Username and Password can be set.

In the section Failover, you can set an alternative email server if the primary one cannot be reached. The primary connection availability will be checked each time an email is send by Callisto.



SMS settings

Using Callisto, SMS can be either sent using the third-party provider aspsms.com or a custom email provider. The Settings dialog box will be different depending on the selected provider.

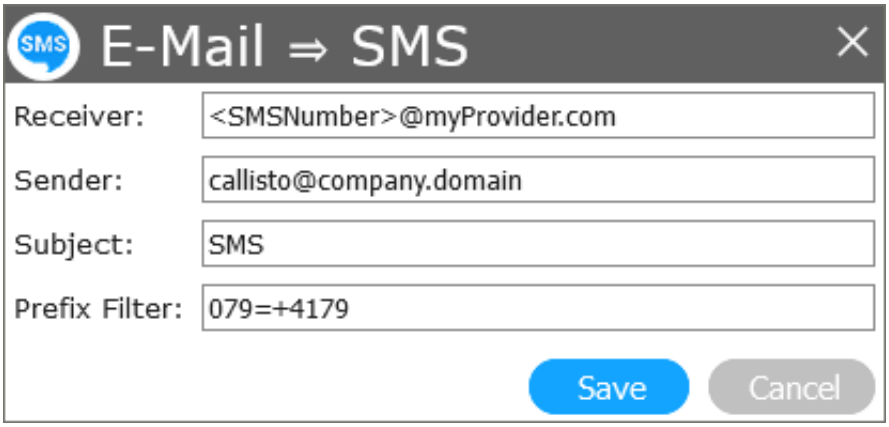
www.aspsms.com

Select www.aspsms.com from the SMS Provider drop-down list and click on Settings…, then enter the credentials of an active *aspsms.com* account.

E-Mail ? SMS

Using this method, Callisto will send an email to a provider of your choice. The provider will then convert the email into an SMS and forward the message.

Select Email to SMS from the SMS Provider drop-down list and click on Settings….

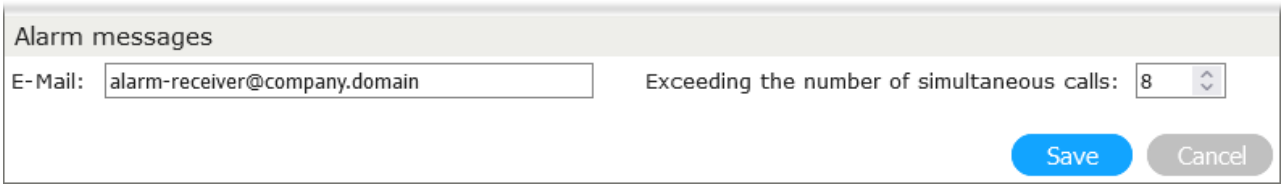


The term <SMSNumber> is a placeholder and will be automatically replaced with the recipient's phone number. Depending on the provider, this placeholder must be used either as part of the Receiver address or the message Subject in order to have the SMS properly forwarded.

Subsection "Alarm messages"

In order to use this function, the email configuration described above must be set up and running. Alarm messages will be sent to the address entered in the E-Mail field.

Exceeding the number of simultaneous calls will set the maximum calls that can be connected simultaneously before an alarm message is sent.



On Callisto for Cisco UCME

Clicking the Router Settings button displays the current Cisco Unified Communications Manager Express configuration.

When saving the system parameters, the Cisco Unified Communications Manager Express is configured automatically by Callisto.

On any Callisto Platform

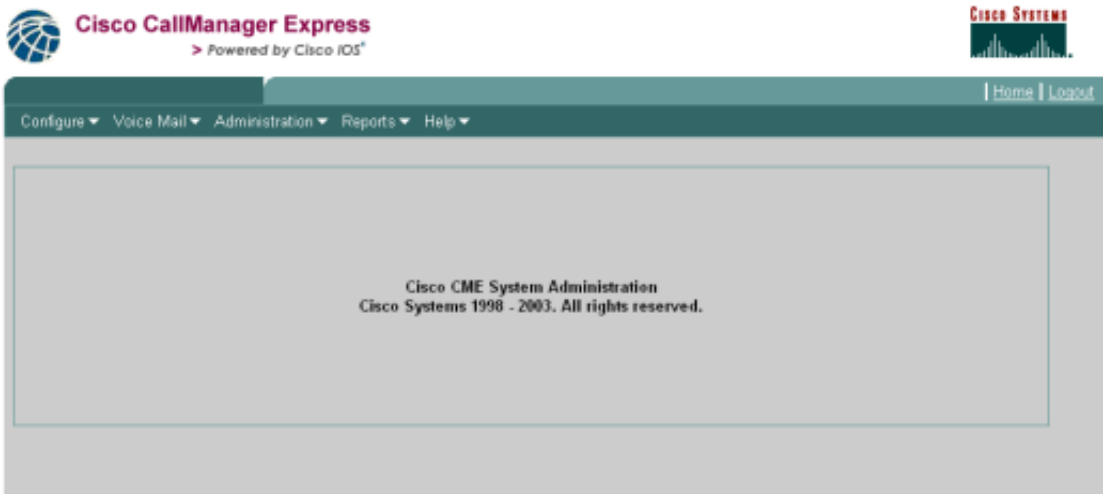
Save the current settings by clicking the Save button.

For the phone configurations to take effect, reboot the Cisco phones. Go to System -> Cisco Phone on the navigation bar, then click on the Reboot all button.

Cisco settings

Callisto for Cisco UCME only

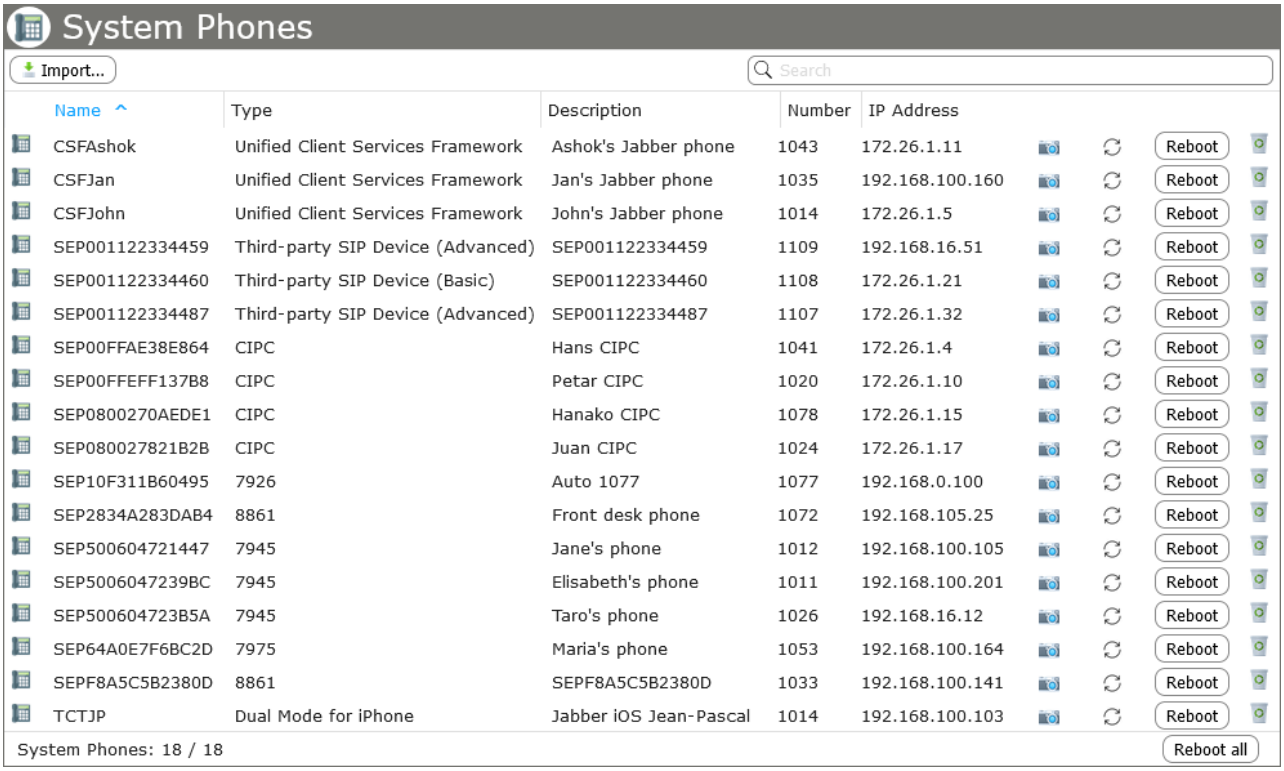
On the Cisco Unified Communication Manager Express, features such as routing of external to internal phone numbers can be configured, which can be used for remote access to voice mail boxes, fax and conference rooms.



Start the Cisco Unified Communications Manager Express configuration Web interface by clicking System on the navigation bar, then click Cisco Settings. For further information please refer to the manuals provided by Cisco Systems.

System phones

Clicking System > System Phones will list all IP Phones connected to the system. Phones can be rebooted individually by clicking on the Reboot button on the right side of the phone's list entry. All phones can be rebooted simultaneously by clicking the Reboot all button. Clicking on the *camera* icon will generate a screenshot of the phone's diplay.



Depending on the number of phones connected, generating a complete list can take several minutes.

The **Extended…** button generates a *txt* file with extended information on the phones, such as hardware revision, serial number, load information and memory overview. Generating this list can also take several minutes.

Only on Callisto for Cisco UCM, HCM, Webex

To initiate a manual import of the phones from the Cisco Unified Communications Manager, click the Import button. Alternatively, the import can be performed using the startup script “Import User Phones”.

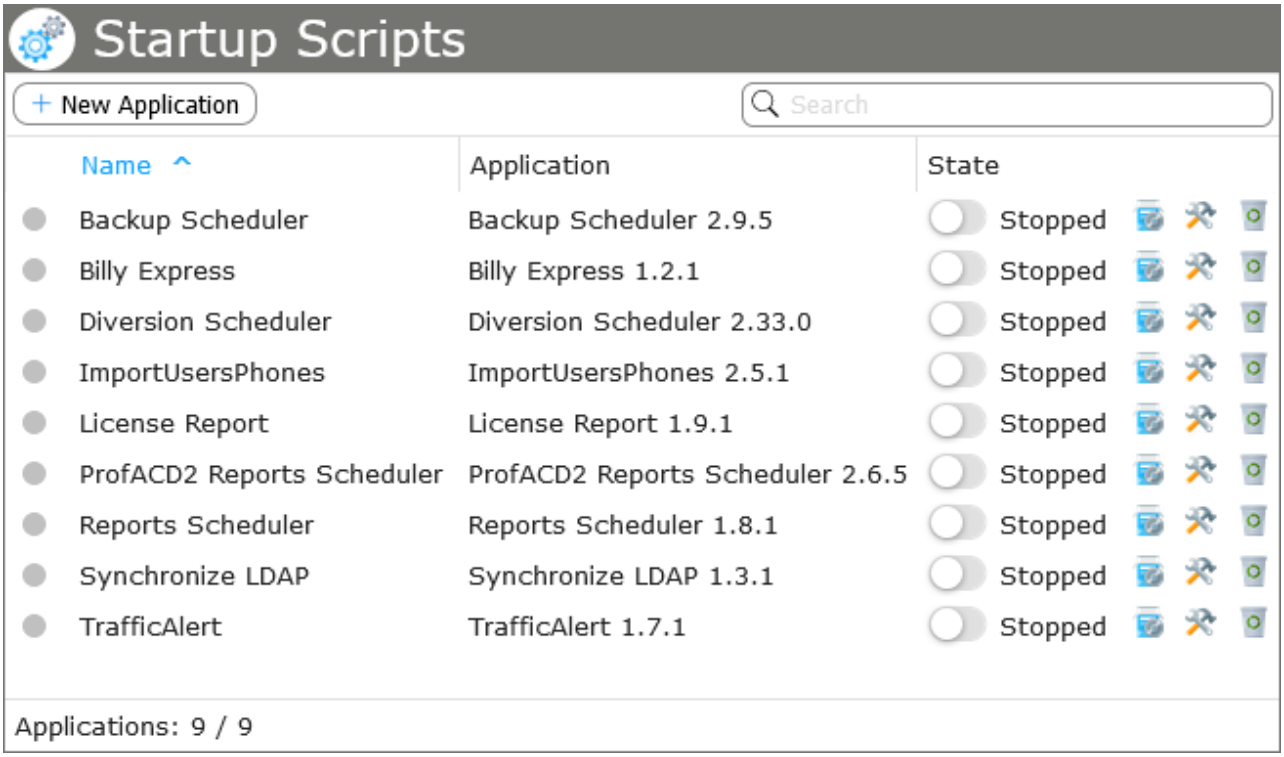
Startup scripts

Update icon

Configure icon

Clicking on Startup Scripts will open the startup script management application. Here, scripts can be transferred to the Callisto system by clicking the button New Application.The scripts can be configured to start automatically during system boot.

Use the *Update* icon to install or update your application. The *Configure* icon opens the configuration if the application has a GUI.



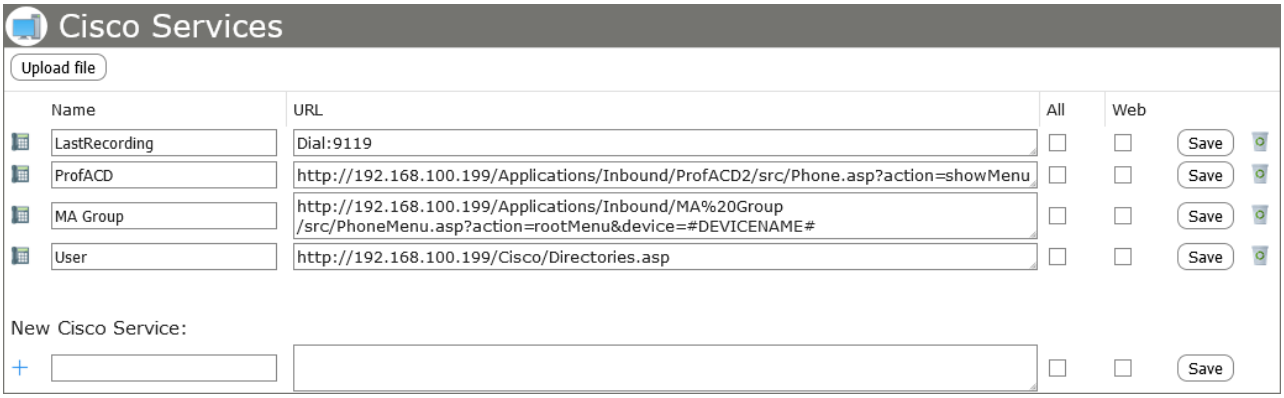
Cisco Services

Services button

Pressing the *Services* button on the Cisco IP Phone will by default display a selection screen for global and local directories. By choosing System > Cisco Services configuration, additional services can be set up that will appear in the Cisco Services selection screen. Examples of such services include:

- Weather forecast, currency and unit converter, world clocks, calendars, etc.
- Visualization and alarming features
- Control for equipment and devices (e.g. intercom systems and door control)
- Directory services

Cisco Services can be managed by choosing System > Cisco Services. A simple example for a service is a quick-dial number: Enter a number in the URL field using the format Dial:<*number*>, where <*number*> is any valid phone number.



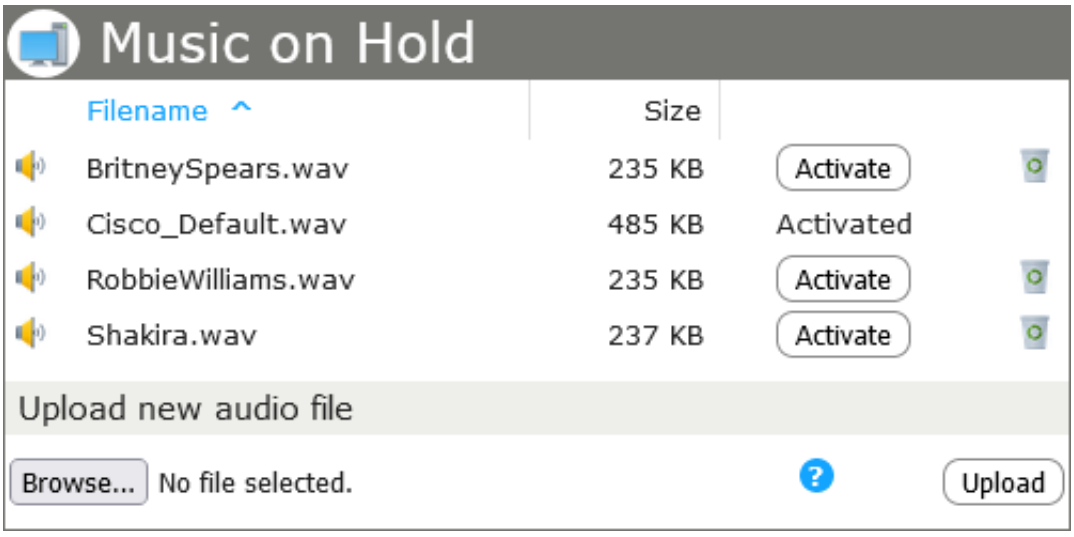
Checking All overrides any user privilege settings and makes the service available to all Callisto users.Checking Web enables the web frontend of this service and makes it available in the the user web GUI. This will only work for Cisco Services that have a dedicated web GUI.

Make sure that the URL of the Callisto Platform is configured properly in the Cisco Unified Communications Manager. Please refer to the Installation Manual.

Music on hold

You can change the music that plays when a phone user is put on hold by uploading a custom *.wav* file to Callisto. To do so, navigate to Music on hold > Browse > Upload.

After uploading, select the file and click Activate.



Recycle icon

Files can be deleted by clicking the *recycle* icon.

The *.wav* files need to be of the following format: CCITT A-Law 8 kHz; 8 Bit; Mono.

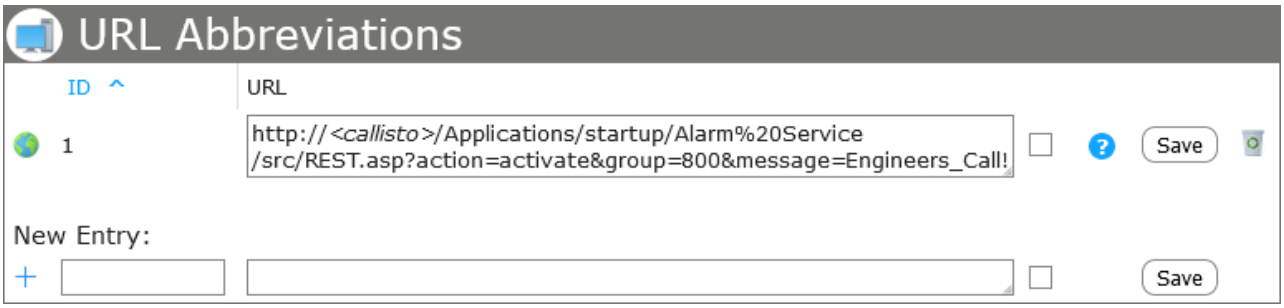
Per default, a Cisco music file (*Cisco_default.wav*) is activated.

On Callisto for UCME

The selection will be automatically stored on the Cisco Unified Communications Manager Express and will be used for all functions that use music on hold.

URL abbreviations

With URL abbreviations, you can shorten URLs using a single ID.



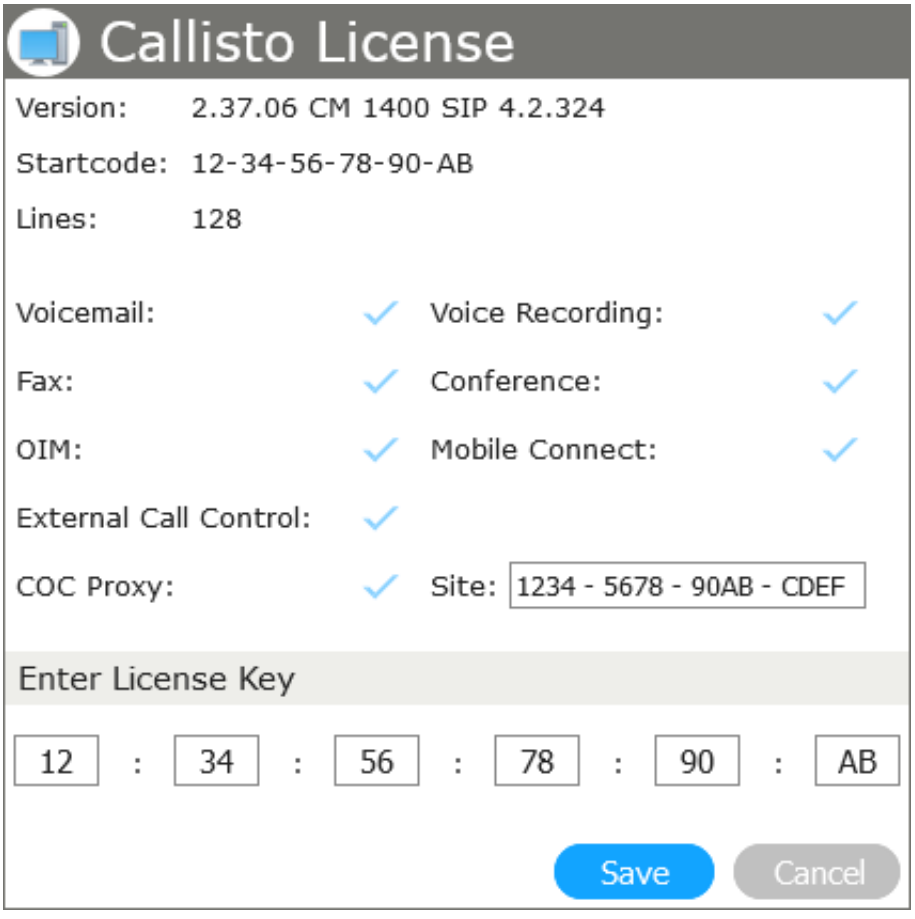
The example above would shorten the URL to http://<*callisto*>/ShortURL.asp?id=1 , with <*callisto*> being the domain name or IP address of your Callisto system and the value after id= being the number to the left of the original URL.

The checkbox to the right of the URL defines how the abbreviated URL will be linked:

- Unchecked: Bridging.
- Checked: Redirect. This option is more efficient, but may not work on all devices.

Callisto license

The basic version of the Callisto Platform includes four lines (*Callisto for UCM, HCS, Webex*) or two lines (*Callisto for UCME*), excluding any options. If you purchase any additional features or upgrades, you will receive a new license key that can be changed by choosing System > Callisto License. To obtain additional license keys, please contact your Callisto dealer (see Options).



The option Voice Recording is only available on Callisto for UCM.

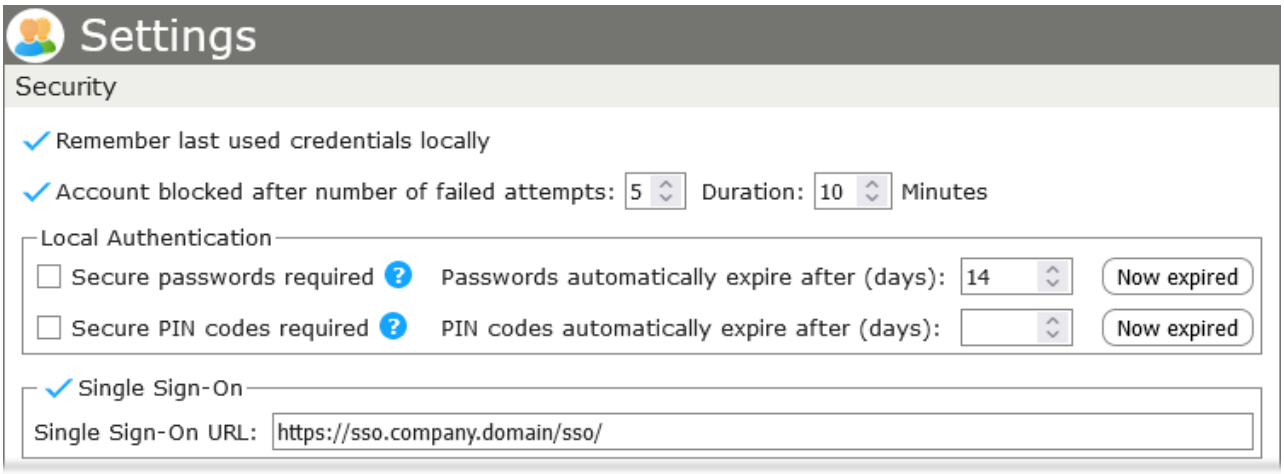
User administration

Administrators have the capability to manage any user's configuration and privileges through the User Administration screen.

User settings

These settings apply to all Callisto users.

Security



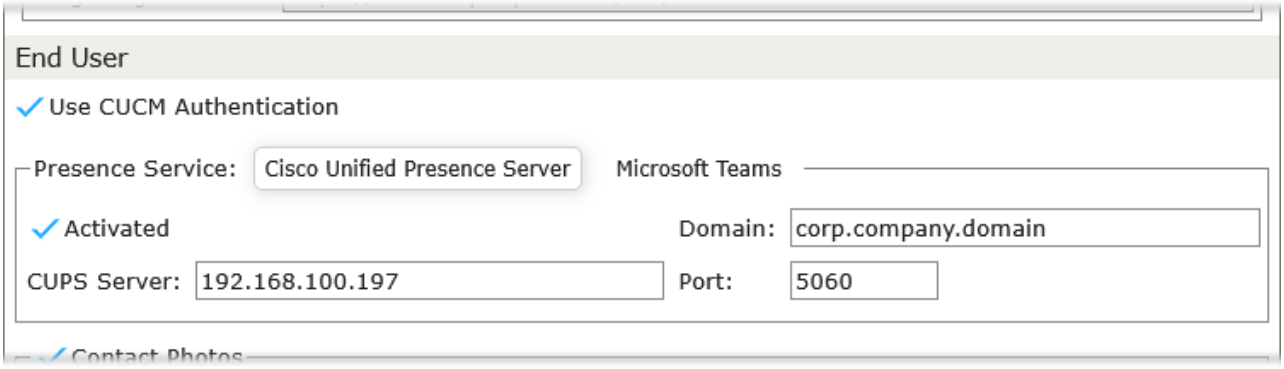
- When Passwords automatically expire after (days) is defined, users will be forced to change their password at the next login after the set expiration period.
- By clicking Now expired, all passwords from all existing users in Callisto will expire immediately. This only works if the parameter Passwords automatically expire after (days) is set.
- When Secure passwords required is set, users are forced to use passwords with higher safety. In this case, a password must be at least eight characters long and include at least one uppercase character, one lowercase character, one number, and one special character.
- PIN codes automatically expire after (days) and Now expired are the corresponding PIN code settings, as outlined in the password settings above.
- When Secure PIN code required is set, users are forced to use PIN codes with safety standards. In this case, PIN codes must have a length of 4–8 digits and may not include periodic sequences like 1234 (ascending digits), 8765 (descending digits), or 3885 (multiple identical digits in a row).

End user

These settings only apply to non-administrator users.

Checking Use CUCM Authentication will authenticate end users using CUCM.

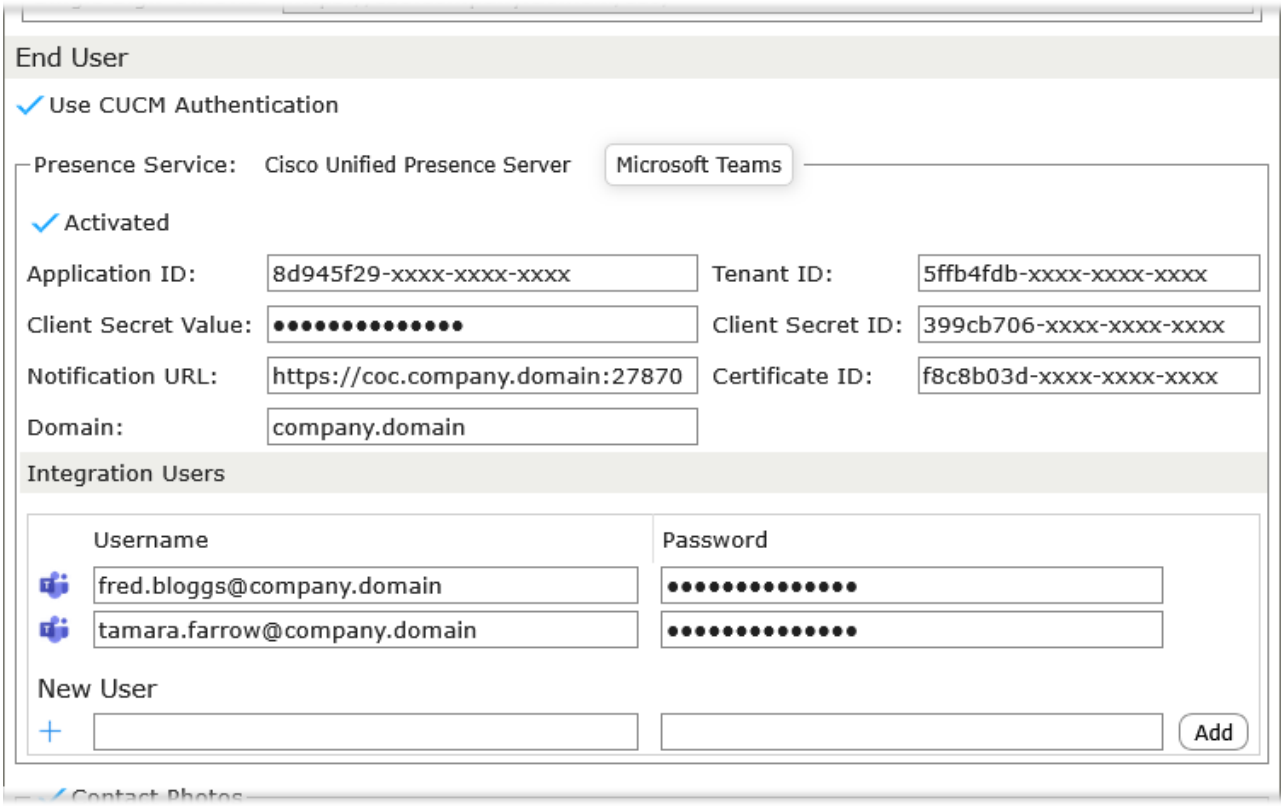
Authentication using Cisco Unified Presence Server



If Presence Service is set to Cisco Unified Presence Server, this section allows you to configure integration with Cisco Unified Presence Server (CUPS) to enable presence status visibility (e.g., available, busy, away) within the system.

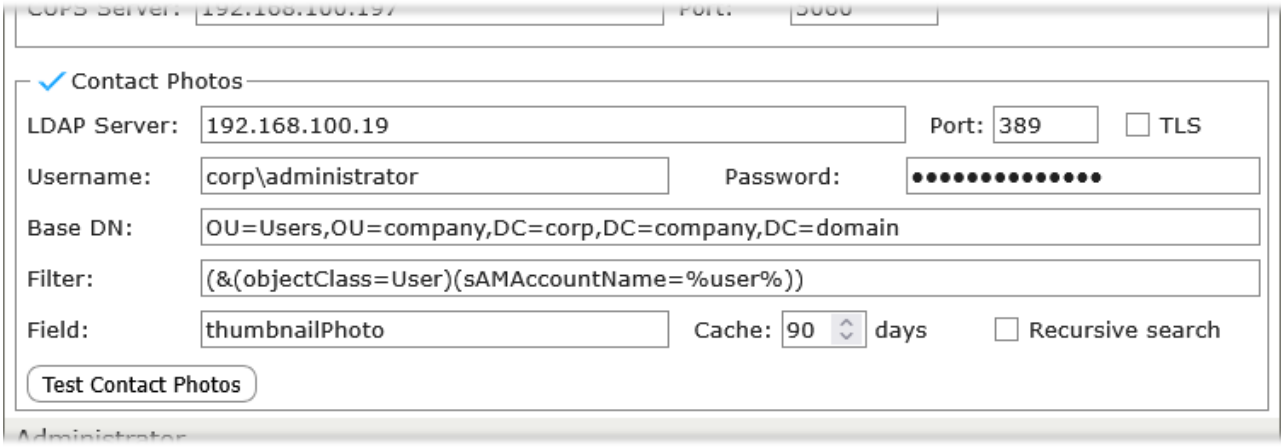
Activated	Check this box to enable CUPS integration. When activated, the system will connect to the specified CUPS server to retrieve and display user presence information.
CUPS Server	Enter the host name or IP address of your Cisco Unified Presence Server. This is the server that manages and distributes presence information.
Port	Enter the port number used to communicate with the CUPS server. Common port values include: • 5060 (for SIP over UDP/TCP) • 5061 (for SIP over TLS) • 8443 (for HTTPS-based communication)
Domain	Enter the domain name associated with your Cisco Unified Communications environment. This is often the same domain used in user SIP addresses (e.g., example.com). Ensure that the CUPS server is correctly configured, reachable from the system, and that proper credentials and licensing are in place.

Authentication using Microsoft Teams Presence



Activated	When checked, the Microsoft Teams presence integration is enabled.
Application ID	The Azure Active Directory (AAD) Application (Client) ID used to authenticate over the Microsoft Graph API.
Tenant ID	The Directory (tenant) ID from Azure Active Directory associated with your Microsoft 365 organization.
Client Secret Value	The secret key generated in Azure for the registered app. This key is used alongside the Application ID to authenticate API requests.
Client Secret ID	The identifier for the client secret in Azure AD. This ID used for managing secrets in Azure but might not be required, depending on the integrations.
Notification URL	The URL where Microsoft Graph sends change notifications for presence updates. It must be accessible from Azure and is provided by CTModule as part of the subscription to Callisto.
Certificate ID	If a certificate is used for encoding/decoding the rich presence data authentication, enter the certificate identifier in this field.
Domain	The domain associated with the Teams user accounts, typically in the form of *yourcompany.com*. This domain will be applied to all subscribed users.
Integration Users section	Used to add Microsoft Teams user credentials for integration. Up to 30 users can be added.
New User	Input the username and password for a user who will be used in the integration process. Click Add to save the credentials.

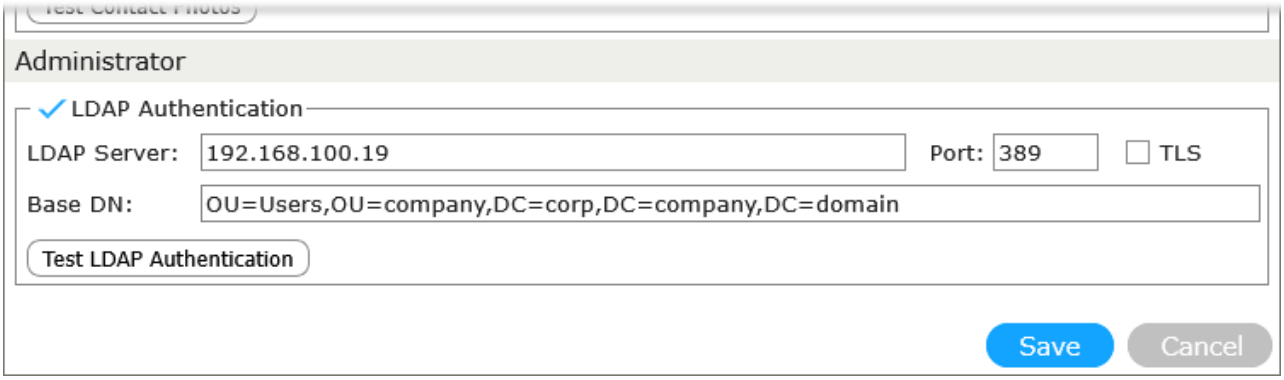
Contact Photos



Contact Photos section is used to retrieve and display user photos from an LDAP directory (such as Microsoft Active Directory).

LDAP Server	The hostname or IP address of the LDAP server (e.g., ldap.company.com).
Port	The port used to connect to the LDAP server. Standard ports: • 389 for LDAP • 636 for LDAPS (if TLS is checked)
TLS	Enables secure LDAP over TLS (Transport Layer Security). Check this if the LDAP server requires a secure connection.
Username	The distinguished name (DN) or login name used to authenticate against the LDAP server (e.g., cn=admin,dc=company,dc=com).
Password	Password for the LDAP user account.
Base DN	The base distinguished name from where the LDAP search begins (e.g., dc=company,dc=com).
Filter	LDAP search filter to locate users, e.g., (objectClass=person) or (sAMAccountName=*).
Field	The LDAP attribute that holds the photo data. For Active Directory, this is typically thumbnailPhoto.
Cache	Number of days to cache the retrieved contact photos to reduce repeated LDAP queries.
Recursive Search	When checked, the search includes sub-containers within the Base DN.
Test Contact Photos button	Allows you to verify the configuration and test photo retrieval without saving the settings permanently.

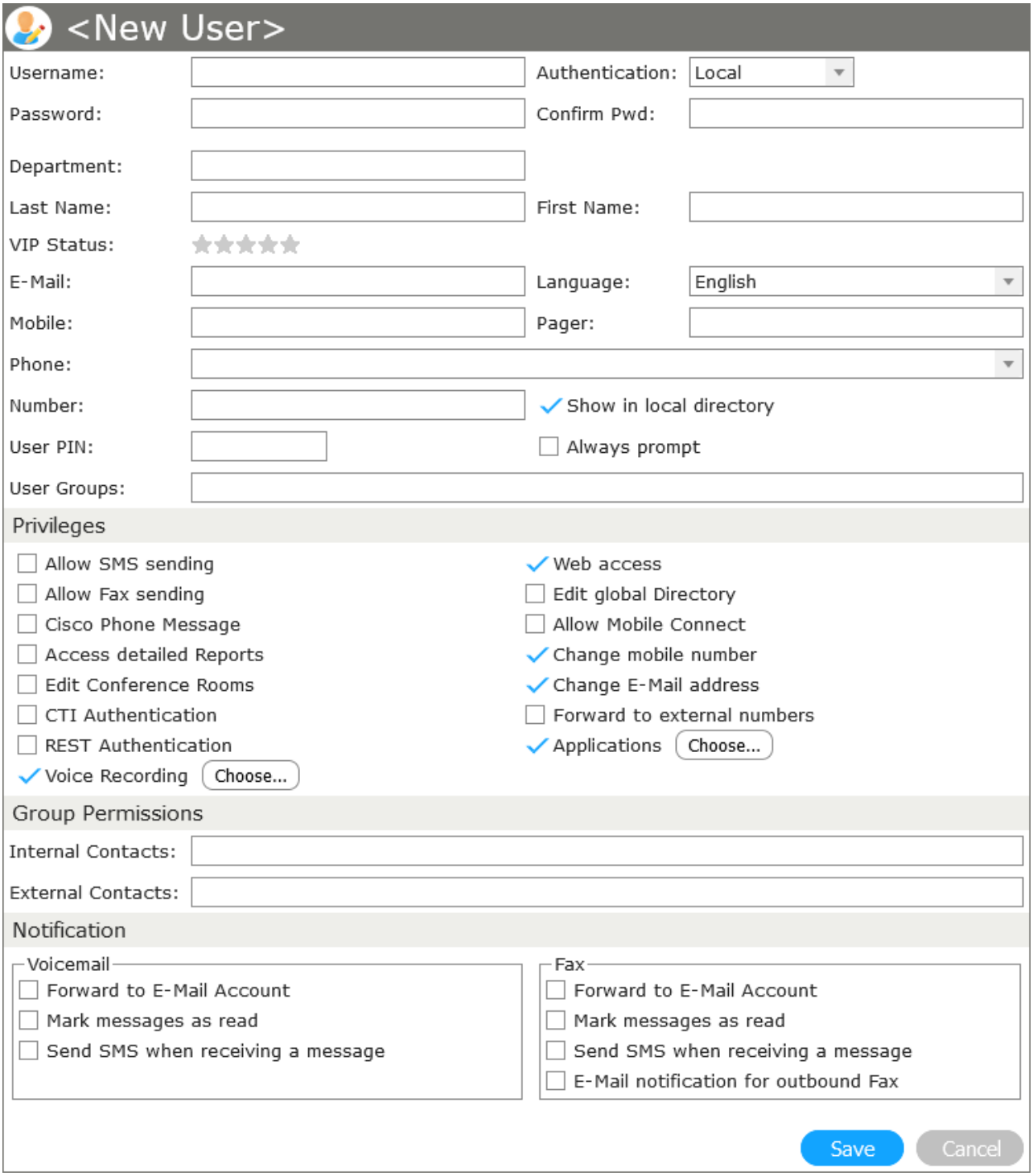
Administrator LDAP authentication



This section enables centralized administrator authentication through an external LDAP directory such as Microsoft Active Directory. This setup allows administrator credentials to be managed via LDAP, which supports centralized authentication and improved security management.

LDAP Authentication	Enables administrator login authentication via an LDAP server.
LDAP Server	The address (hostname or IP) of the LDAP server used for authentication, e.g., ldap.company.com.
Port	The port number used to connect to the LDAP server: • 389 for standard LDAP • 636 for LDAPS (if TLS is checked)
TLS	Enables Transport Layer Security (TLS) encryption for secure LDAP communication. Typically used with port 636.
Base DN (*distinguished name*)	Specifies the starting point in the LDAP directory tree for searching users, e.g., dc=company,dc=com.
Test LDAP Authentication button	Validates the LDAP settings by attempting a connection and search within the specified Base DN.

Add a new user



From the User menu, click New User to add a new user. Assign the corresponding IP phone by selecting it from the Phones drop-down menu, enter all other parameters and set the user privileges. When you're done, click on Save.

Click on the Choose… buttons to access additional settings.

The availability of some privileges depends on the license in use.

Options

Show in local directory	If checked, this user will be listed in the local directory on Callisto.
Always prompt	The user will always be asked to enter his phone PIN if he is calling the voicemail system. If left unchecked,

	the PIN needs only be entered if the call doesn't originate from the user's telephone extension.

Privileges

Allow SMS sending	Enables sending Fax by choosing Messages > Send SMS on the web GUI. Furthermore, the user can enable SMS notifications for incoming voicemail and fax messages.
Allow Fax sending	Enables sending Fax by choosing Messages > Send Fax on the web GUI. The user will also have access to the fax printer driver.
Cisco Phone Message	Enables Messages > Cisco Phone Message on the web GUI.
Access detailed reports	Enables Reports > Call Reports (global) on the web GUI. If unchecked, the user will find the function Reports > Call Reports (local) instead.
Edit Conference Rooms	Enables Conference Rooms > Conference LiveView > Edit on the web GUI. A user can only edit conference rooms that have been added by an admin beforehand.
CTI Authentication	Allows usage of the COC Proxy. If unchecked, the user will not be able to log on to the COC client.
Voice Recording	Sets options for Voice Recording. See Options – Voice Recording.
Web access	Allows the user to log on to the web GUI.
Edit global Directory	Enables Directory > New Entry > Category: Global on the web GUI. The user will also be able to edit already existing entries in the global directory.
Allow Mobile Connect	Enables Messages > Settings > Forward > Mobile Connect on the web GUI.
Change Mobile Number	Enables editing of the mobile number by choosing User > Account > Mobile on the web GUI.
Forward to external numbers	Enables using external numbers in the menu Messages > Settings > Forward on the web GUI. Make sure that the internal number length and internal prefix are configured properly in the menu System > System Parameters > Messages.
Applications	Access to individual applications like OIM applications, startup scripts or Cisco Services can be made available to the user. See also Options – Open Application Manager. For many applications, additional privileges can be set to control the scope of access individual users have for each application. Such privileges can be configured by clicking the button labeled "…" next to the application name. Refer to an application's administration manual for more details.

Voicemail notifications

Forward to E-Mail Account	Enables forwarding of voicemails to the user's email address.
Mark messages as read	Marks voicemails in the users inbox at Messages > Inbox on the web GUI as read.
Send SMS when receiving a message	Will send an SMS to the user's mobile phone when a new voicemail is received. To enable SMS notifications, the privilege Allow SMS sending must

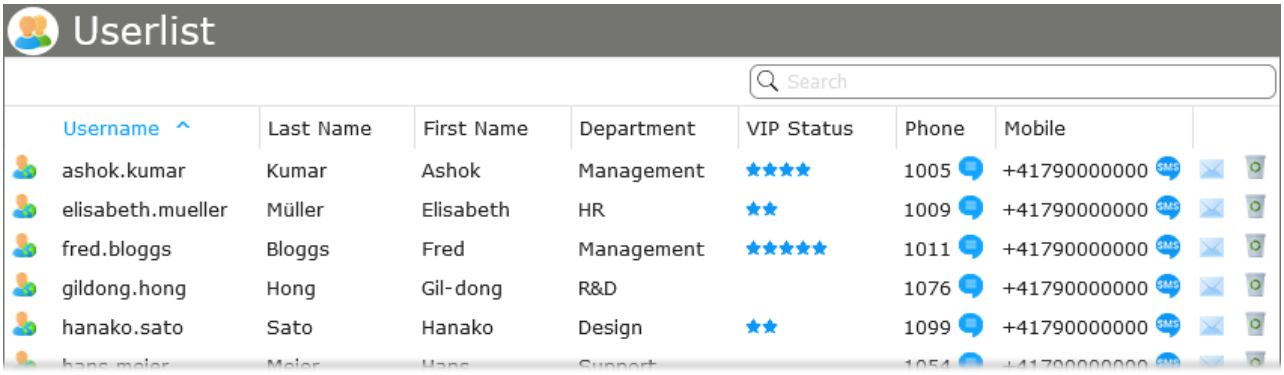
be checked.

Fax notifications

Forward to E-Mail Account	Enables forwarding of fax messages to the user's email address.
Mark messages as read	Marks fax messages in the users inbox at Messages > Inbox on the web GUI as read.
Send SMS when receiving a message	Will send an SMS to the user's mobile phone when a new fax is received. To enable SMS notifications, the privilege Allow SMS sending must be checked.
E-Mail notifications for outbound fax	Enabling this option will send a confirmation message to the user's email address whenever a fax message is sent. The user will be notified on both successful and failed fax transmissions. The original fax will be included as an attachment.

Edit users

Users' data can be verified, edited or deleted by choosing User > Userlist.



Recycle icon

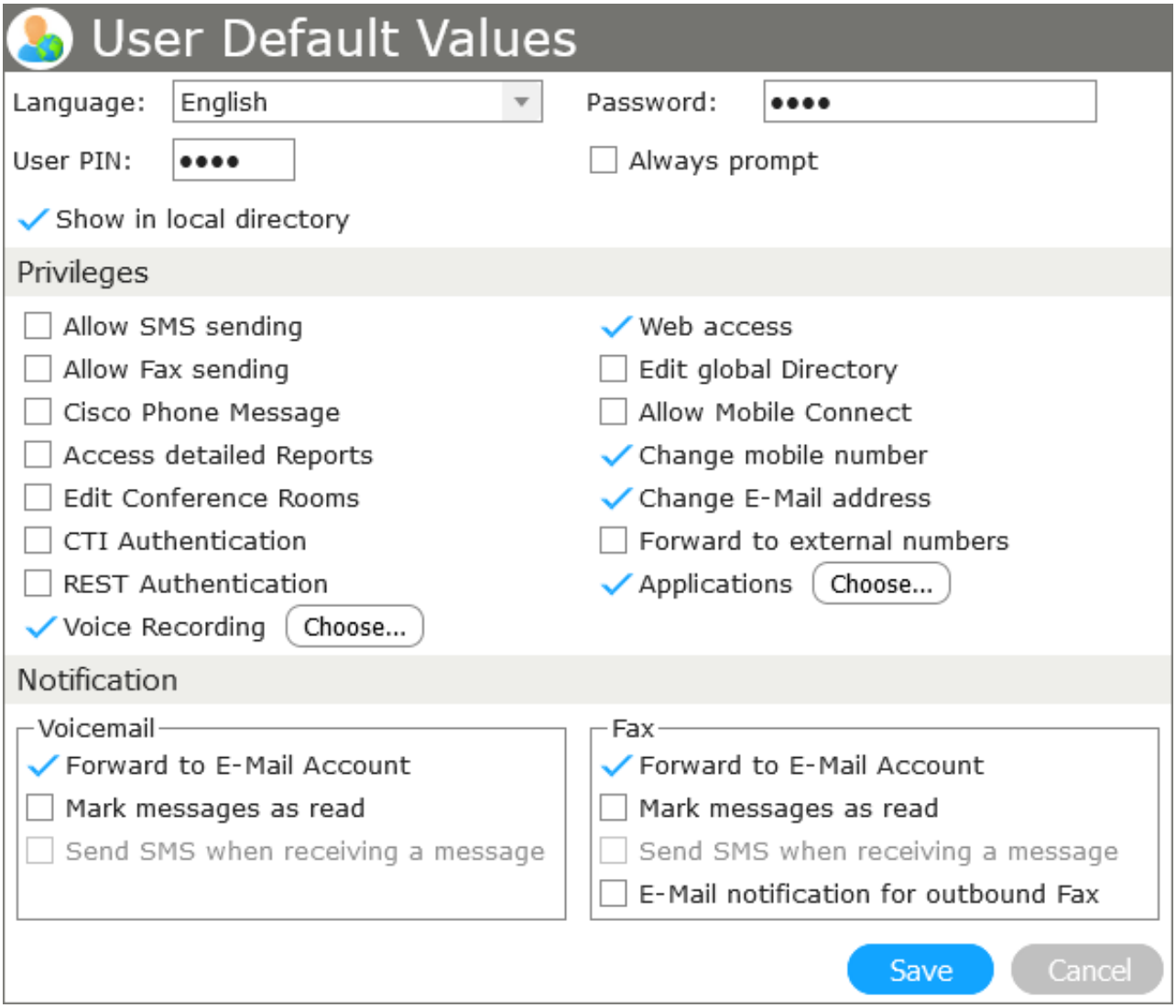
Phone message icon

SMS icon

- Use the Search box on the title bar to find any user or selection of users. For details on available search operators, refer to the search operators quick reference.
- User details and privileges can be edited by clicking on the list entry. Clicking on the *recycle* icon deletes the user.
- Click the *phone message* icon to send a Cisco phone message. The *SMS* icon initiates an SMS.

Default values

You can customize the default values assigned to new users by choosing User > User Default Values. These default values are also used when importing users (see Import users) if the import doesn't contain any user information.



User groups

User groups are used to manually group together multiple users to a set that can be used in various applications (e.g., granting access rights to all members of a group). Choose User > User Groups to add, edit, and delete user groups. Every group consists of a name, an optional description and an ID which cannot be edited.

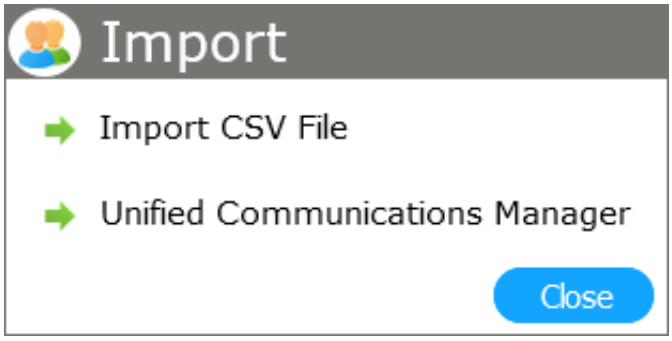
To add or remove a user from a group, choose User > Userlist, select the user you want to edit and choose all groups the user is a member of in the User Groups field.

Import users

Import with Unified Communications Manager

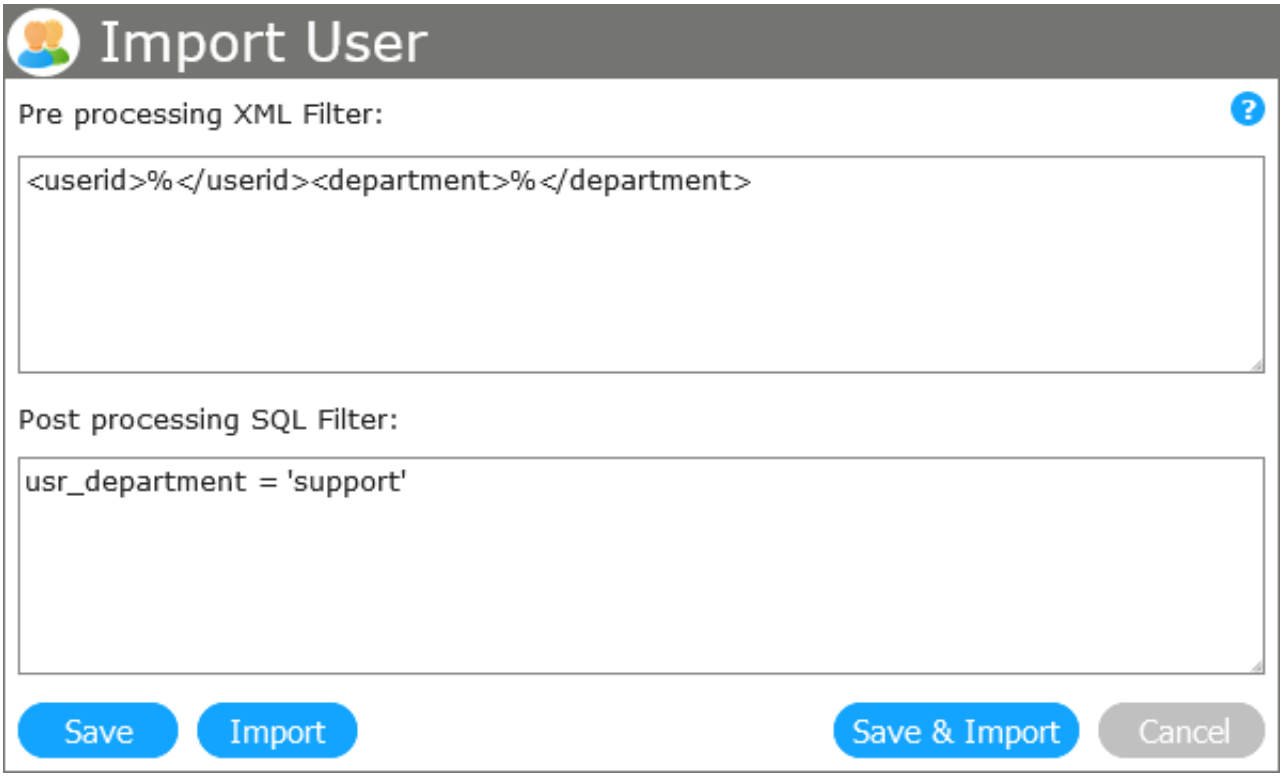
This option is only available on Callisto for UCM, HCS, Webex.

Choose User > Import User to import users by either importing a CSV file or to directly import the users saved in the Unified Communications Manager.



If you choose Unified Communications Manager, an additional dialog box will open which allows you to set XML and SQL import filters: The XML filter is run before importing. The SQL filter's field definitions match directly to the fields used in the Callisto user database.

All users previously imported from CUCM that do not match the filter will be deleted.



Post-processing SQL filter for all users that are in the *support* department, have a phone number between 1000 and 1999, and whose email address ends with *@example.com*.

```
(usr_department = 'support')
AND (usr_PhoneNumber >= '1000')
AND (usr_phoneNumber <='1999')
AND (usr_EMail like '%@company.domain')
```

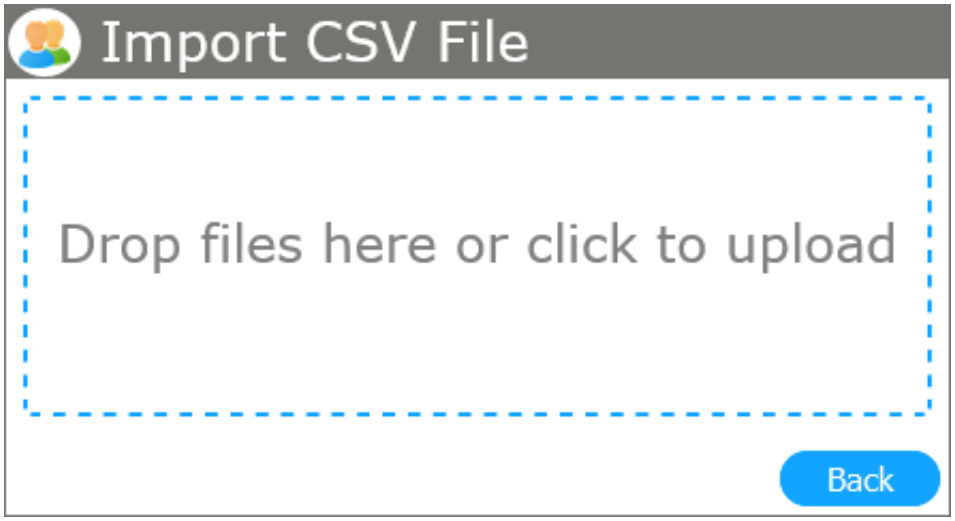
Additional SQL fields

Name	Type	Example
usr_Name	string	'paul.smith'
usr_LastName	string	'smith'
usr_FirstName	string	'paul'
usr_eMail	string	'user@company.domain'
usr_PhoneMac	string	'SEP002304342534'

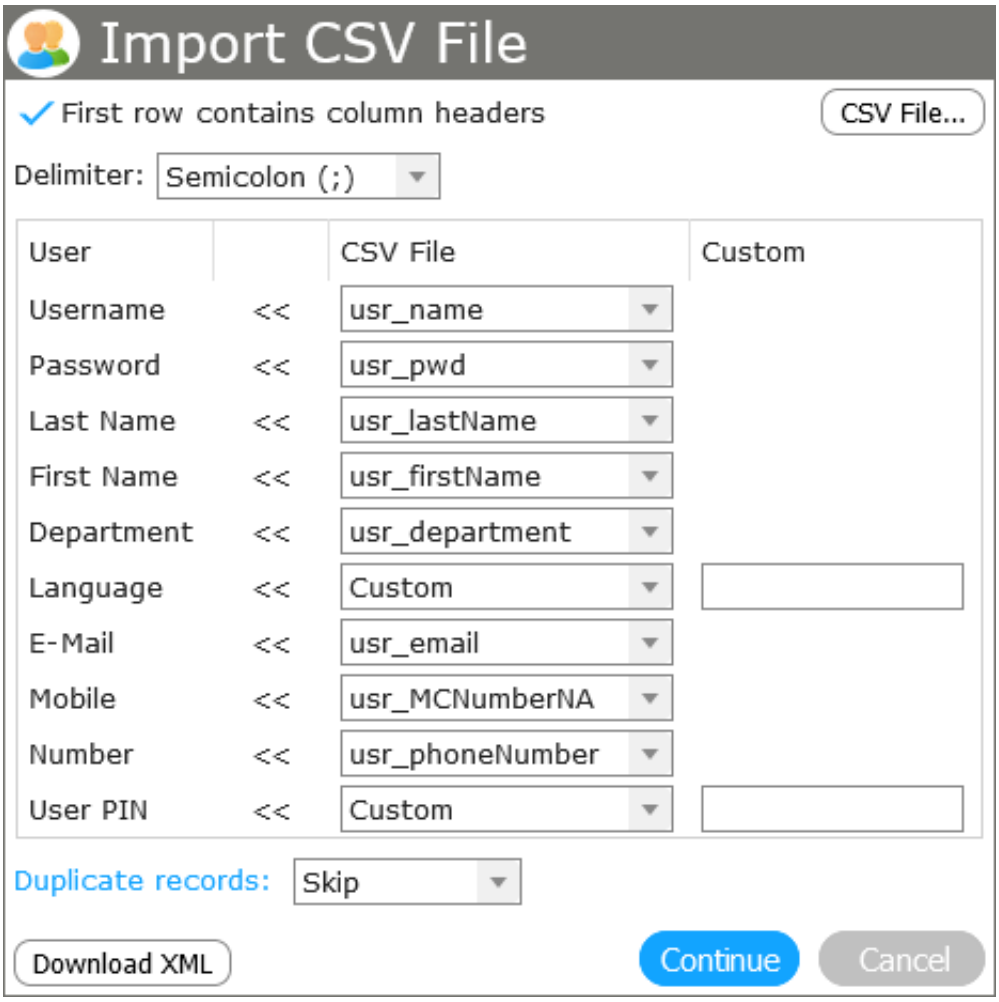
Name	Type	Example
usr_PhoneNumber	string	'1001'
usr_Department	string	'support'

Import with CSV

If you choose Import CSV File, you will be guided through the import process with additional dialog boxes.



Select the CSV file and it will be uploaded automatically. In the next window, you can assign the source CSV fields to Callisto fields.



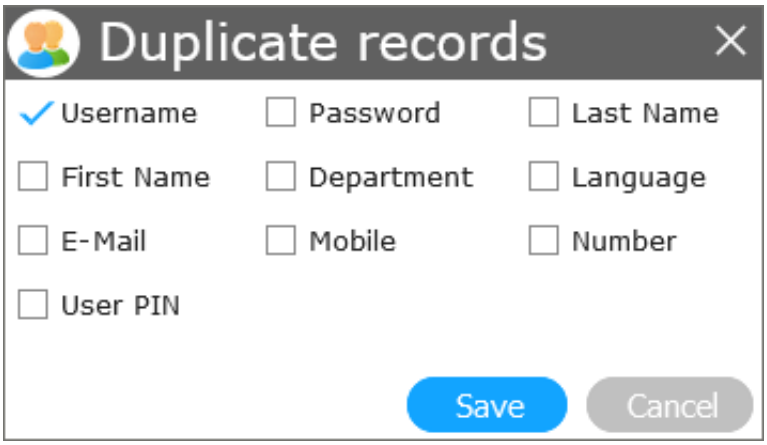
Select the proper Delimiter used in your CSV file. If the file's first row consists of a header record, check First row contains column headers.

Select the fields that correspond to the data in your CSV file.

The language is represented as a value between 1 and 5.

- 1 = English
- 2 = German
- 3 = French
- 4 = Italian
- 5 = Spanish

Clicking on Duplicate Records gives you the option to determine records that already exist in your contact list. If you select multiple checkboxes, the records where *all* values are identical will be treated as duplicate records.



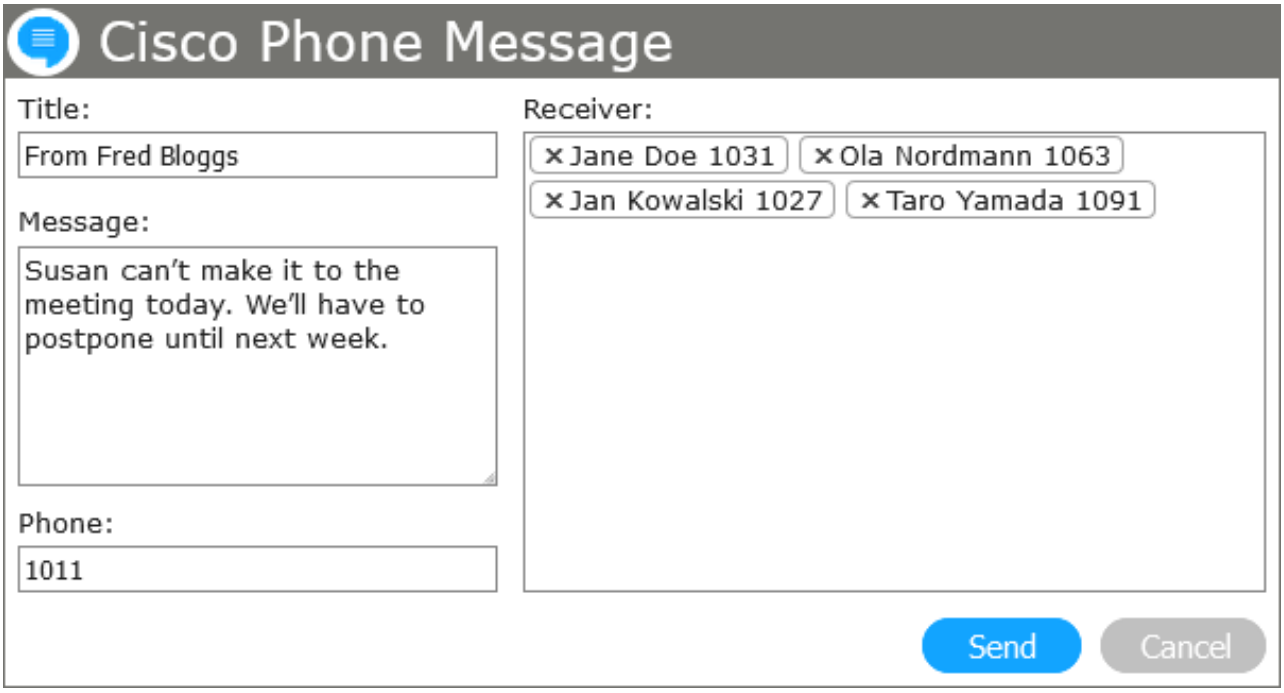
In the drop-down list to the right of Duplicate Records, you can decide how to handle duplicates.

When you are ready, click on Continue and the import will start. Once the import is finished, a summary will be displayed.

Messages

Choosing Messages > Cisco Phone Messages lets you use the messaging service. Messages sent from this service will be displayed on the phones of all selected users, allowing any user of the PBX system to be contacted at any time.

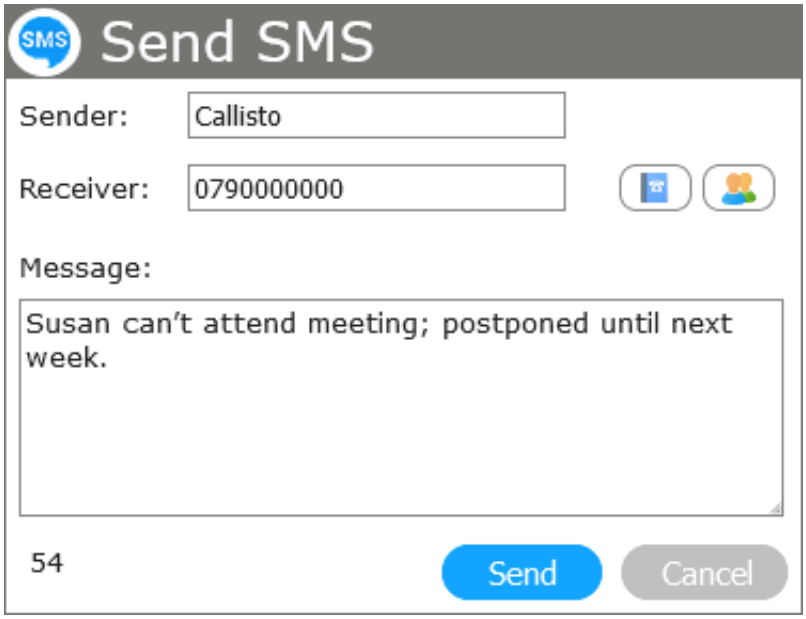
Type a title, the message and your phone number. The recipients can call back to the number you entered by the press of a button on their Cisco IP Phone.



Message > Send SMS allows users to send short messages to any phones which are able to receive SMS. In order to use this service, the SMS provider needs to be set up and working (see System parameters – SMS).

SMS icon

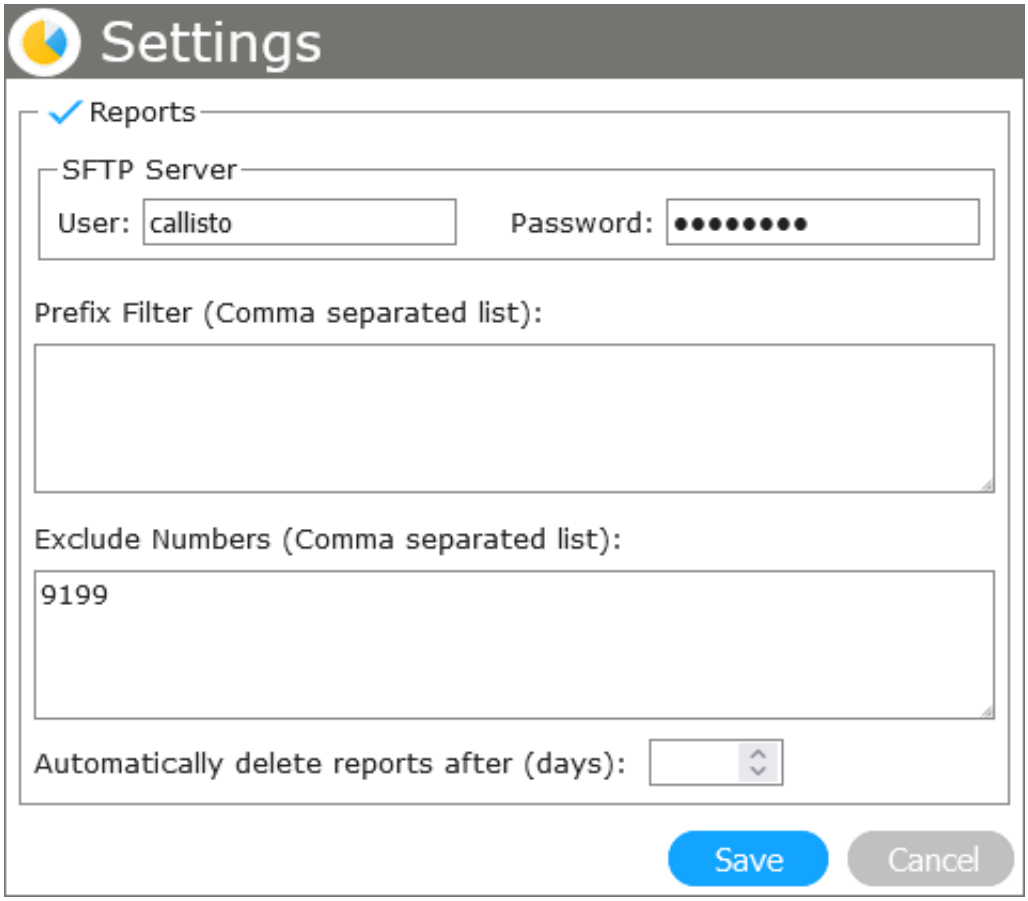
Enter the number or select a recipient from your directories. Open a directory, search the recipient, and confirm the number with a click on the *SMS* icon. To send the message, click Send.


Send SMS
Sender:
Callisto
Receiver:
0790000000
Message:
Susan can't attend meeting; postponed until next week.
54
Send
Cancel

Reporting

This chapter will provide a detailed overview of the reporting capabilities the Callisto Platform provides.

By selecting the relevant checkbox in the Privileges section of the user administration (User > Userlist, then click user to edit) the rights for access to the reporting feature can be assigned to any individual user. (see chapter 0, User Administration).



Click Settings and enter a username and password. The same credentials will be used in the Cisco Unified Communications Manager for SFTP CDR transfer.

Enter a value if you want to automatically delete reports after a specific amount of days.

With the Prefix Filter, you can enter values which will be stripped from the numbers (e.g. prefixes used by Mobile Connect).

If you want specific numbers to be excluded from the reports, you can enter them in the Exclude Number text field. Numbers are separated by commas (,).

Filter Analyses

Create a New Filter for analyzing the data. After entering a Filter Name and a Description, the filter can be edited. You can enter a different filter name and description for each system language.

In the drop-down menu Field, the following entries can be selected:

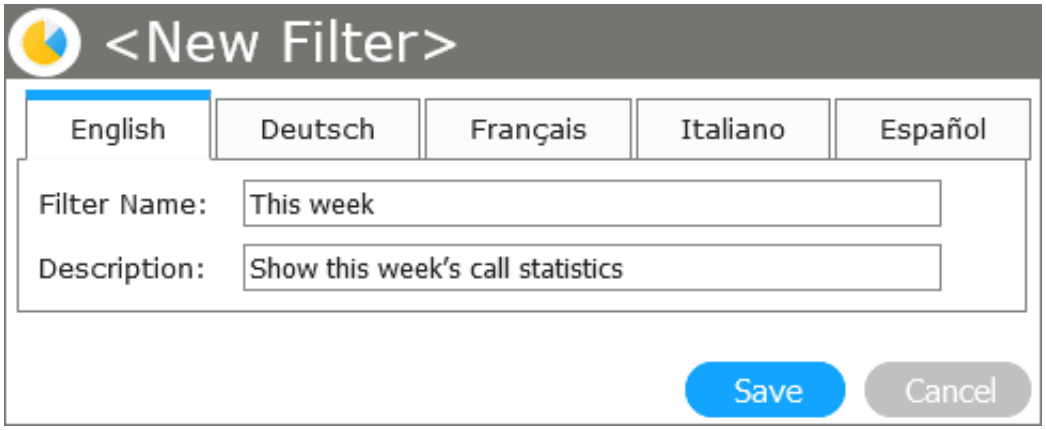
- Date/Time, Caller
- Called
- Duration
- Account Code
- SQL

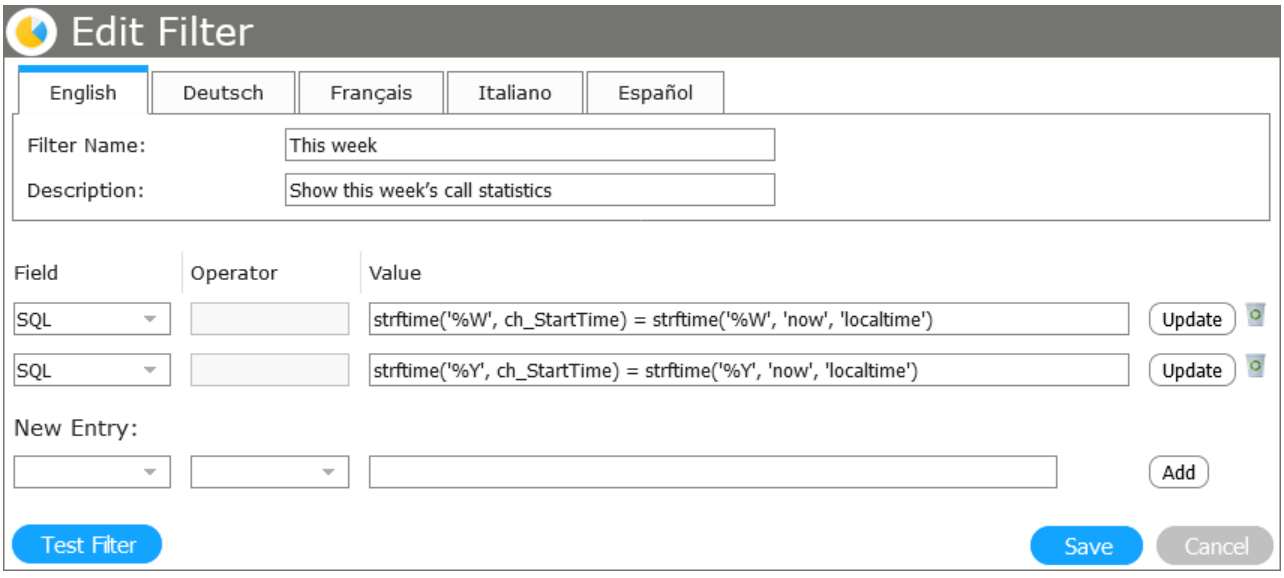
The following operators can be selected:

- equal to
- greater than
- smaller than
- different from
- SQL

A value must be added for the filter criteria to be valid.

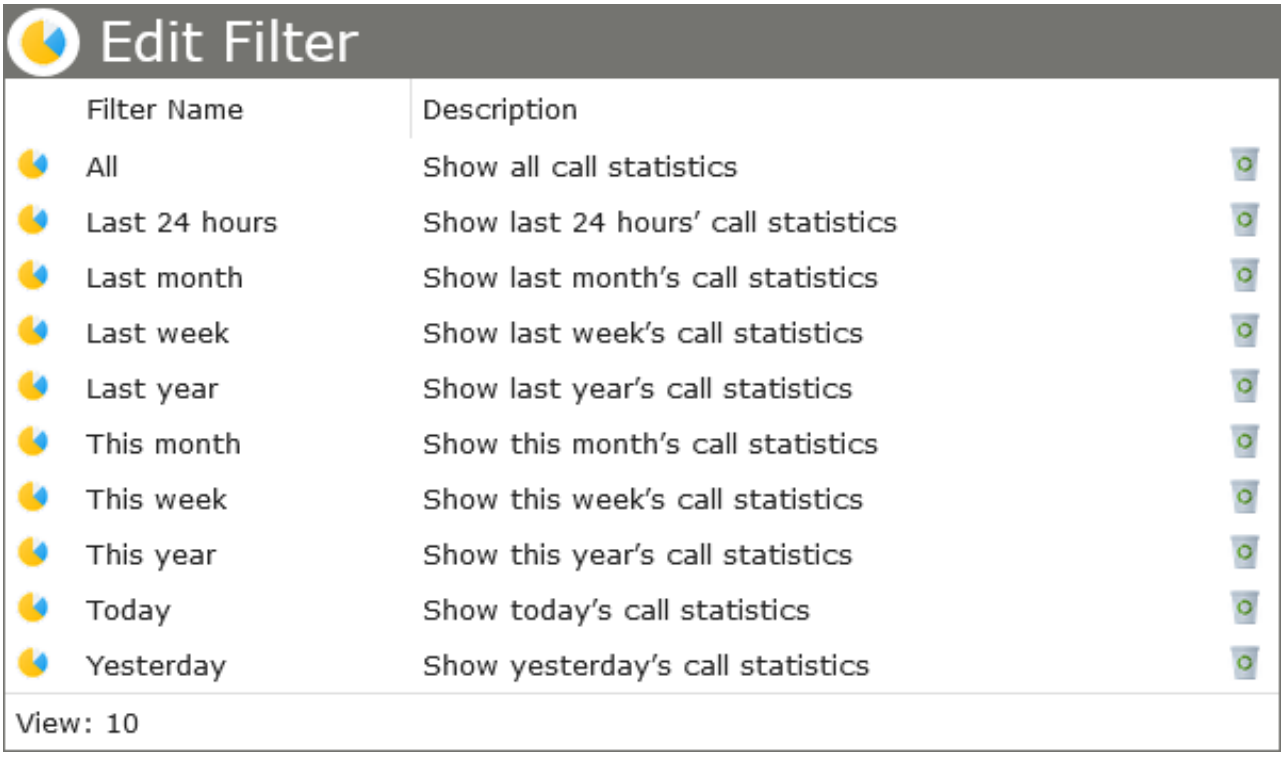
By clicking Add, the parameter will be added to the list. Only data entries that match *all* filter criteria will be included in the output (*AND relation*). Parameters can be deleted by clicking the *recycle* icon.





The settings can be tested by clicking the Test Filter button.

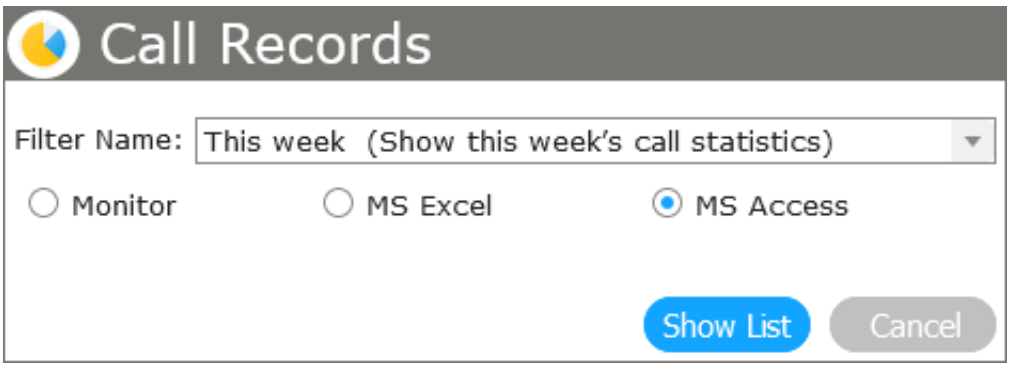
Clicking the button Save stores the new filter and makes it available to all authorized users.



Choosing Reports > Edit Filter lists all filters. Each can be changed by clicking on it, or deleted by clicking the *recycle* icon.

Call Reports

Clicking on Reports > Call Records shows the call detail records. Filters and output/export options (display records on screen, export as Microsoft Excel file, export as Microsoft Access file) can be selected here.



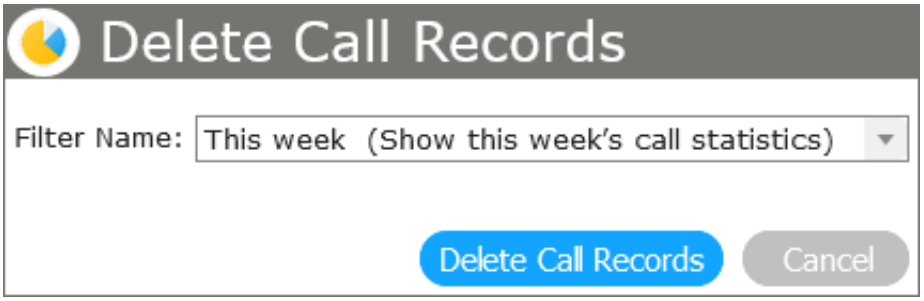
The following data will be listed:

- Date/Time
- Caller
- Called
- Duration
- Account code.

The account code is used on the Cisco IP Phone. More information can be found in the respective Cisco phone manual.

Exporting to Microsoft Access provides extensive call statistics, visualized as schedules and diagrams.

Delete Call Records deletes the call detail records that fit the selected filter.



Downloads

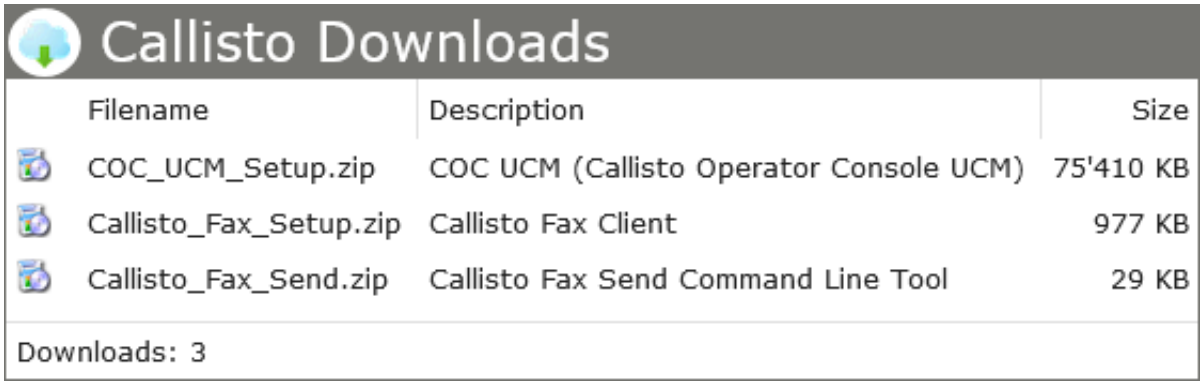
The Downloads menu provides access to all available Callisto downloads. Those can be installed on client PCs by administrators.

The download section has two categories: Callisto Downloads and User Downloads.

Callisto downloads are maintained by CTModule AG and are only available to the admin user. User downloads can be customized and are directly available to client users.

Log on to a client's PC using an administrator account, and choose Downloads > Callisto Downloads or Downloads > User Downloads respectively. Select the file you want to download by clicking on the file name. It will be stored locally or opened in the current folder. Edit and/or install the downloaded file following the setup instructions.

Callisto downloads

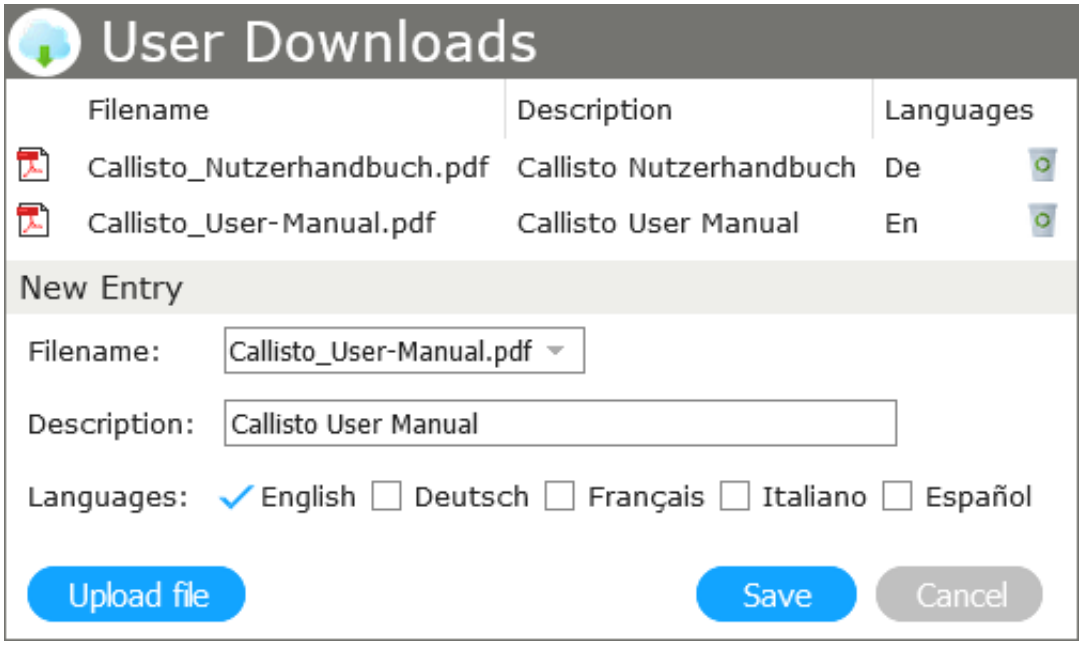


In the menu Downloads > Callisto Downloads, you'll find application installers, e.g. for the fax client or the Callisto Operator Console, depending on the edition of the Callisto Platform and what options are enabled.

The download links point to the most recent version of the software, provided via the CTModule FTP server (Internet connection required),

Callisto will provide further available downloads (e.g. updates and upgrades) in the Callisto Downloads menu.

User downloads



In the menu User Downloads, you can add your own downloads that will be available to the client via the web GUI.

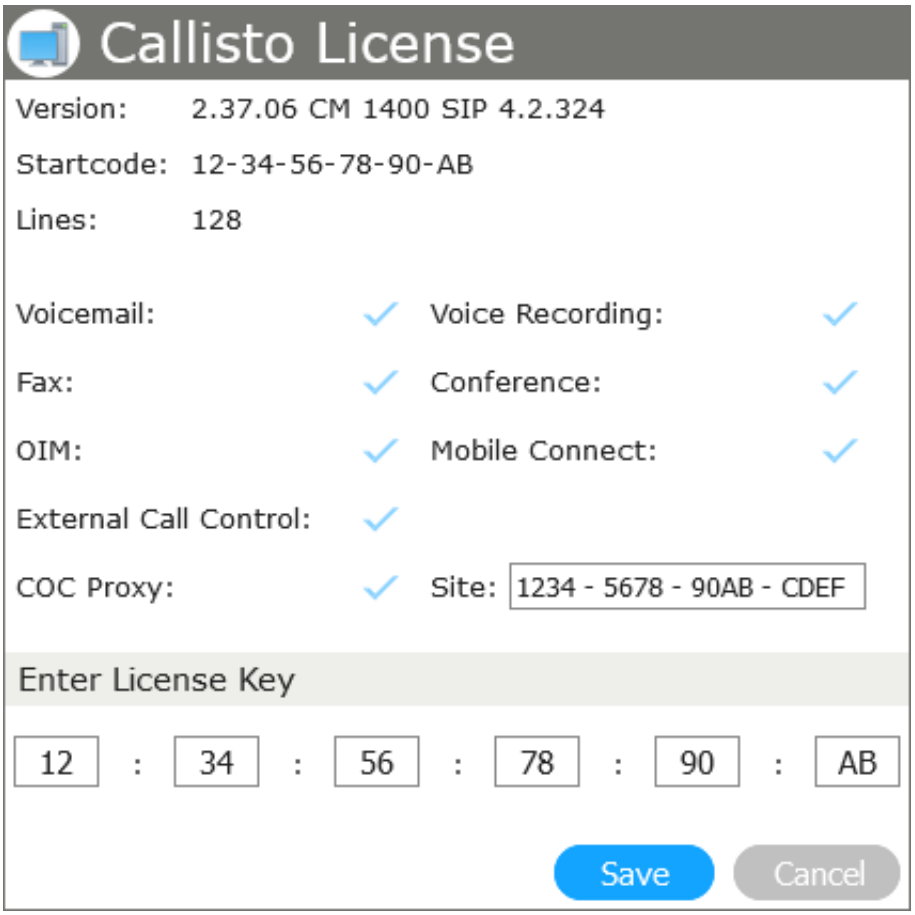
To upload a file, click on Upload File. After the upload is finished, select the file from the drop-down menu to set a Description and check the Languages the file is intended for. The file will only be visible to clients who set their web GUI in a language that you've enabled here.

Options

Installation

The basic version of the Callisto Platform includes four lines (*Callisto for UCM, HCS, Webex*) or two lines (*Callisto for UCME*), excluding any options. Callisto can be upgraded by using additional license keys. New license keys can be acquired via your Callisto vendor or by contacting support@ctmodule.com.

Once you obtained a new license key, enter it by choosing System > Callisto License.



Callisto Express only

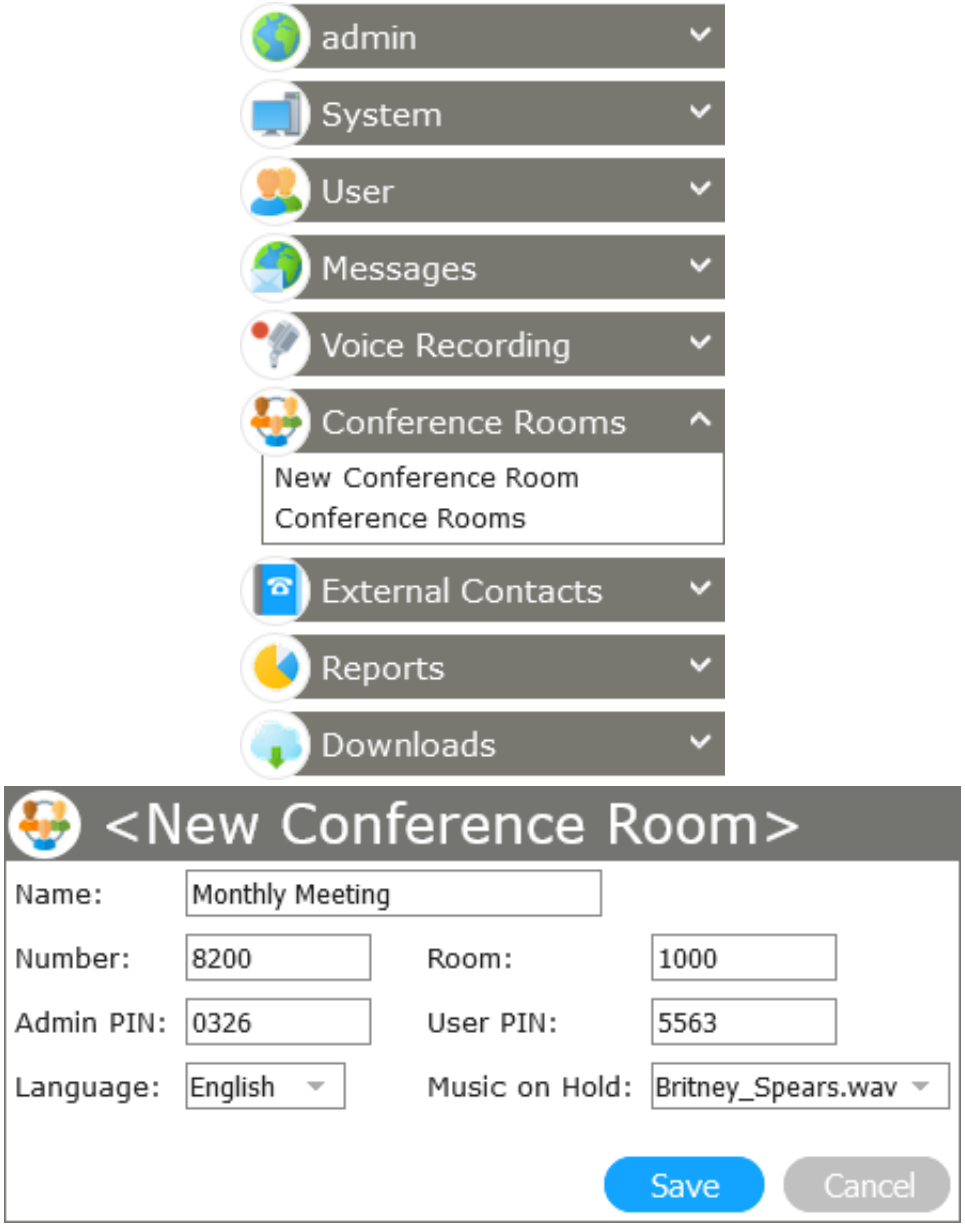
After activating the *COC Proxy Service* option,the configuration of COC Express needs to be updated: Instead of the Cisco UCME IP address, enter the IP address of the Callisto Platform.

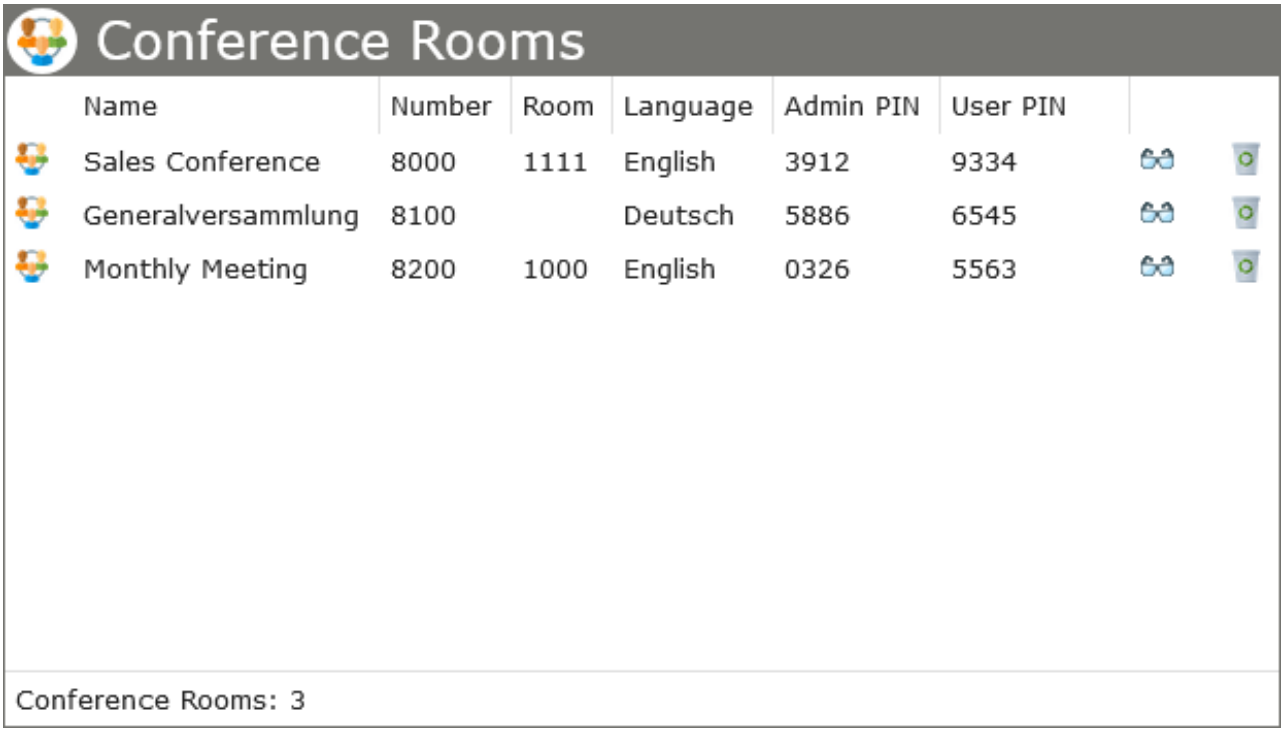
If you use a COC multi-user solution, the site license needs to be added to the Callisto configuration. This way, all installed workstations will be centrally activated through Callisto?eliminating the need for any additional or individual license registrations (see Option “COC Proxy Service”).

Option “Virtual Conference Room”

Callisto provides a Virtual Conference Room, enabling companies to quickly and easily create virtual meetings. On Callisto, the meeting place is referred to by a “room number”, which is allocated by an

administrator.





Choose System > Conference Rooms to set up and configure conference rooms. You can configure the following parameters:

- Phone number: the number to dial when accessing the conference room
- Room number (optional): Leave this field empty if you want to set up only one room for this number.
- Administration PIN (optional): A caller who logs in using this PIN will be able to invite further participants (see user manual) and can control the conference by using LiveView from a browser.
- User PIN
- Language
- Music on hold

You can delete conference room assignments by clicking the *recycle* icon.

The maximum amount of simultaneous conference participants is determined by the total number of available and licensed Callisto lines.

For Callisto UCM

Configure a new route pattern on the Cisco Unified Communications Manager which includes the new conference room number. For details, refer to the Cisco UCM configuration manual.

For Callisto Express

The settings will automatically be stored on the IOS router.

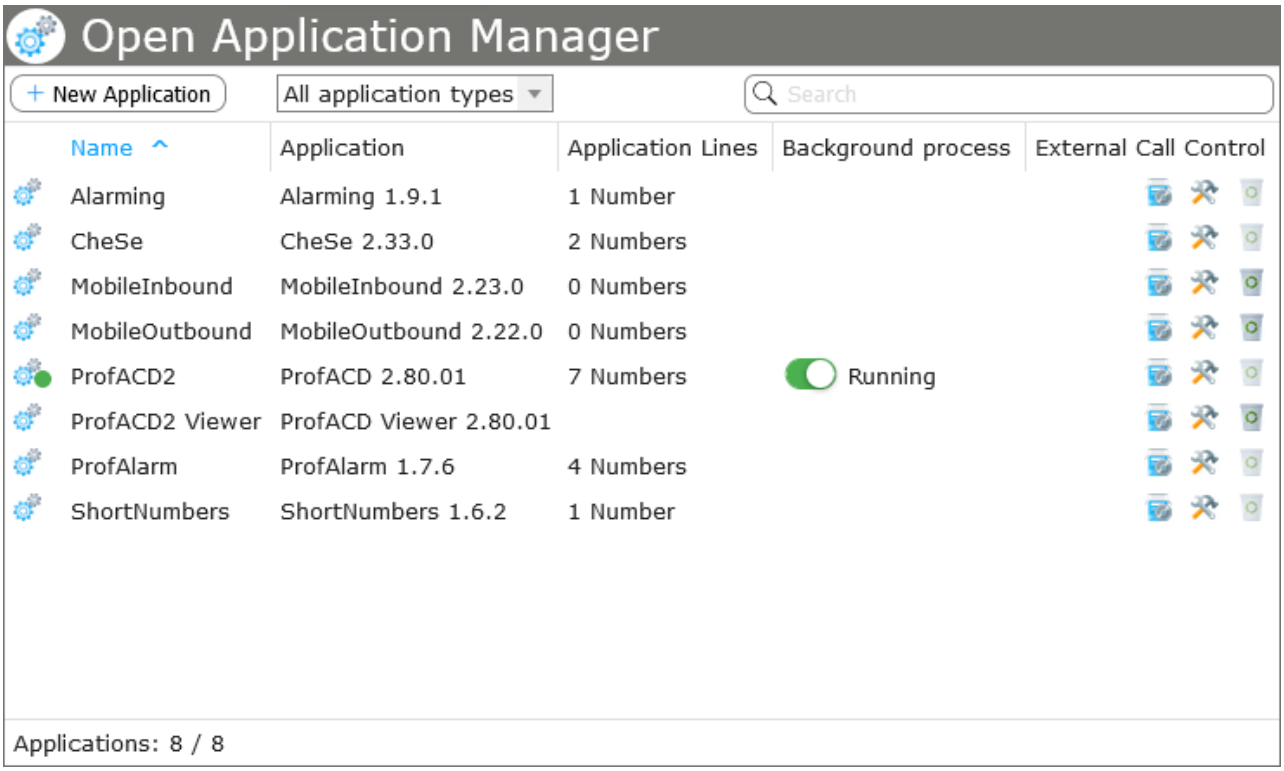
Option “Open Application Manager”

With Callisto's Open Application Manager, administrators are able to define inbound numbers for Callisto applications such as Interactive Voice Response (IVR), Automatic Call Distribution (ACD), Auto-Attendant, etc. A structured file administration of custom applications is accessible by the web GUI.

Inbound applications can be created with the development environment CTMaker and tested using the integrated simulator and debugging tools.

After creating an application, open a text file, copy the application code into it, and save this file with the extension *.cts*.

Go to System > Open Application Manager and enter a name for the new application in the New Application field.



Update

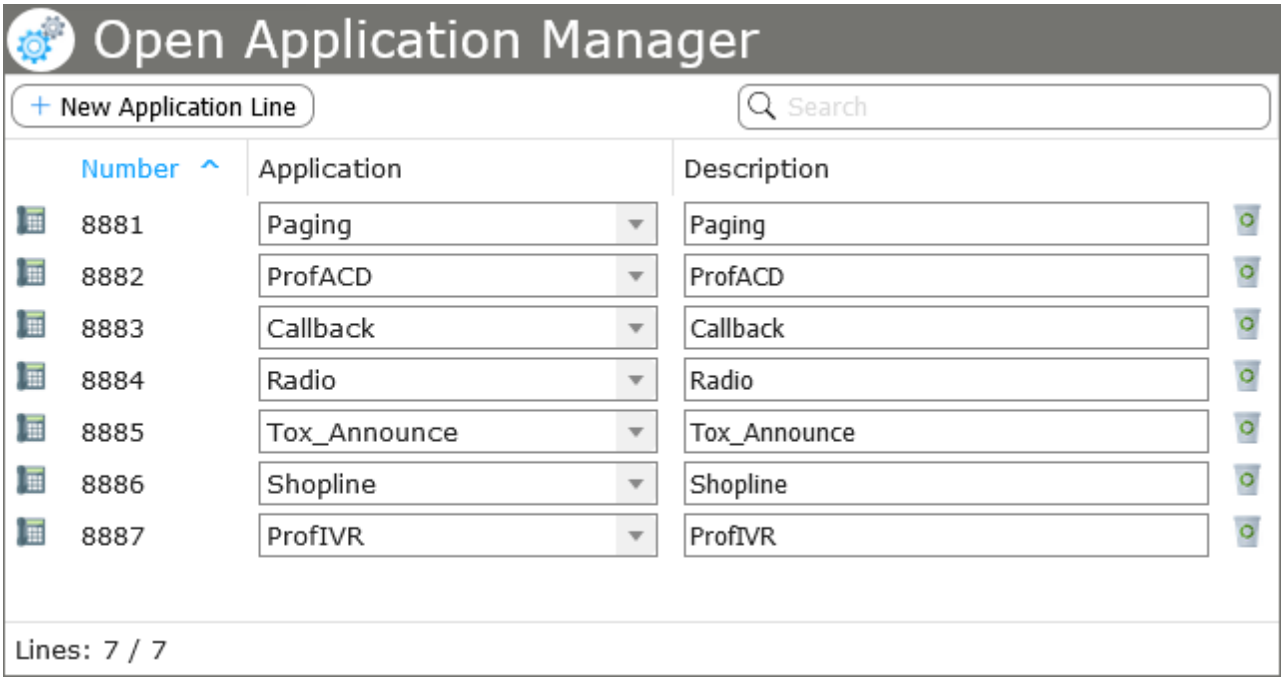
Configure

Delete record

Use the *update* icon to install or update your application. The *configure* icon opens the configuration, if the application has a frontend.

For Callisto UCM, HCS, Webex

Configure a new route pattern on the Cisco Unified Communications Manager which includes the new OAM number. For details, refer to the Cisco UCM configuration manual.



Choose System > Open Application Manager, then click on the tab Application Lines. Enter the OAM number and assign the new application from the drop-down list. Optionally, you can also add a description.

For Callisto Express

Your selection will automatically be stored on the IOS router.

The maximum amount of simultaneous inbound calls are determined by the total number of available and licensed Callisto lines.

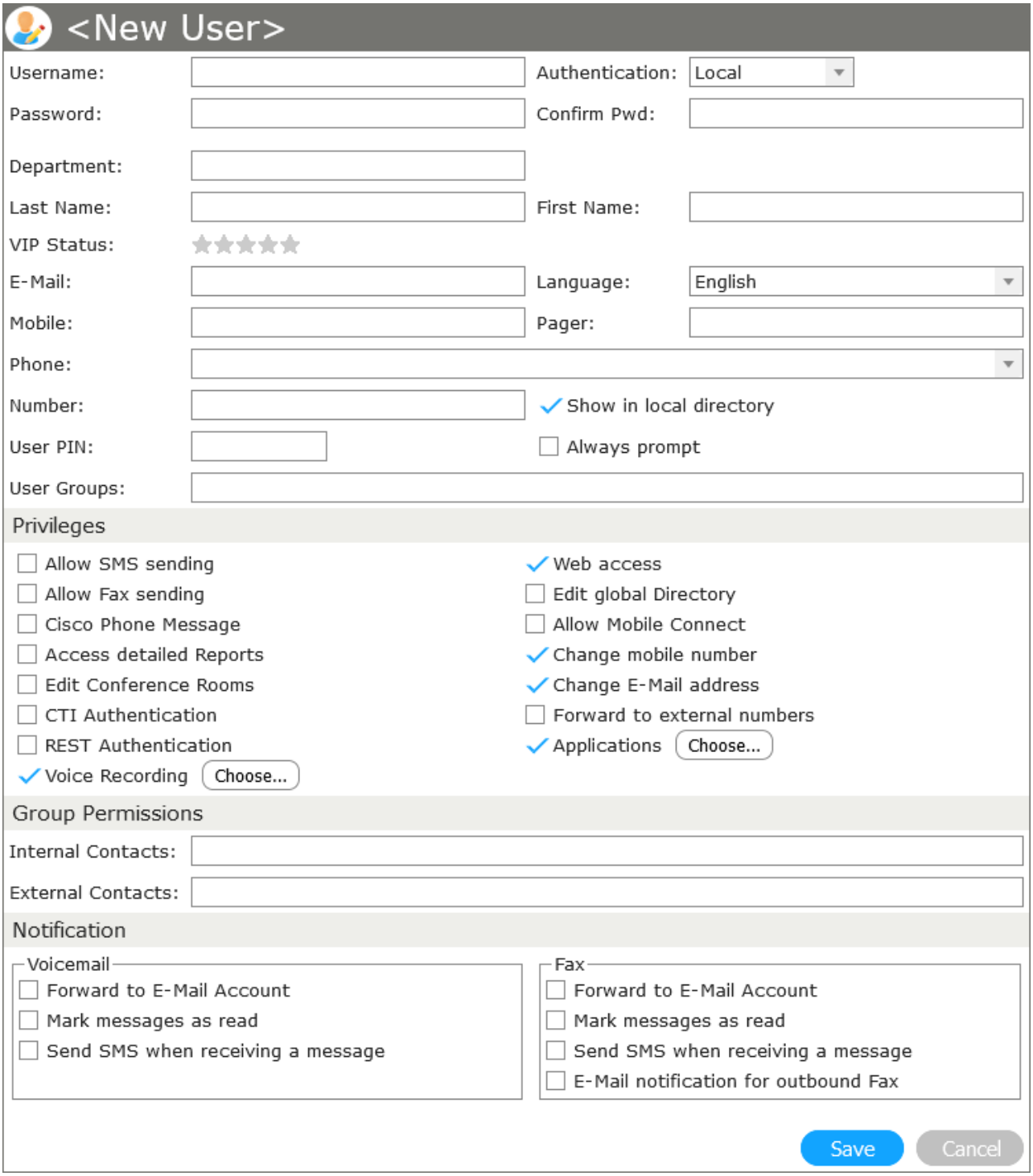
Option “Mobile Connect”

The option *Mobile Connect* is used to connect mobile phones or external landline connections to your company’s communication infrastructure. With this option, calls can be made between external phones and company phones using only internal phone numbers. A detailed description can be found in the user manual .

The option Mobile Connect needs up to 3 lines according to the switching status and/or the chosen function. Please ensure that Callisto has a sufficient number of lines available.

By choosing User > New User, permissions regarding *Mobile Connect* for each user can be configured.

After enabling Allow Mobile Connect, users are able to forward calls to *Mobile Connect* and external phone numbers in the user settings (please refer to the user manual).



Option “COC Proxy Service”

On Callisto for UCME

By default, Cisco Unified Communications Manager Express allows a phone to be used only by one single client software application (e.g. COC Express). Using the option *COC Proxy Service* enables the Operator Console COC Express to be used as a multi-user solution. Additionally, COC Express and other TAPI client software can be installed side-by-side on a client PC, for example, Microsoft Outlook Phone Dialer (Cisco TAPI Service light).

There are three cases:

1. Option COC Proxy Service switched off: COC Express can be used as single-user version (COC

Express itself being licensed) without any additional client software (such as Cisco TAPI Service light).
2. Option COC Proxy Service switched on: COC Express can be used as single- and multi-user version (COC Express itself being licensed) with additional client software such as Microsoft Outlook Phone Dialer (Cisco TAPI Service light).
3. Option COC Proxy Service switched on, Site License active: COC Express can be used as multi-user version (no licensing in COC Express necessary, the licensing is done centrally in Callisto for UCME), in conjunction with additional client software such as Microsoft Outlook Phone Dialer (Cisco TAPI Service light).

On Callisto for UCM, HCS, Webex

The COC Proxy Service will provide the connection needed by the Cisco Unified Communications Manager to enable COC clients. Please refer to the Callisto COC UCM manual.

1. To enable the COC Proxy, add the Site License for the COC Proxy Service. All installed work stations will be centrally activated through Callisto, so no further individual license registrations will be necessary.

2. After activating the COC Proxy Service option, the COC Express configuration needs to be updated with the Callisto Express IP address in place of the previously configured Cisco Unified Communications Manager IP address. If a site license has already been added to the optional COC Proxy Service, no further licenses are necessary on the COC Express client.
3. For COC UCM Client connection please refer to the Callisto COC UCM manual.

Option “Voice Recording”

See the VoiceRecording administration manual.

Option “External Call Control”

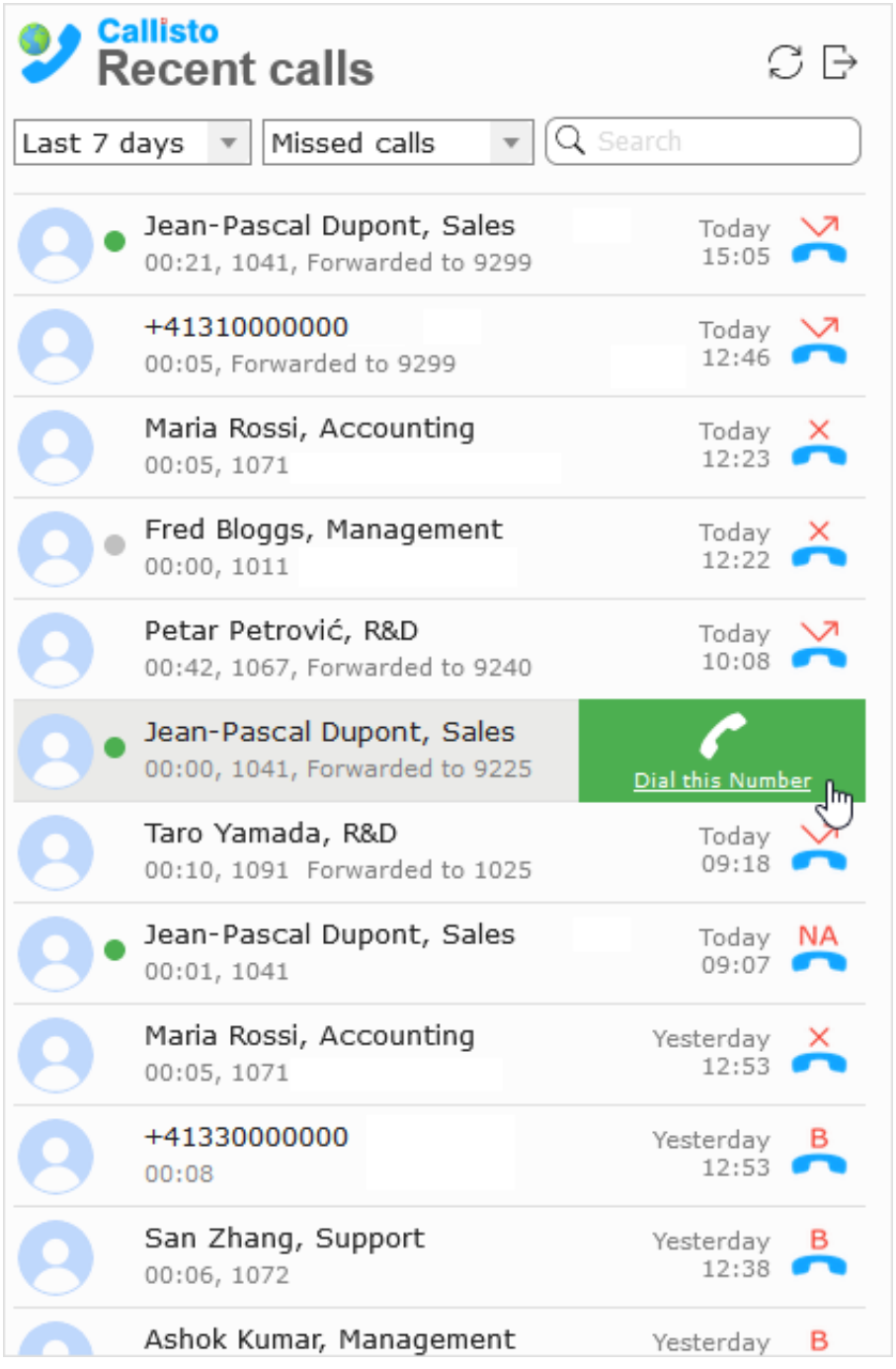
See the External Call Control administration manual.

Callisto Gadgets overiew

By default, the URLs are in a format similar to http://<*callisto*>/LogonPage.asp, where <*callisto*> is the address of your Callisto installation. To access the Gadgets, you can also use any of the methods described in the chapter Integration of Callisto Gadgets.

Recent calls

The URL of this gadget is: http://<*callisto*>/Jabber/RecentCalls/RecentCalls.asp

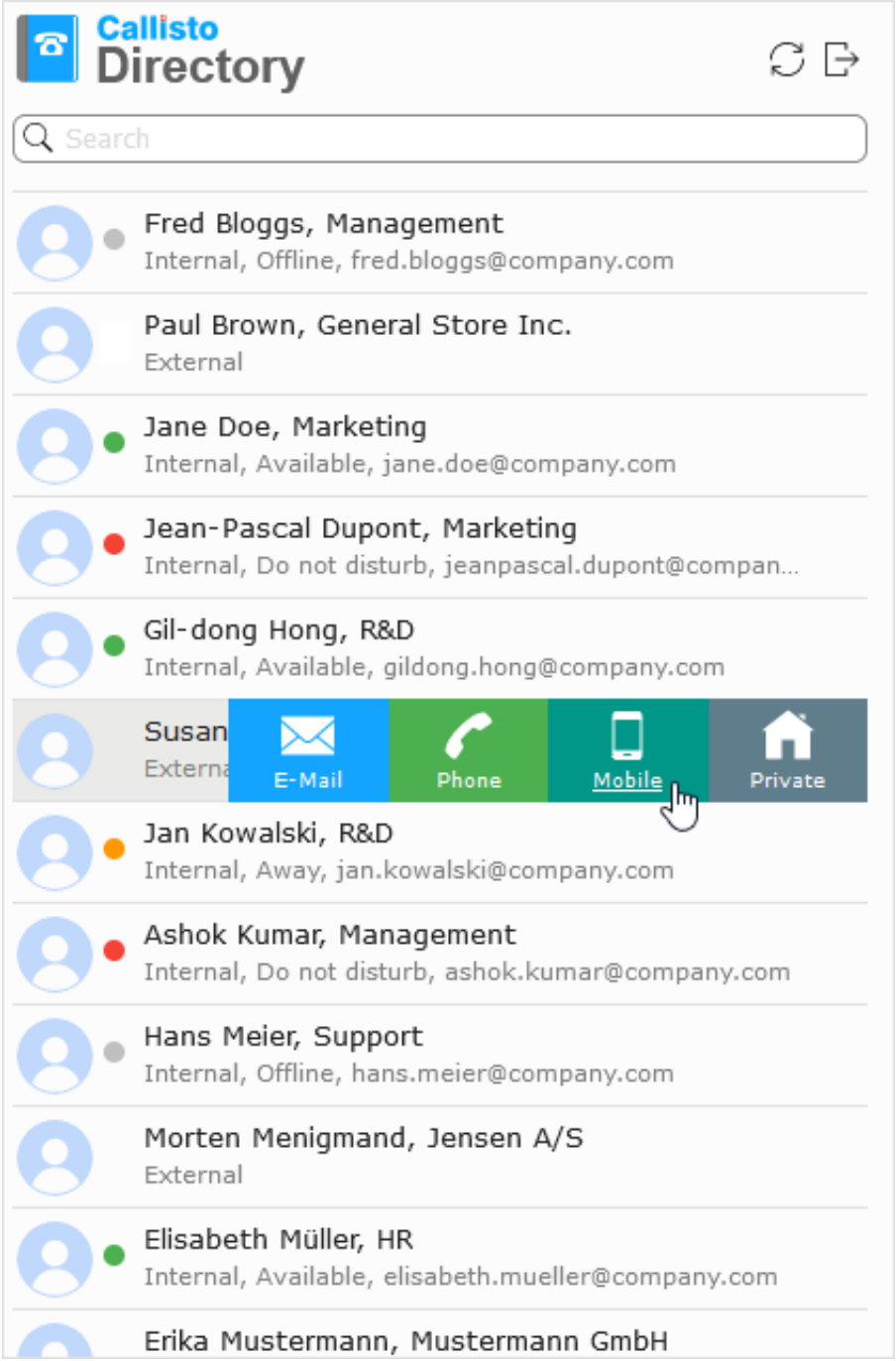


Recent calls shows the following call types:

	Connected outbound call
	Outbound call; destination not reached
	Connected inbound call
	Missed inbound call
	Missed inbound call; phone was busy
	Missed inbound call; call was diverted
	Missed inbound call; phone was offline

Directory

The URL of this gadget is: http://<*callisto*>/Jabber/Directory/Directory.asp

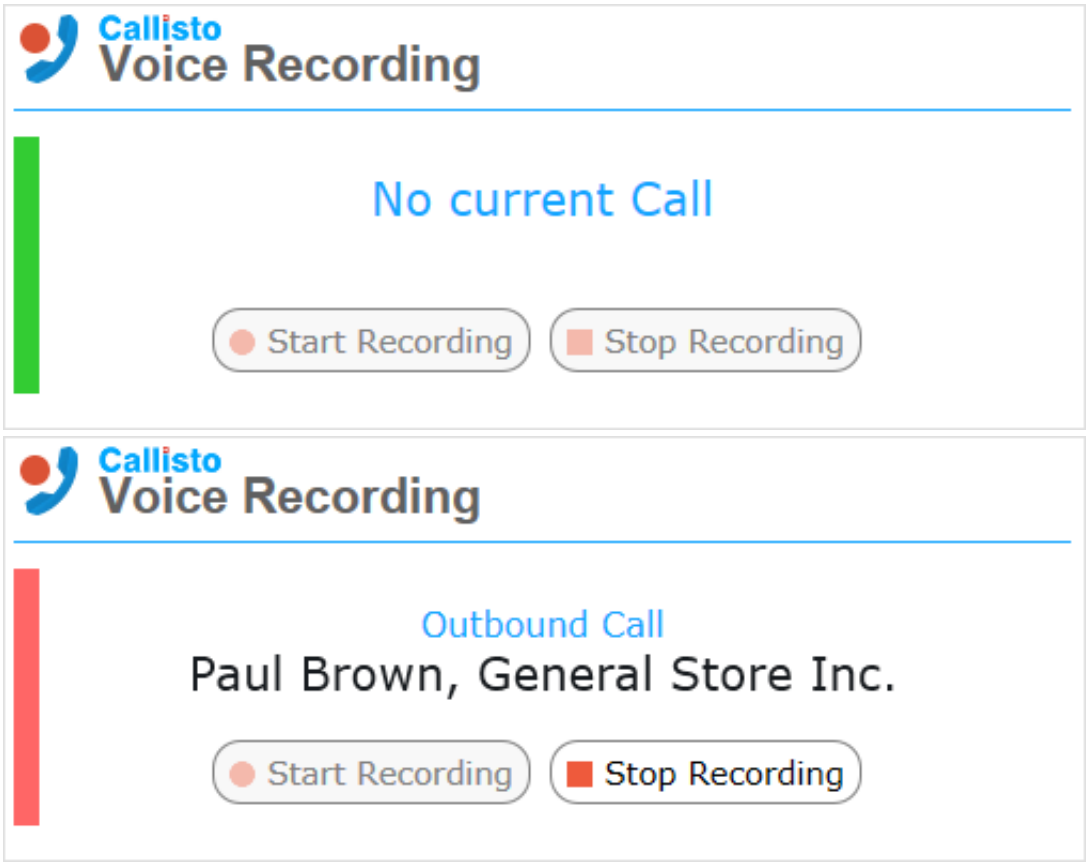


The search function will show results from both internal and external contacts saved in your Callisto directory. For more details on available search operators, refer to the quick reference.

Clicking on an entry from the search result list will reveal all available shortcuts for messaging or calling the contact.

Voice Recording

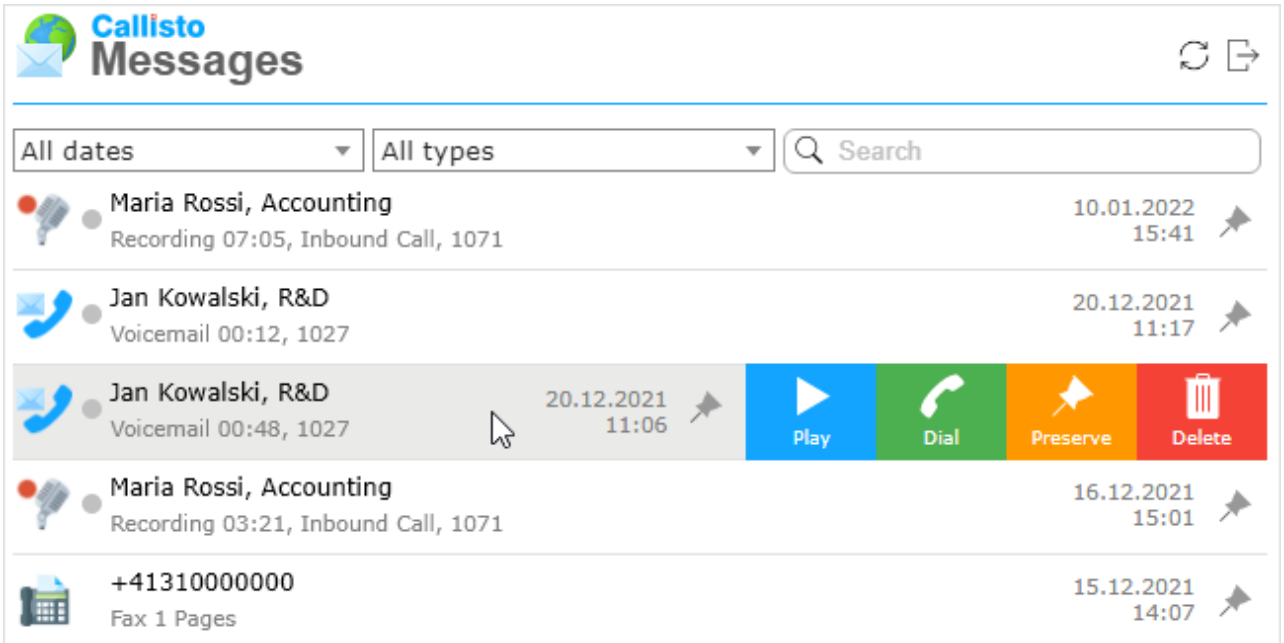
The URL of this gadget is: http://<*callisto*>/Jabber/Recording/Recording.asp



This gadget enables you to start and stop manual recordings. To use it, the option Voice Recording needs to be set up and activated.

Messages

The URL of this gadget is: http://<*callisto*>/Jabber/Messages/Messages.asp



Depending on the license and privileges of the logged-in user, this gadget shows voice mails, faxes and voice recordings.

In the upper part, you can reload the page, define display filters and search directly for specific people or

phone numbers. If you move the cursor over an entry, the available actions are displayed. Depending on the entry, these are:

- Play the recording
- Dial the caller’s number
- Open the fax message
- Toggle preserve message
- Delete the message

Depending on the configuration, opening a fax message will open the PDF file directly, show it in the lower part of the UI as an icon, or a dialog box appears asking whether the document should be opened or saved.

When clicking on a voice mail or voice recording,an audio control panel will appear, allowing playback and volume control. Clicking on Download will allow you to save an audio file of the recording to your hard drive. Clicking on Close audio player or clicking somewhere outside the list entry will abort playback.

Integration of Callisto Gadgets

Some Callisto features (Gadgets) can be integrated in various platforms and using different authentication methods.

Standalone page

To add a standalone page in Windows, open the respective URL in Edge and then choose Apps > Install this site as an app. You can then create a desktop shortcut using the option Apps > Manage apps.

Authentication with URL query strings

You can create a URL that includes login credentials. In the following example, the user with the name *username* is logged in and redirected to the *SmallAgentDesk* page.

```
http://<callisto>
/LogonPage.asp?page=/Applications/inbound/ProfACD2/src/SmallAgentDesk.asp&user=
username&pwd=password
```

<*callisto*> is the root path of your Callisto installation. The three query strings are:

- page: The page to which user will be redirected after authentication.
- user: The username which is used to login to Callisto.
- pwd: The respective user password.

Login using the default Callisto authentication HTML form

To use the default authentication form, use the following URL, where <*callisto*> is the root path of your Callisto installation:

```
http://<callisto>/Jabber/Messages/Messages.asp
```

After entering valid credentials, the user gets redirected to the page. If you use this authentication method, checking the option Remember last used credentials in the user settings dialog is recommended.

Login using SSO (Single Sign-On)

To use single sign-on authentication, use the following URL ,where <*callisto*> is the root path of your Callisto installation:

```
http://<callisto>/LgonPageSSO.asp?page=/Jabber/Messages/Messages.asp
```

This will authenticate the user with the defined Single Sign-On provider.

Integration with COC

COC provides *HtmlPanes* that can be used to integrate Callisto Gadgets. For details on configuring HtmlPanes, refer to the COC configurator manual.

All the authentication methods described in the section Standalone page can be also used in COC integration, but the recommended method is authentication with URL query strings. When using this method, the URL should be modified in the following way, where <*callisto*> is the root path of your Callisto installation:

```
http://<callisto>
/LogonPage.asp?page=/Applications/inbound/ProfACD2/src/SmallAgentDesk.asp&user=
%user%&pwd=%pwd%
```

COC will automatically replace the %user% and %pwd% placeholders with the credentials of the currently logged in user.

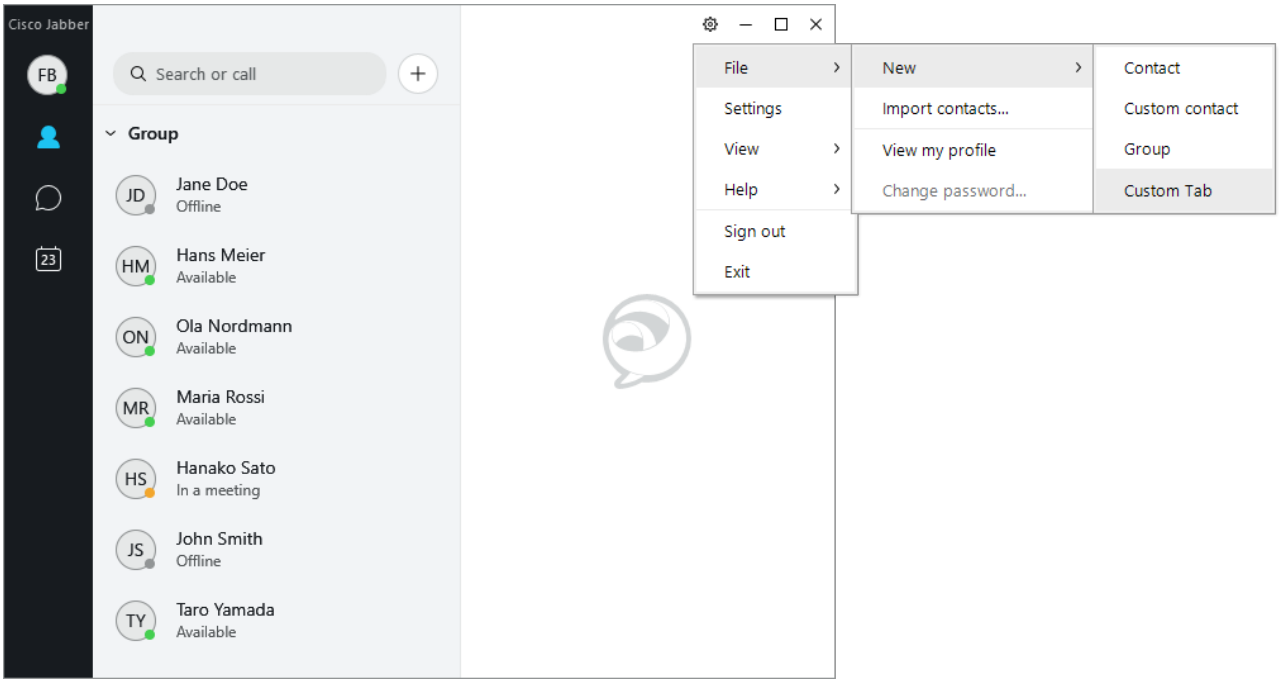
If you use one of the other two authenentication methods, the URLs to be used are identical to the ones described in the section Standalone page.

Integration with Cisco Jabber client

To integrate Callisto in Jabber, a custom tab needs to be created. A custom tab can be created in two ways:

Integration using Cisco Jabber GUI

In Jabber, click the menu icon and choose File > New > Custom Tab.



The window Create new custom tab will open. Enter the name of the tab, and the URL of the respective Jabber tab (see below). After entering the link, click Create and the custom tab will appear in the tab bar on the left.

Integration by uploading a configuration file

A more reliable way to deploy custom tabs is by adding or editing a Jabber configuration file.

Here is an example of a Jabber configuration file:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
 <Client>
  <jabber-plugin-config>
   <browser-plugin>
    <page refresh="false" preload="true">
     <tooltip>Recent Calls</tooltip>
     <icon>http://<callisto>/Jabber/RecentCalls/JabberIcon.png</icon>
     <url>http://<callisto>/Jabber/RecentCalls/RecentCalls.asp</url>
    </page>
    <page refresh="false" preload="true">
     <tooltip>Recording</tooltip>
     <icon>http://<callisto>/Jabber/Recording/JabberIcon.png</icon>
     <url>http://<callisto>/Jabber/Recording/Recording.asp</url>
    </page>
    <page refresh="false" preload="true">
     <tooltip>Messages</tooltip>
     <icon>http://<callisto>/Jabber/Messages/JabberIcon.png</icon>
     <url>http://<callisto>/Jabber/Messages/Messages.asp</url>
    </page>
   </browser-plugin>
  </jabber-plugin-config>
 </Client>
 <Options>
  <ShowTabLabel>true</ShowTabLabel>
 </Options>
 <Policies>
```

```
  <EnableSIPURIDialing>true</EnableSIPURIDialing>
 </Policies>
</config>
```

Replace <*callisto*> in the URLs with the domain name or IP address of your Callisto installation. Save the file using UTF-8 encoding, name it Jabber-config.xml and upload it it to the CUCM TFTP server. Once the file is uploaded, you will have to restart the TFT server.

After the next login, the respective Jabber users will find the defined tabs in the Jabber navigation bar.

More information about setting up custom tabs in Cisco Jabber is available on the official Cisco website:

- On-Premises Deployment for Cisco Jabber 11.5 – Create and Host Client Configuration Files
- Feature Configuration for Cisco Jabber 12.7 – Custom Embedded Tabs

Smartphone integration

All available Gadgets can also be used as so-called *WebApps* on iOS and Android devices. The URLs described can be adopted unchanged.

iOS

Open the corresponding URL in Safari and click on the *share* icon. Select Add to Home Screen. The icon of the WebApp appears and you can complete the process with Add.

Android

Open the corresponding URL in Chrome and click on the top-right menu icon. Select Add to Home screen and click Add. Finish the process by dragging the icon to a place of your choice on the home screen, or by clicking Add automatically.

Maintenance and service

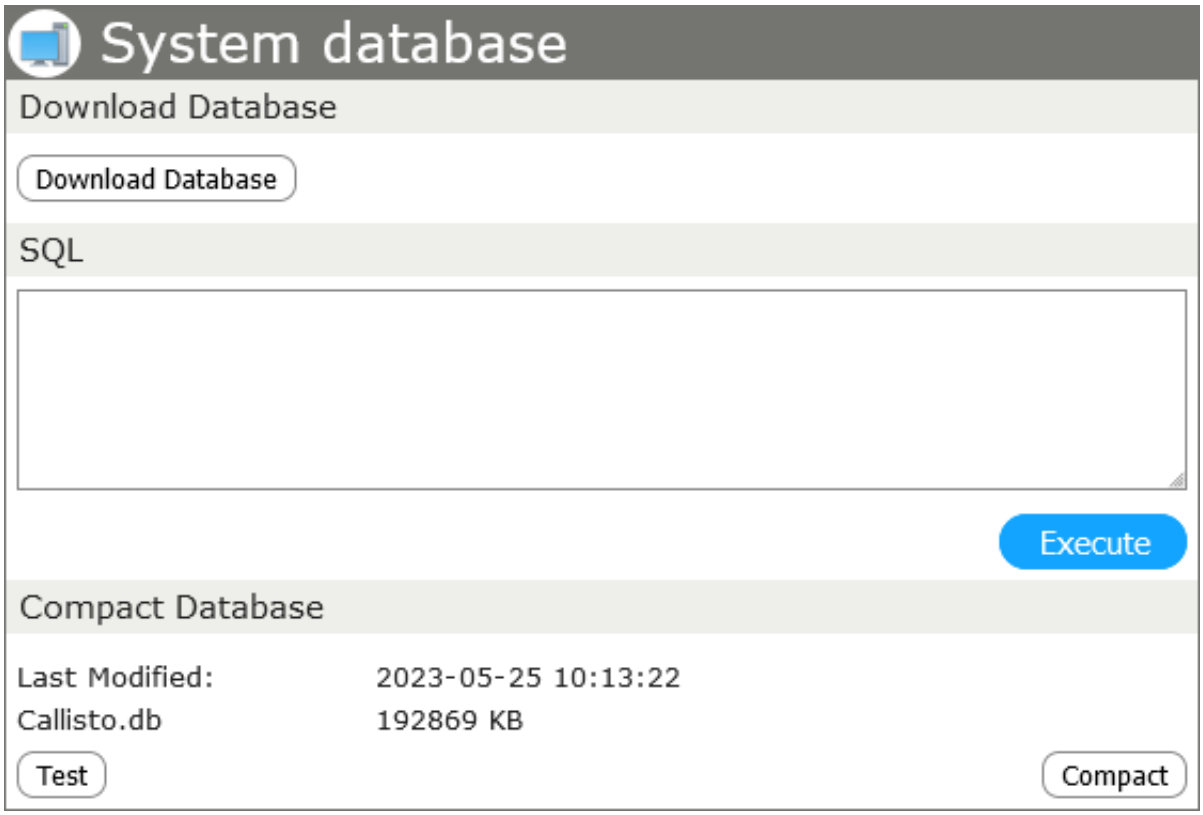
The Callisto concept ensures a maintenance-free system for years. In the unlikely event of a system failure, CTModule differentiates between services within a defined warranty period and those outside a defined warranty period.

The warranty duration is defined in the relevant GTC document, valid at date of purchase. After warranty expiration, CTModule endeavors to facilitate replacements quickly and efficiently in order to keep down-time to a minimum.

Backup and restore

It is highly recommended to backup system parameters and user settings periodically, especially immediately before and after large changes. Additionally, the system database should be cleaned up from time to time by choosing System > Backup and clicking the Compact button.

After a system update, it is essential to generate a new backup. Earlier backups may not be compatible any longer.



- To clean the current Callisto database, click the Compact button. The database will be cleaned and the new file size will be displayed.
- To back up all Callisto data (including voice mails, fax mails, personal greetings etc.), click the Backup tab. You can set a password for the backup file or leave the password field empty. Click the Backup button; after the backup process is finished, a ZIP file containing all Callisto configurations and settings will be downloaded to your hard drive.
  A backup can also be done to an (S)FTP server using the startup script Backup Scheduler.

- In the tab Restore, you can restore the Callisto installation from a backup file. Select HTTP Upload to upload a file from your hard drive or use FTP Server / SFTP Server if your backup file is saved on a respective server.

Updates and upgrades

Occasionally, CTModule provides Callisto updates and upgrades. Updates contain bug fixes, minor improvements, or minor functional extensions of the Callisto software and are provided free of charge. Upgrades are new Callisto software packages, providing a substantially extended set of features and are are available for purchase.

1. Read any notes or information provided alongside the downloaded files. Upload and install the updates/upgrades by choosing on System > Update System and upload the installation files to the Callisto system. Normally, a system restart is not required.
2. After the upload is finished, the file appears under the section Install. Check the data and install the software by clicking Install. You can delete the uploaded software from the list by clicking the *recycle* icon.

After a system update, it is essential to generate a new backup. Earlier backups may not be compatible any longer.

Bug reporting

Before you report a bug, please check the following:

- The hardware on which Callisto is installed is set up and working properly.
- The system on which Callisto is installed is properly connected to the network.
- Entering http://callisto/ or the root address of the Callisto installation on a client PC's browser will shows the Callisto login window.
- The Cisco Unified Communications Manager is configured correctly according to the Cisco UCM configuration manual.
- The communication between the Cisco Unified Communications Manager and Callisto is working.

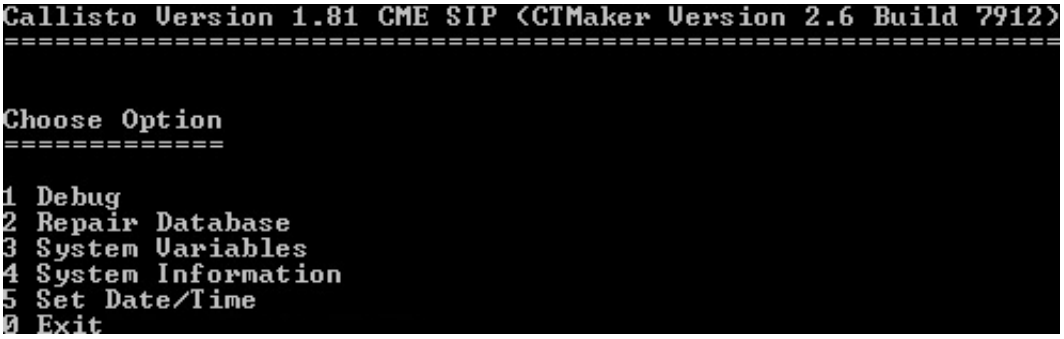
If you experience any problems, contact your Callisto dealer or follow the instructions according to the Callisto GTC and/or SLA. In case of software and/or configuration problems, you might be requested to activate trace logging, which is described in detail in the following section.

Telnet access

Telnet access is an alternative way of configuring some functions in the Callisto system and/or providing extended configuration sets, which are not accessible via the web GUI. Additionally, tracing can be enabled, which may be helpful during analysis of software/configuration problems.

By default, Telnet access is provided by port 23 of the appliance. Consult with your system administrator on how to establish a Telnet connection.

Via Telnet, use your administrator credentials to log on. You can select between the following options:



Debug

If you select this option, your Telnet client displays all running processes Callisto is currently executing. This trace information will be saved to a log file and may be used to analyze software/configuration problems. Try to keep the trace records as brief as possible so that they only contain actions relevant to the issue.

Repair Database

Starts the database maintenance routine. The web server will be stopped temporarily during this process.

System Variables

Enables modifying configurations which are not accessible by web. The following system variables may be displayed and/or changed:

Variable	Description	Values
gBridgeTransfer	Calls are transferred with the CUCM(E) or bridged if CUCM(E) doesn't support transfer.	• 0 (default): Use PBX transfer. • 1: Transfer will not be used and the call is bridged through Callisto.
gCocProxyMemory	Heap-memory available for the COC proxy.	<*integer*>: Memory in megabytes
gCocProxyRestart	Enables periodic restarts of the COC proxy.	<*DayBitmask*>,<*Time*> • <*DayBitmask*>: Integer, see day bit masks. • <*Time*>: Time of day, in 24h format.
gDefaultMailbox	Forwarded voice messages, which are not assigned to any user, will be routed to this box	• <*blank*> (default): No default mailbox. • <*integer*>: Internal user number to be used as box number.
gDisablePersHistory	Deactivates the Web menu Reporting for users without access rights to detailed reports. Thus, these users also have no access to the logs of their own phone extension.	• 0 (default): Personal reporting on. • 1: Personal reporting off.
gInboxNotifyRefresh	Defines the time interval after which the display of the number of new messages should be refreshed.	<*integer*>: Interval in seconds (default: 60).
gMCSpeakNumber	For MobileConnect: speaks out the number of the caller.	• 1 (default): Number is spoken. • 0:

Variable	Description	Values
		Number is not spoken.
gMwiWebControls	Shows in the voice mail settings the MWI controls (MWI lamp on/off) in the Web interface.	• 0 (default): Controls hidden. • 1: Controls shown.
gMaxForwardNumberLen	Maximum length of a diverted number. This way, you can limit diversion, e.g. only to internal users.	*<integer>* equal to or smaller than 100: Number length (default: 100).
gPhoneLoginWithNumber	Switches on and off prompting for a box number when logging in with by phone. Turning on prompting gives you the possibility to log in to other boxes.	• 0 (default): Automatic dialing of the box number. • 1: Box number will be prompted.
gPhonePrivateDirPIN	If PIN always prompt is set and gPhonePrivateDirPIN has the value 1, the Private Directory for the Cisco phone will protected by a PIN code.	• 0 (default): No PIN code requested. • 1: PIN code requested.
gRecordVolume	Volume for audio recordings.	*<integer>*: Audio volume, in percent of the system value (default: 400).
gStripCallerID	Set a number of digits that will be stripped from the beginning of the CallerID. This way, you can omit unnecessary leading zeroes.	*<integer>* (default: 0)
gSyncLineName	Automatically set the line name of the phone with the actual user name (Callisto Express only)	• 0 (default): Off. • 1: On.
gTimeServer	Used time server.	*string* (default: time.windows.com)
gTransferWithCallerID	Outgoing calls are signalled with the caller number.	• 0 (default on UCME): Voice mail number will be used. • 1 (default on UCM, One): Caller number will be used.
gWebServerRestart	Enables daily restarts of the web server.	*<DayBitmask>*,*<Time>* • *<DayBitmask>*: Integer, see day bit masks. • *<Time>*: time of day, in 24h format.
gWebTimeout	Timeout period after which an inactive web user automatically is logged out by the Callisto system.	*<integer>*: Minutes to wait until logout (default: 20). Set to 0 to deactivate automatic logout.

Day bit masks

A day bit mask is an integer between 0 and 127 which, when converted into binary, will show a string where every day of the week is represented by a single bit. Whether a bit is set to 1 or 0 will mark the corresponding day of the week active or inactive, respectively.

The decimal value of the day bit mask is therefore the sum of all the active days, with each day having the following values:

- Sunday: 1
- Monday: 2
- Tuesday: 4
- Wednesday: 8
- Thursday: 16
- Friday: 32
- Saturday: 64

You want the web server to restart every Sunday and Wednesday. In a bit string, set the bits representing Sunday and Wednesday to 1 and every other day to 0:

Sat

0

The number 0001001 is written as 9 in decimal. Therefore, setting the value of gWebServerRestart to 9,02:00 will restart the web server every Sunday and Wednesday at 02:00 am.

System Information

Provides an overview of the most important system information.

Set Date/Time

Offers the possibility to set the Callisto Date and Time.

PLATFORM

USER MANUAL

Quick start

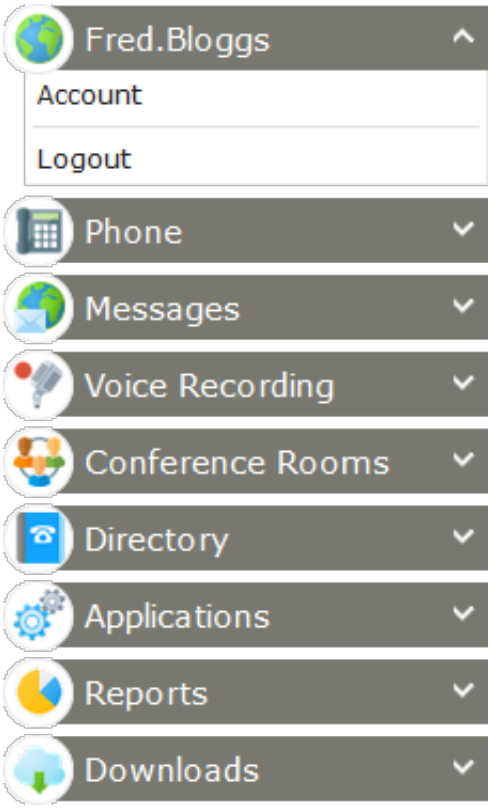
Open your web browser and navigate either to http://calllisto or an URL specified by your administrator.

Type your username and password provided by your administrator and click Logon. Note that both are case-sensitive. If your credentials don’t work or if you forget your credentials, contact your Callisto administrator.

For security purposes, it is highly recommended to change your password after logging in for the first time: from the main menu, click your user name (the topmost element), then select Account. Enter a new password in the Password and Confirm Password fields. In the same menu, you can also set your preferred Language and verify if all the user data provided by your adiminstrator is correct. To apply any changes you made, click the Save button.

In case you forget your logon details, contact your Callisto administrator for assistance.

User menu



In the Callisto web interface, the main menu's topmost menu item is the user menu. It is labeled with your user name.

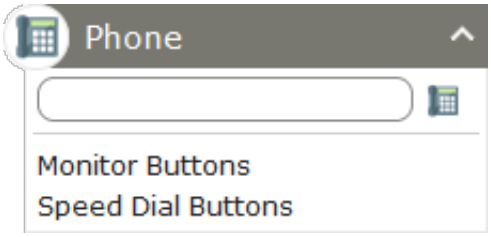
Account

Here, you can manage user-specific settings and preferences such as password, email address, phone number and the UI language. Clicking Save will apply your changes, clicking Cancel will discard them.

Logout

Click this item to quit the Callisto session. You can also log out by clicking the logout link located in the top-right corner of the Callisto interface. For security reasons it is recommended to always log out manually from Callisto.

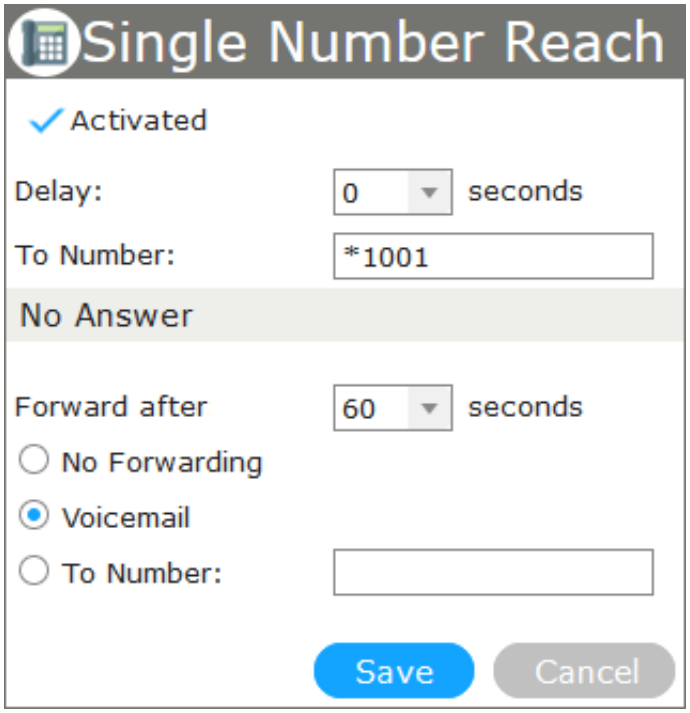
Phone menu



The first item in the Phone menu is an input field for your phone. From here, you can dial any phone number directly (for example, a number copied from a website).

Single number reach

This feature is only available with Callisto Express.



When your main phone is ringing, Single Number Reach allows for a secondary phone to ring at the same time. The same call can be picked up from either phone, and both phones stop ringing once the call is picked up.

With the Delay option, you can set how many seconds the main phone should keep ringing before the before the secondary phone starts ringing. To Number sets the number of the secondary phone. In addition, a forwarding option can be set in case the call remains unanswered. Forward after defines the time after which the call will be forwarded. No Forwarding deactivates forwarding, Voice Mail redirects the call to the voice mail number, and To Number sets another phone number to which the call will be redirected.

Select the Activated check box to quickly enable/disable this feature.

Monitor buttons

This view lists the phone’s buttons which can be used for monitoring. The buttons already in use are shown as unavailable, any other buttons can be edited. Click the Save button to apply the changes you made.

Speed dial buttons

This view lists the phone’s buttons which are available for speed dialing. Click the Save button to apply the changes you made.

Message settings

The first item in the Messages menu are the settings regarding voice mails, Fax messages, and SMS messages.

Security

To access voice mail from any phone, setting a User PIN is required. This PIN may consist of an arbitrary number of digits. After dialing in, type your phone extension and then authenticate by typing your PIN.

Selecting Always prompt will promt the PIN any time you access voice mail, also when using your internal Cisco IP phone.

Forward

Set the phone's forwarding actions. These settings can be configured individually for the call diversion states Unconditional, Busy and No Answer.

To configure a call diversion state's forwarding settings, click on the respective tab. The following settings are available:

No Forwarding	Your phone will be called directly.
Voicemail	Calls will be forwarded to your voice mail box.
To Number	Calls will be forwarded to the provided number.
Voicemail with Transfer	Callers are asked to leave a voice mail; if they refuse, calls will be forwarded to your mail box.
Mobile Connect	Calls will be forwarded to a mobile number or any other external phone number (see section Mobile Connect).
Forward after […] Seconds	Set the time the phone will keep ringing before forwarding the call. This option is only available for the No Answer state.

Mobile Connect

Allows you to forward a call to a mobile phone or any other external phone. On the configured phone, your company's central number will be shown as caller. After accepting by pressing the key 1 on your phone, an automatic voice message announces the caller's number (if available). Hanging up dismisses the call.

All calls that make use of Mobile Connect have the following capabilities:

Call-back to internal or external parties

During the call, press the star key ? on your phone. The call will be held while you enter an internal or external phone number to which this call should be redirected. Wait until the connection is established. Alternatively, you can return to the held call at any time by pressing the star key ? again.

Transfer an internal or external party

Follow the same steps as with *Call-back to an internal or external party*. Once the internal or external party answers the phone, press the pound key # ort hang up; the call will automatically be transferred to the called

party.

Three-way conference

Follow the same steps as with *Call-back to an internal or external party* but instead of pressing the star key, press 3 after the third party has answered. The calls will be connected to a three-party conference.

Notification

Forward to Email Account will send an email to your account whenever such a message arrives. The voice mail or fax message itself will be included in the email as attachment.

Mark messages as read will mark messages as read and stores them as old messages; no messages are subsequently signaled on any phones, neither by means of MWImessage waiting indicator nor on the displays. Select this option if you use an external email client only and do not intend to access your voice mail messages on the phone or via Callisto's web interface.

Send SMS when receiving a message will send a notification to your mobile phone whenever a new message arrives. This option is only available if your account is authorized to send SMS messages.

Announcement

Here you can modify and select your custom messages and announcements. The following options are available:

- Standard option for Callisto standard welcome message
- Announcement A option for your custom welcome message A
- Announcement B option for your custom welcome message B
- Announcement C option for your custom welcome message C

Select the Recording active check box next to the corresponding message to give callers the ability to leave a message. Per default, the standard greeting has recording enabled.

To record a custom message, you can either use the phone (see Phone functions – Change settings) or upload a wave file:

1. In the *Announcement* menu, click Upload new audio file.
2. From the Announcement drop-down menu, click either Announcement A, Announcement B, or Announcement C.
3. Click Browse and select the target file.
4. Upload the wave file to Callisto by clicking Upload.

Wave files must be of the format Wave (PCM); 8 kHz; 16 Bit; mono.

To listen to a message, click on the speaker icon.

On rare occasions, the MWI of your phone desynchronizes with new incoming voice messages. To resolve this, you can calibrate the MWI with the MWI On or Off buttons (if the option is available).

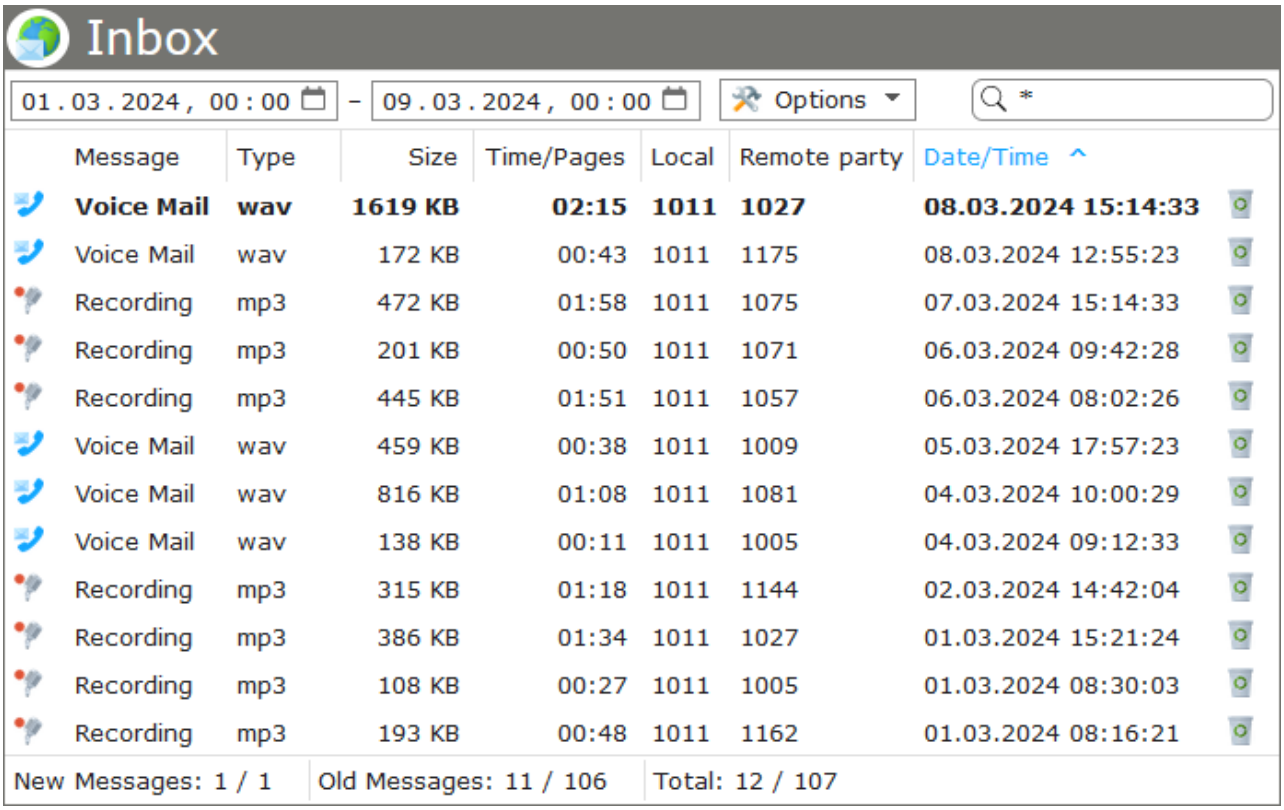
Make sure to click Save, otherwise any changes will be lost.

Message functions

In the main menu's *Messages* menu, all menu items below *Settings* are functions for managing various kinds of messages.

Inbox

All your incoming voice mail and fax messages are listed here. Click a caller's number to initiate a call back. Clicking the *recycle* icon deletes the message.



New messages will be displayed in bold. Once a message is played or read, it will be marked as old message and be shown in a regular font.

Sent items

List of all messages which were successfully transmitted to the receiver.

Outbox

Messages which are pending, outgoing, or could not be delivered are listed in the outbox. The State lets you know the reason why the message hasn't been delivered (yet).

Send Fax

Send your fax messages from the Callisto web-interface. Alternatively, you can send faxes directly from any

Windows-compatible application which is able to print or to create a PDF.

Enter the receivers number and provide the document you want to send in PDF format

Send SMS

Send SMS messages directly from Callisto. To use this feature, your Callisto administrator must have configured it first.

Cisco Phone Message

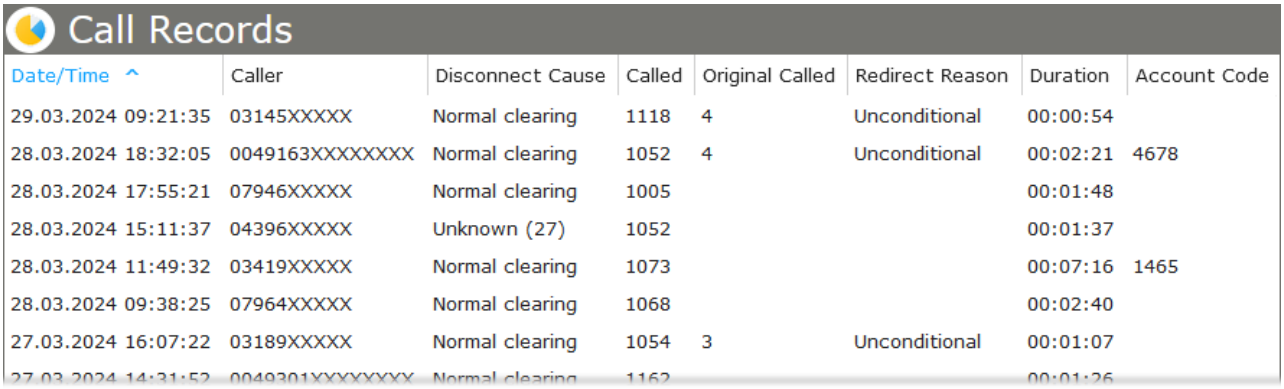
Similar to SMS messages, you can send messages to other Cisco IP phones in your domain.

Enter a title, message, and your phone number, then you can send it to a single or multiple users at once.

Reports menu

In the main menu, choose Reports > Call Records to view records of conducted calls. Access to use report filters is given to users by Callisto administrators. Contact your administrator for permission and creation of new filters.

Select the filter apply and then select an output option from the radio buttons: Monitor will display the records in your browser, MS Excel will export the reports as an XLS file and MS Access will export the reports as an MDB file. Microsoft Access reports contain additional details, like lists and graphs.



Call Records

Date/Time	Caller	Disconnect Cause	Called	Original Called	Redirect Reason	Duration	Account Code
29.03.2024 09:21:35	03145XXXXX	Normal clearing	1118	4	Unconditional	00:00:54	
28.03.2024 18:32:05	0049163XXXXXXXX	Normal clearing	1052	4	Unconditional	00:02:21	4678
28.03.2024 17:55:21	07946XXXXX	Normal clearing	1005			00:01:48	
28.03.2024 15:11:37	04396XXXXX	Unknown (27)	1052			00:01:37	
28.03.2024 11:49:32	03419XXXXX	Normal clearing	1073			00:07:16	1465
28.03.2024 09:38:25	07964XXXXX	Normal clearing	1068			00:02:40	
27.03.2024 16:07:22	03189XXXXX	Normal clearing	1054	3	Unconditional	00:01:07	
27.03.2024 14:31:52	0049301XXXXXXXX	Normal clearing	1162			00:01:26	

Call reports shown in *Monitor* view.

Account codes can be provided during ongoing calls by typing the code digits on the Cisco IP phone's keypad.

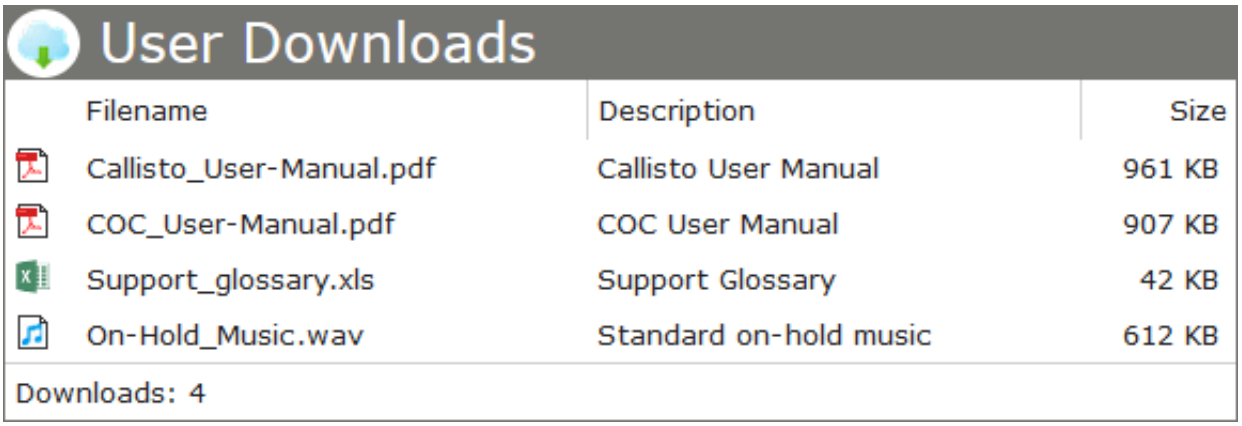
If the caller's number is associated with a directory entry, hovering over the number will reveal detailed information about the caller.

Callisto UCM limits the CDR output to reports on fax messages only, since Cisco Unified Communications Manager already provides call detail records for voice calls but not for fax messages.

Callisto Express provides records for both voice calls and fax messages, since no CDRs are available in Cisco Unified Communications Manager Express.

Downloads

In the main menu, choose Download > User Downloads to see a list of downloadable content such as features (e.g. Jabber extensions), information or other files provided by your system administrator.



Administrators can associate download files with one or multiple languages. Such files will only show up in your download list when your account language is set to one of the associated languages, e.g., an English-language file will only appear in the download view if your account language is set to English as well.

The account language can be changed in the user menu.

Virtual Conference Rooms

The optional *Virtual Conference Rooms* service provides telephone conferences for three or more participants. Rooms are protected by passwords, which are managed by the system administrator.

Virtual Conference Rooms can be accessed either by phone or by LiveView.

Access via phone

Dial the conference room's access number and password on your phone's keypad. If you are the first participant to enter, you will be welcomed by music on hold. As soon as another participant arrives, a ring tone signal will play. Any further participant entering the conference will be announced by a ring tone as well.

If you have a conference administrator password, you can invite other parties to the conference. To do so, press the asterisk key ? on your phone, followed by the phone number of the person you wish to invite to the conference. If the invitee is available, pressing the pound key # returns both of you to the conference. Alternatively, press the asterisk key ? again to terminate the call and return to the conference without the invitee.

Access and visualization via LiveView

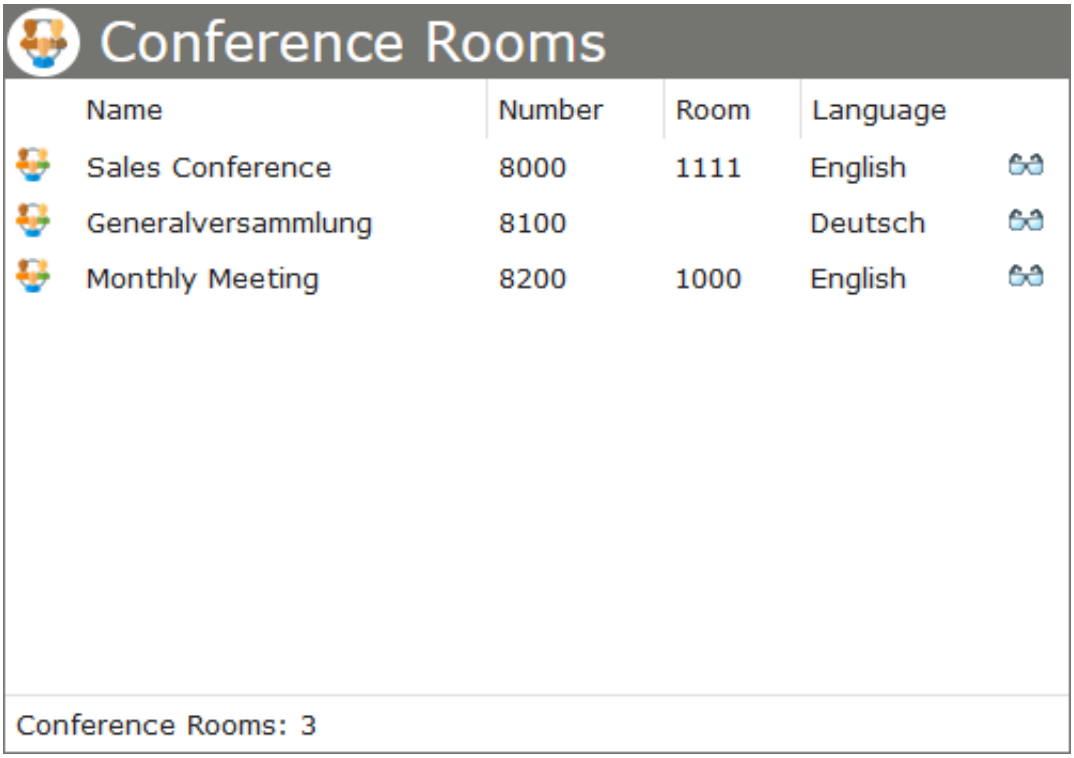
The LiveView plug-in only works within Firefox and Internet Explorer; Chrome no longer supports Java applets.

To prevent problems, the Callisto IP address should be added to the local Java configuration (Control Panel > Java or Startmenu > Java Control Panel) within the Security tab. To modify the exception site list, click on Edit Site List and add the Callisto IP. Additionally, navigate to the General tab and delete the temporary Java cache. Choose Settings > Delete Files and select all checkboxes.

The Callisto conference's LiveView offers complete control of Virtual Conference Rooms through a regular web browser.

LiveView icon

From the main menu, choose Conference Rooms > Conference LiveView to show a list of all available conference rooms. Select a conference room by clicking its *LiveView* icon and enter an administrator PIN to access the LiveView visualization of this conference room.



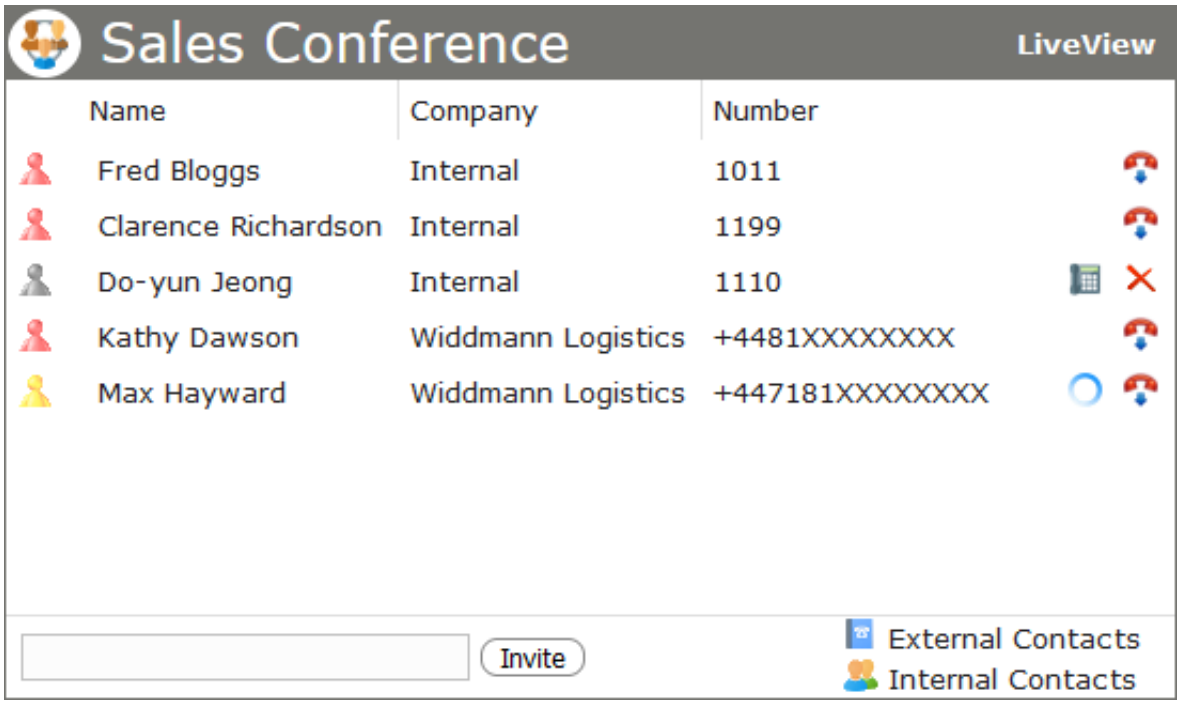
During the LiveView session, all participants are listed showing their current state. The following states are defined:

participant is active

participant currently being added

participant currently being invited (called)

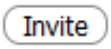
participant has left the conference or has declined the invitation



The following options are available to manage the conference:

Select external contacts to be invited to the conference.

Select internal contacts to be invited to the conference.



Invite a contact to the conference by entering a phone number.

Terminate a participant’s connection/invitation.

Remove a participant from the conference.

Re-invite a participant to the conference.

Phone functions

Using an internal Cisco IP phone

The following functions are available for Cisco IP phones that are integrated in the same environment as your Callisto installation.

Call forwarding to voice mail

Press the *Forward* button on your Cisco IP phone and type the voice mail number given to you by your Callisto administrator.

Listening to voice mail messages

Messages button on
a Cisco IP phone

Dial the voice mail number or press the *Messages* button on your Cisco IP phone. The total number of new messages is announced and the last message is played back.

1	Store the message (will appear in *Old Messages* afterwards).
2	Listen to the message again.
3	Delete the message.
4	Listen to message information (caller number, date and time of the call).
5	Call back immediately (if the call is answered, the message is stored; otherwise it is played again).
#	Return to the main menu.

Directories

Services button on
a Cisco IP phone

All three types of Callisto directories (global, local, and private) can be selected through your IP phone's display. Press the *Services* button on your Cisco IP phone and select a directory. The phone's keypad can be used to search for contacts. The search behaves the same way as with Callisto's search operators, and the star key ? can be used for the asterisk (*) wildcard. Contacts can be called directly from this menu.

Callisto administrators have the possibility to add further services to the service menu. Ask your administrator about custom services available with your Callisto system.

Using an external phone

The following functions can be accessed with any phone supporting DTMF, by calling the voice mail service number provided by your Callisto administrator. Callisto welcomes you in your company's language and

you are asked to enter your internal phone extension followed by your user PIN. The user PIN can be configured in Callisto (see Message settings). After entering the internal phone extension and the user PIN, you will enter the *main menu*.

Each entry can be terminated by pressing the pound key #.

Main menu

1	Listen to voice mail messages.
2	Change settings.
?	End the call.

Listen to voice mail messages

After pressing 1 in the main menu, all voice mail messages marked as *new* will be played.

1	Store the message (will appear in *Old Messages* afterwards).
2	Listen to the message again.
3	Delete the message.
4	Listen to message information (caller number, date and time of the call).
5	Call back immediately (if the call is answered, the message is stored; otherwise it is played again).
#	Return to the main menu.

Change settings

After pressing 2 in the main menu, you enter the settings menu.

1	Activate a diversion (call forwarding) to your voice mail.
2	Activate a diversion to an internal or external subscriber number. Enter an internal or external subscriber number and confirm with the pound key #. The entered phone number will be read by the Callisto system, and you will be returned to the settings menu.
3	Change personal announcements. The currently active announcement will be played. Change it by pressing:

?	1	Activate the standard announcement.
	2 3 4	Activate the alternative announcement A, B, or C, respectively.
	?	1 Listen to the currently configured announcement (recording will be played).
		2 Record a new announcement (speak after

	the beep sound and press 0 to complete the recording).
3	Activate the alternative announcement you chose in the previous step.

CALLISTO

PLATFORM

QUICK REFERENCES

Search operators

Most search fields inside Callisto (e.g., in the Userlist) support a basic range of search operators. Search queries are case-insensitive.

If you search for multiple terms separated by spaces, they work by logical conjunction (i.e., only results that contain a match for *all* terms will be shown).

There are two wildcards available:

- An asterisk (*) will substitute for zero or more characters, e.g., searching for h*on will find words like Honey or Harrison.
- An underline (_) will substitute for exactly one character, e.g., searching for b_n will find words like Ben or Bannister.

Search terms match only words that begin with the term, i.e. they always behave as if an asterisk is trailing each term. For example:

- Searching for j will find words like John, Jane, and Jenkins, but will not find words like Benjamin or Elijah.
- Searching for man will find words like Manuela and Manchester, but will not find words like Germany or Newman.

If you are searching contacts, you can use the tags #vip0 to #vip5 to limit the search to contacts with the corresponding VIP status. For example, searching for #vip3 will show all contacts that have VIP status 3.

Regular expressions

CTMaker, SQLite as well as some functions in Callisto support regular expressions. The following basic regex syntax is available:

Character	Legend
^	Match the beginning of a buffer.
$	Match the end of a buffer.
()	Group characters or capture them as substring.
\s	Match whitespace.
\S	Match non-whitespace.
\d	Match decimal digit.
\n	Match new line character.
\r	Match line feed character.
\f	Match form feed character.
\v	Match vertical tab character.
\t	Match horizontal tab character.
\b	Match backspace character.
+	Match one or more characters (greedy; match as many as possible).
+?	Match one or more characters (lazy; match as many as needed).
*	Match zero or more characters (greedy; match as many as possible).
*?	Match zero or more characters (lazy; match as many as needed).
?	Match zero or one character (lazy).
x|*y*	Match either *x* or *y* (alternation operator).
meta	Literally match one of the meta characters: ^$().[]*+?|\ Example: \? matches a question mark.
\x*HH*	Match a character by its hexadecimal value. Example: \x4a matches the letter J.
[…]	Match any character from a given set. Ranges like are supported.
[^…]	Match any character except the ones from the set.

The following functions evoke a search by regular expressions. They return the matching string, or an empty string if there is no match.

- SQLite: regexp(*pattern*, *data*)
- CTMaker: STR_Regex(*pattern*, *data*)

Copyright

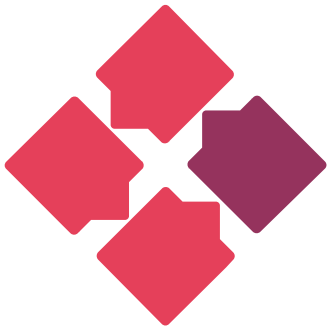
Disclaimer

Changes are possible without notice.

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

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