CALLISTO

PLATFORM

ADMINISTRATION MANUAL

Table Of Contents

Administration manual 3
Documentation reference, requirements 3
Administration management 4
System 6
User administration 18
Messages 30
Reporting 32
Downloads 36
Options 38
Callisto Gadgets overiew 46
Integration of Callisto Gadgets 51
Smartphone integration 55
Maintenance and service 56
Copyright Information, Disclaimer 61

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.

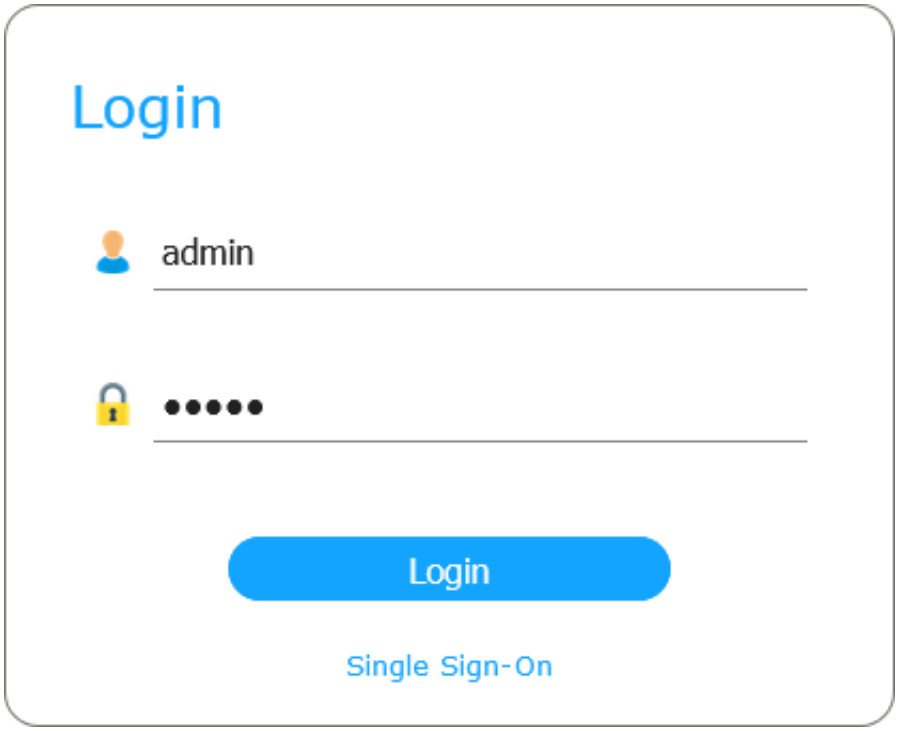
For administration tasks, a browser is required:

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

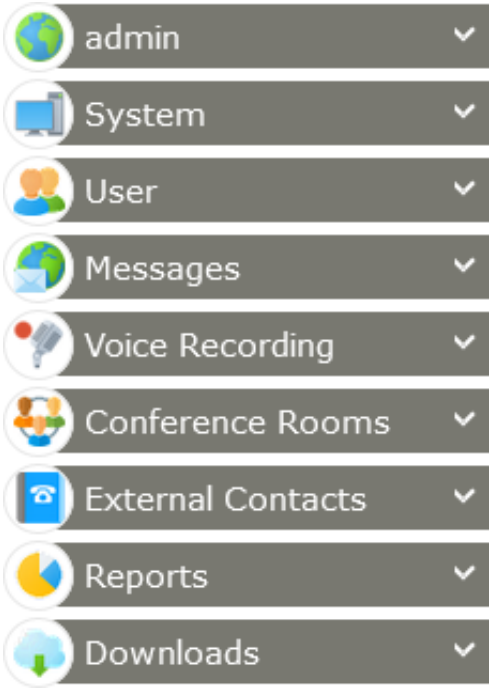
Administration management

Access Callisto with a browser from a client PC:

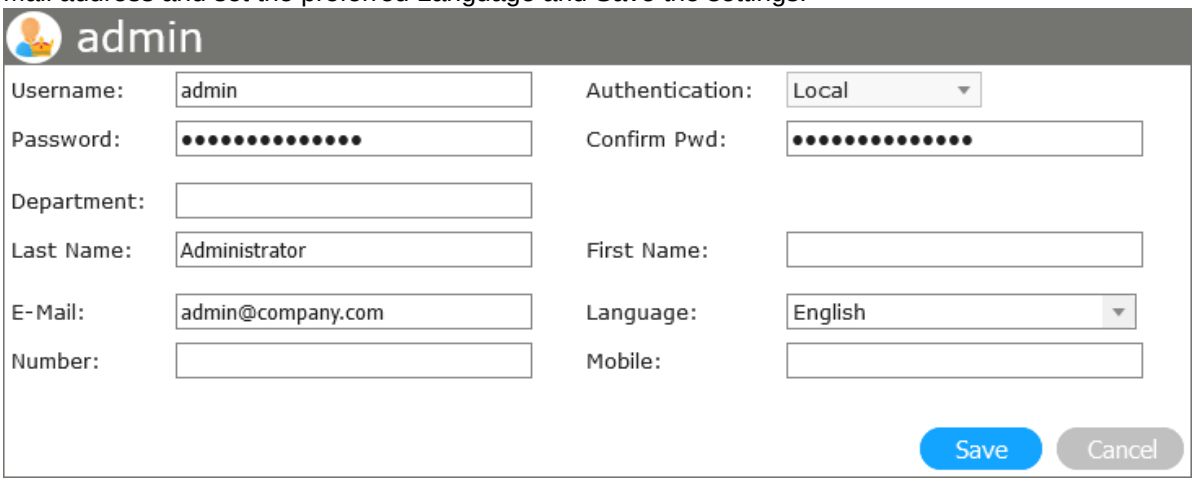
1. Connect to: http://<*callisto*>/, where <*callisto*> is the domain or IP address of your Callisto installation.
2. To logon, type the user name admin and default password admin. It is possible that the default administrator password was changed during installation. In this case, consult with the Cisco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

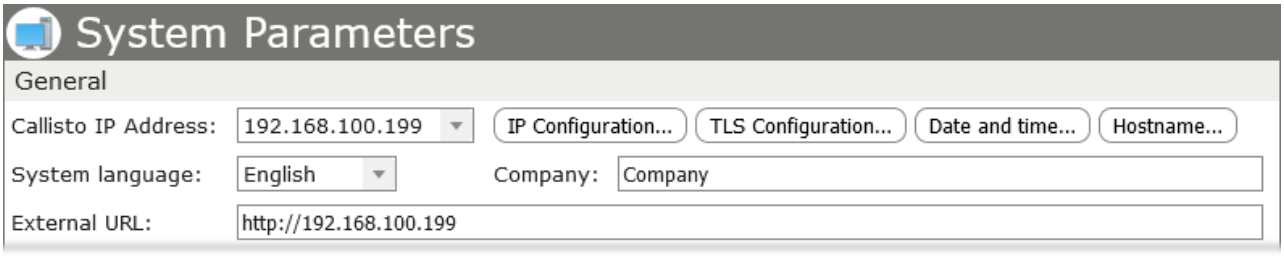


5. Administrator accounts cannot be used concurrently. Only one administrator at a time can be logged on to the appliance.
6. If the administrator's logon details should get lost, they can be retrieved from the backup system file. Therefore it is important to ensure that no unauthorized user has access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

System

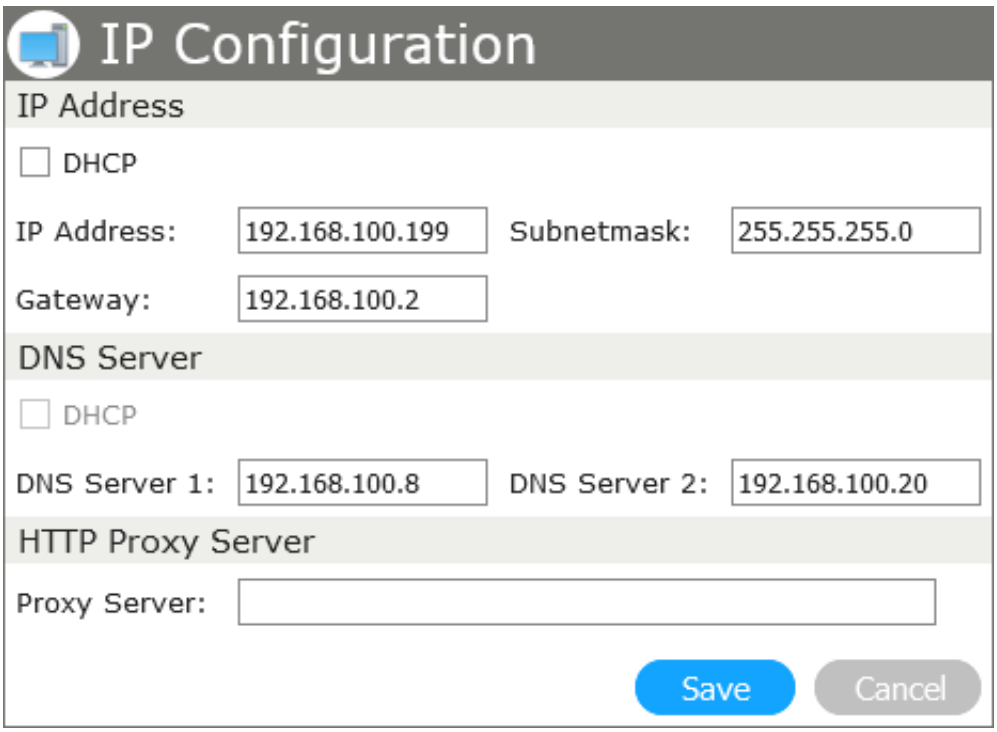
System parameters

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



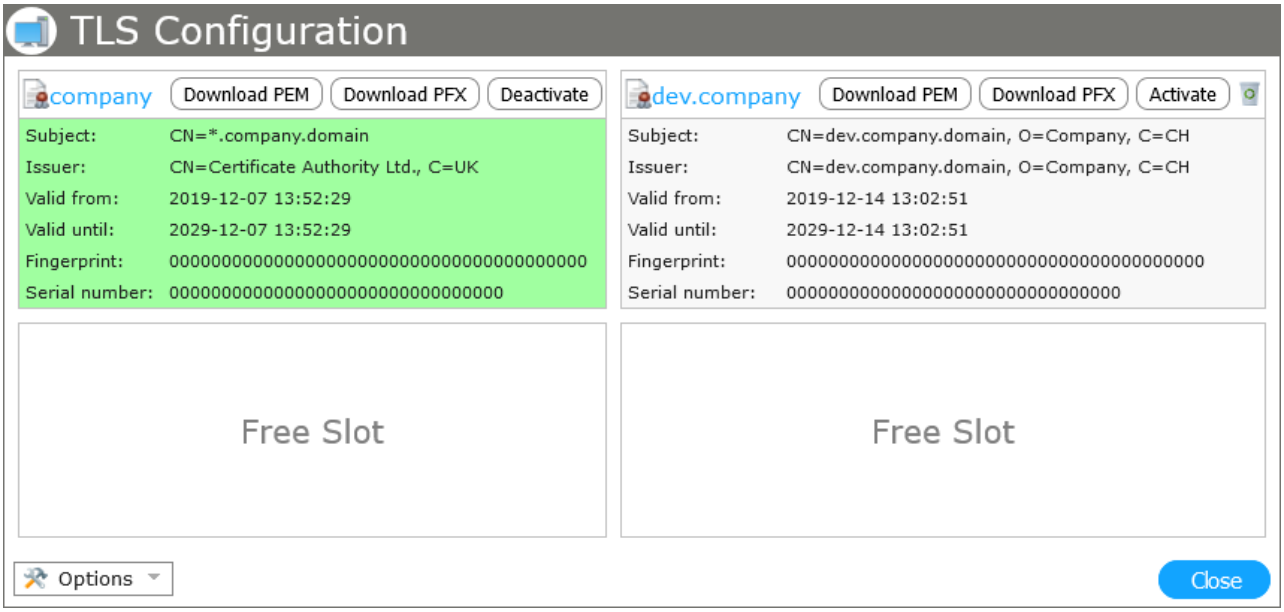
Callisto IP address(DHCP or static)

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”

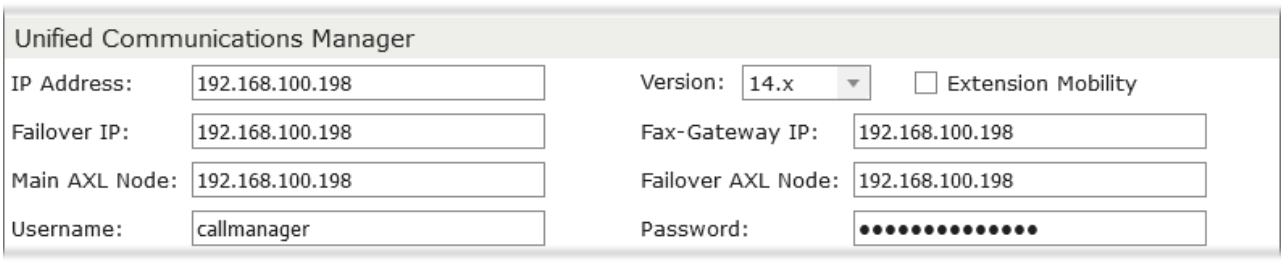
This section is only available on Callisto for CUCM Express.

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”

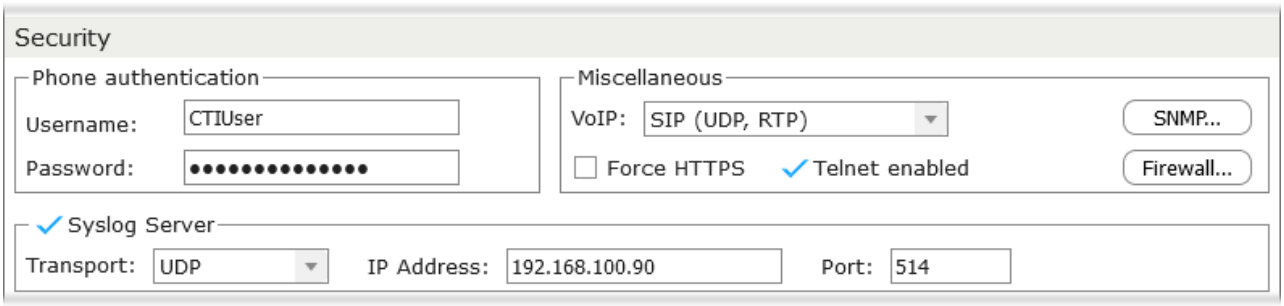
This section is only available on Callisto for Cisco UCM, HCS, Webex.



- 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).

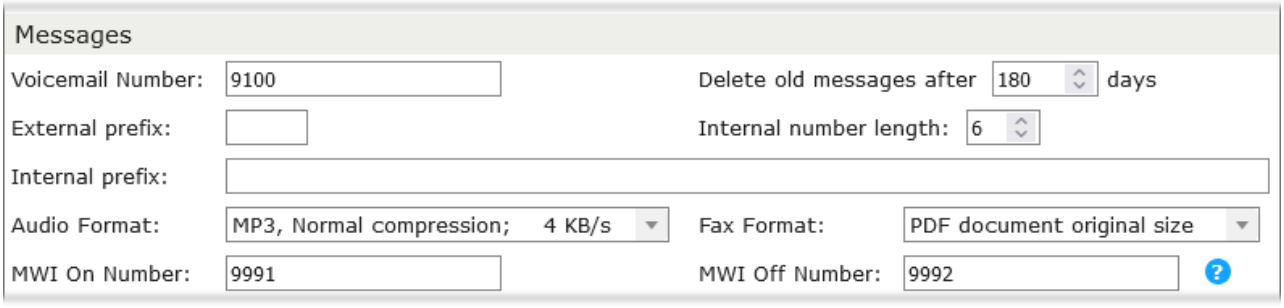
Miscellaneous

- 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).

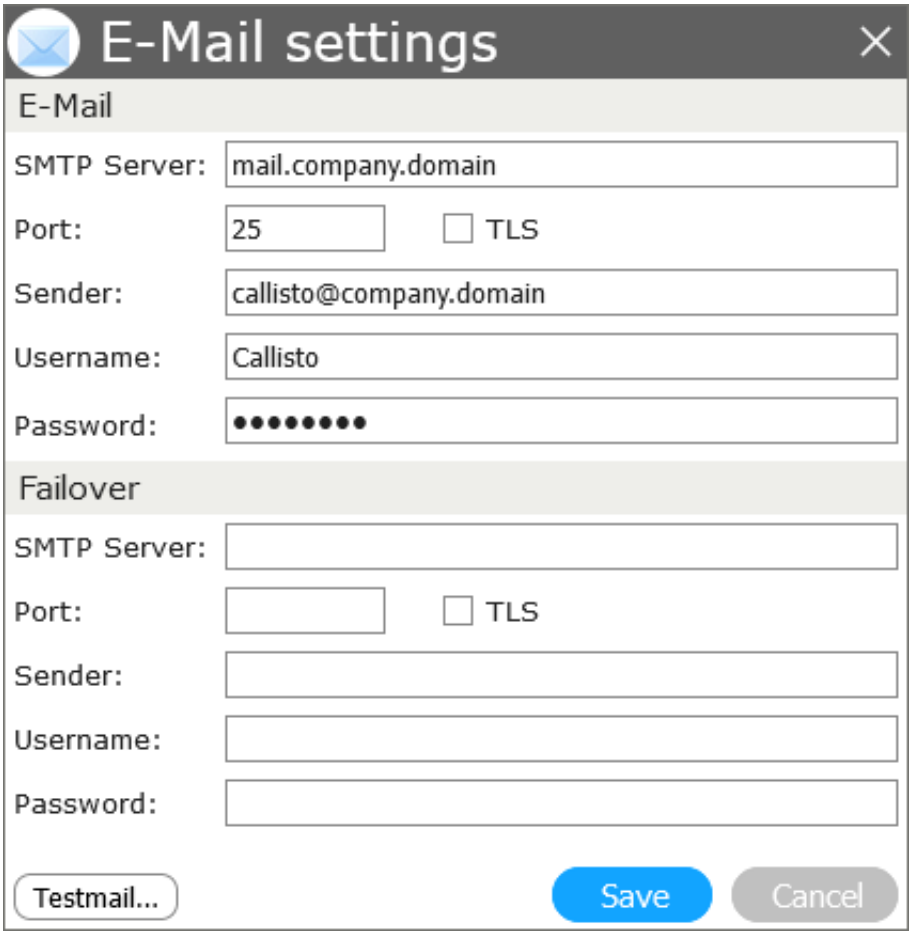
To listen to a voice mail by phone, dial the internal voice mail number. This number is dialled by users to access the voice messages for their phone. For external access an external number on the public telephone network must point to the internal number.

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.

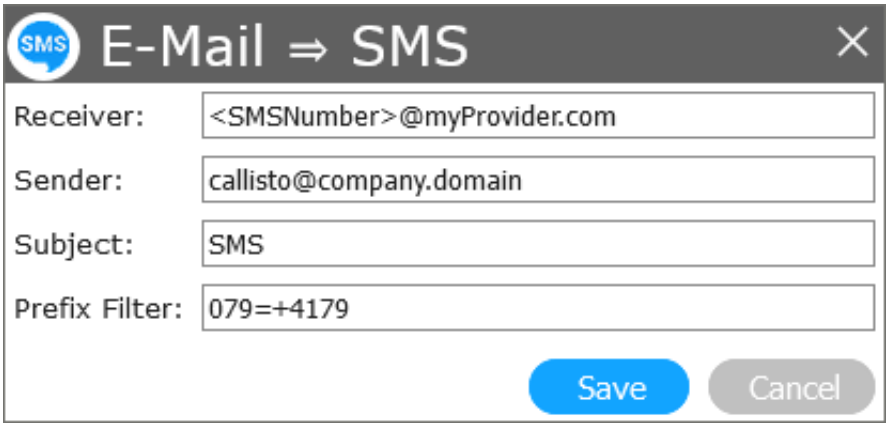
www.aspsms.com

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….

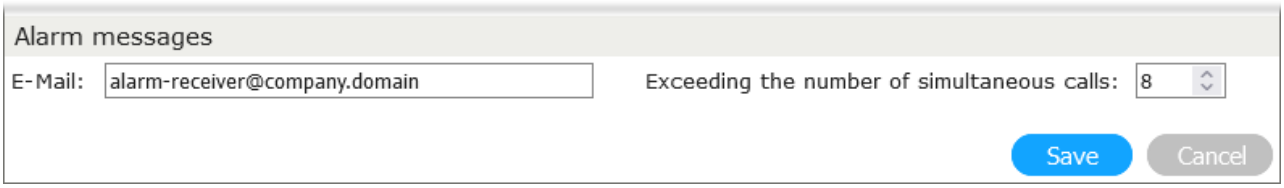


The term <SMSNumber> is a placeholder and will be automatically replaced with the recipient's phone number. Depending on the provider, this placeholder must be used either as part of the Receiver address or the message Subject in order to have the SMS properly forwarded.

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

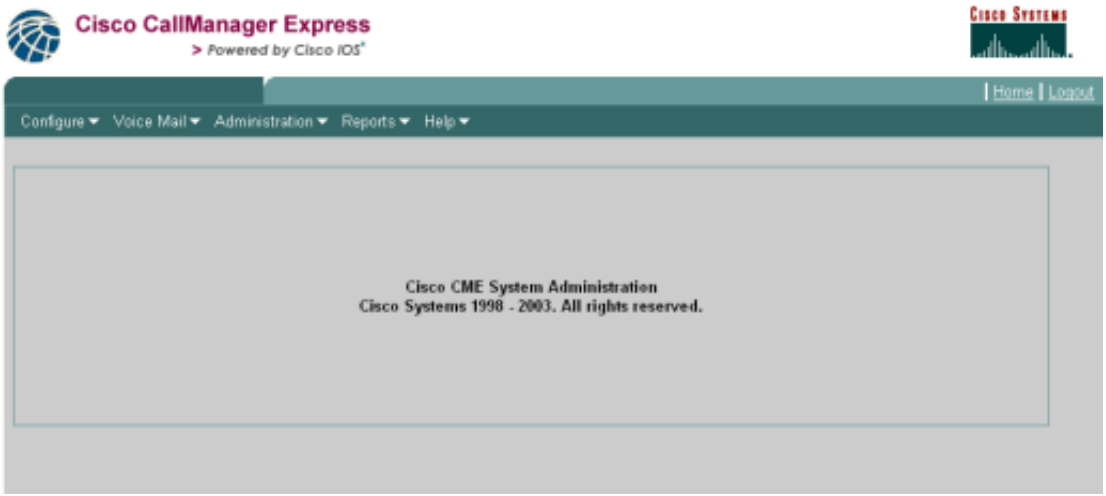
Save the current settings by clicking the Save button.

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

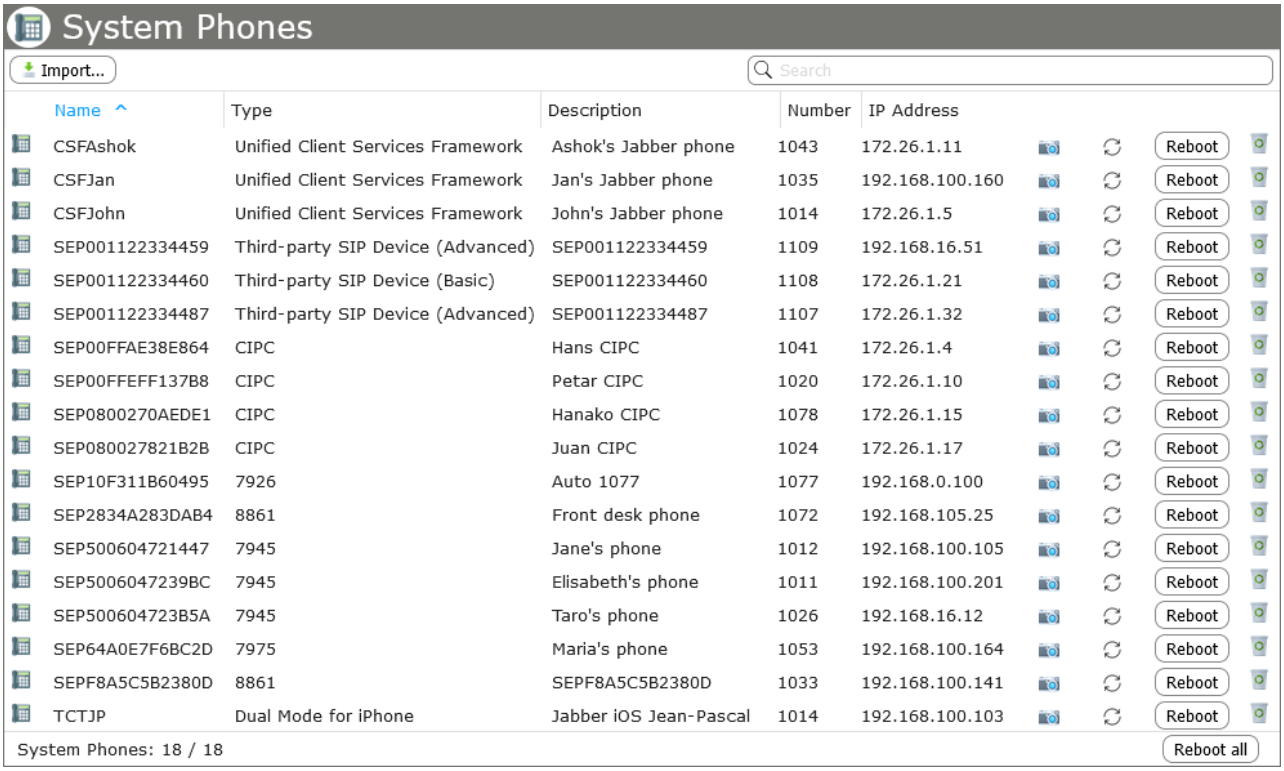
On the Cisco Unified Communication Manager Express, features such as routing of external to internal phone numbers can be configured, which can be used for remote access to voice mail boxes, fax and conference rooms.



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”.

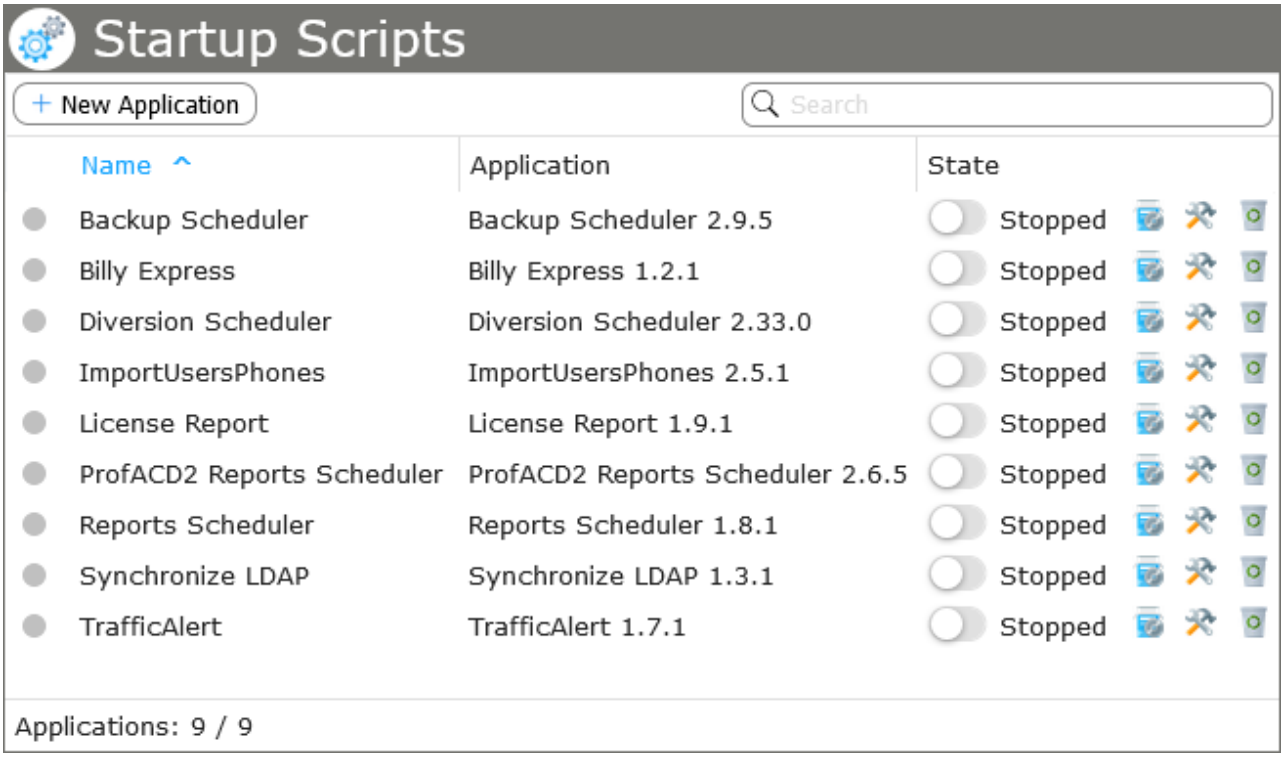
Startup scripts

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.



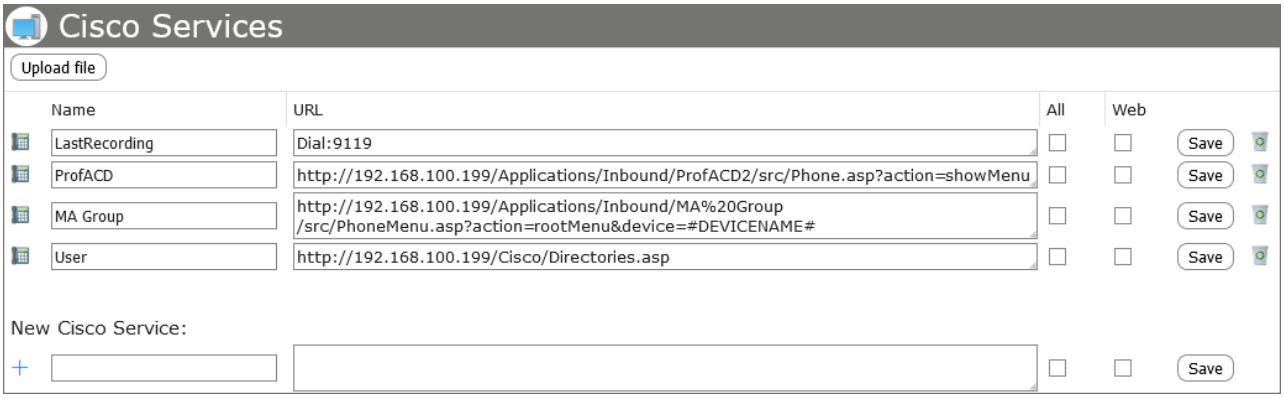
Cisco Services

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.



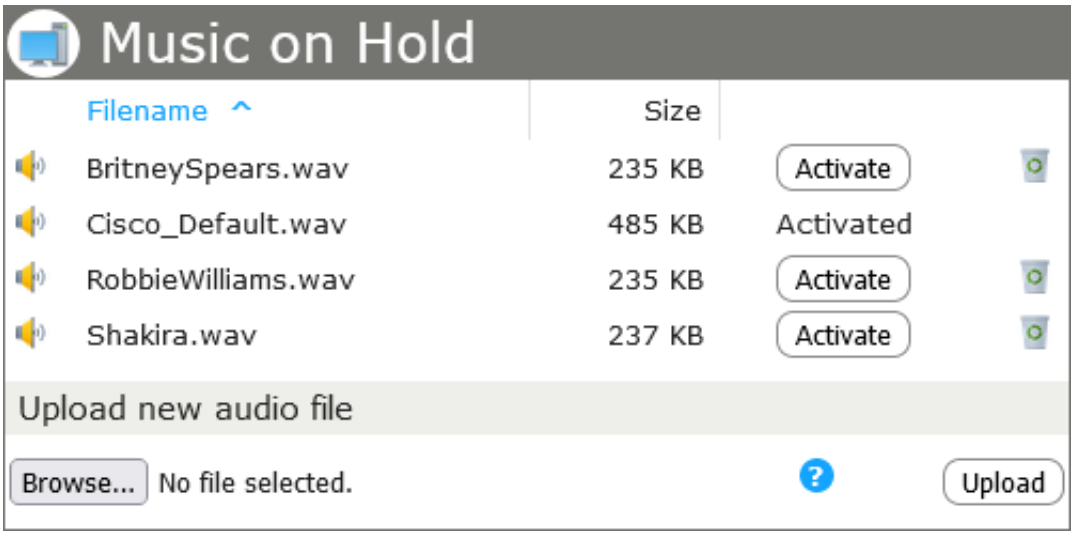
Checking All overrides any user privilege settings and makes the service available to all Callisto users.Checking Web enables the web frontend of this service and makes it available in the the user web GUI. This will only work for Cisco Services that have a dedicated web GUI.

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.

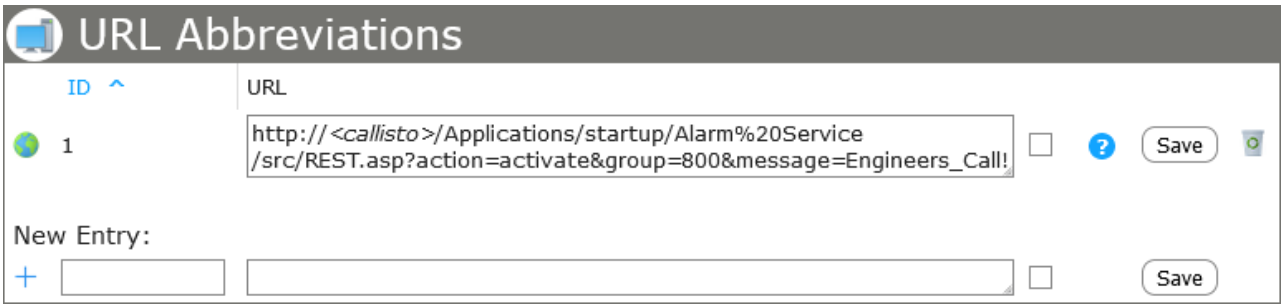
Per default, a Cisco music file (*Cisco_default.wav*) is activated.

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.



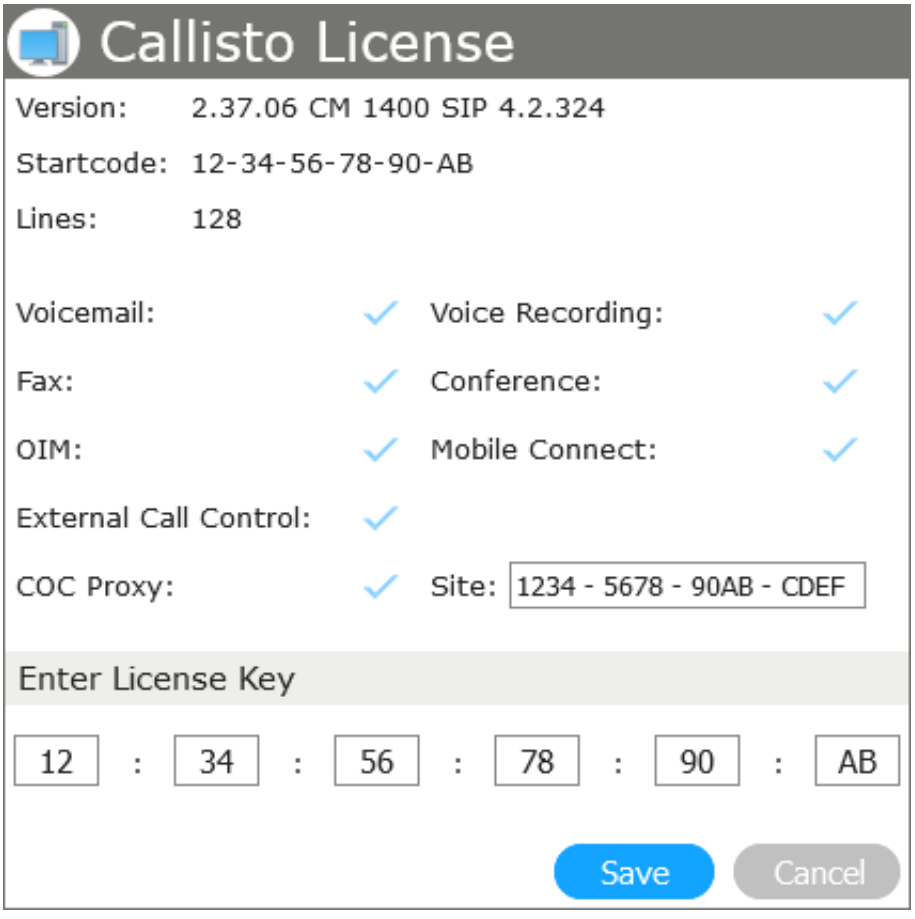
The example above would shorten the URL to http://<*callisto*>/ShortURL.asp?id=1 , with <*callisto*> being the domain name or IP address of your Callisto system and the value after id= being the number to the left of the original URL.

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.

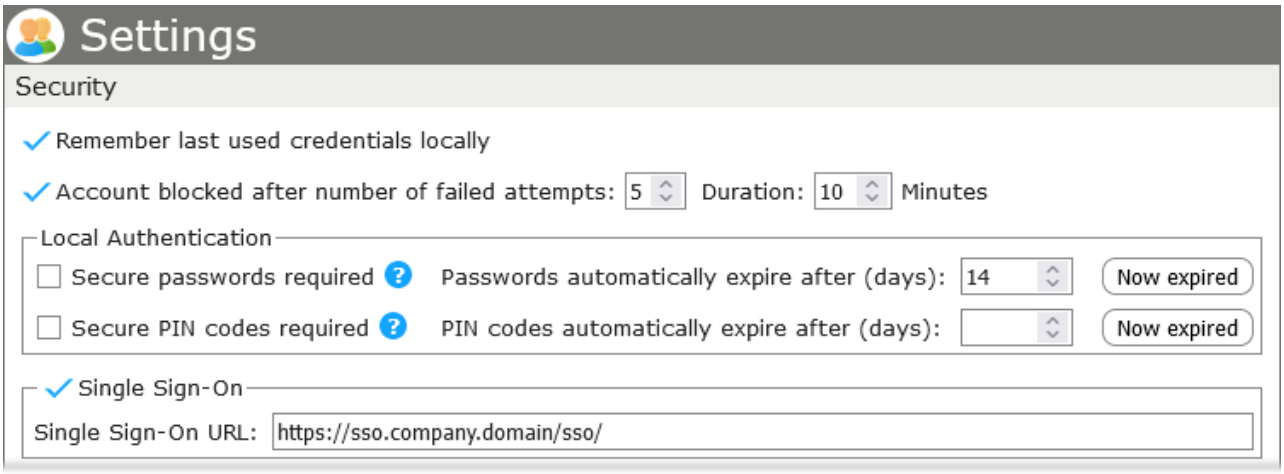
User administration

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



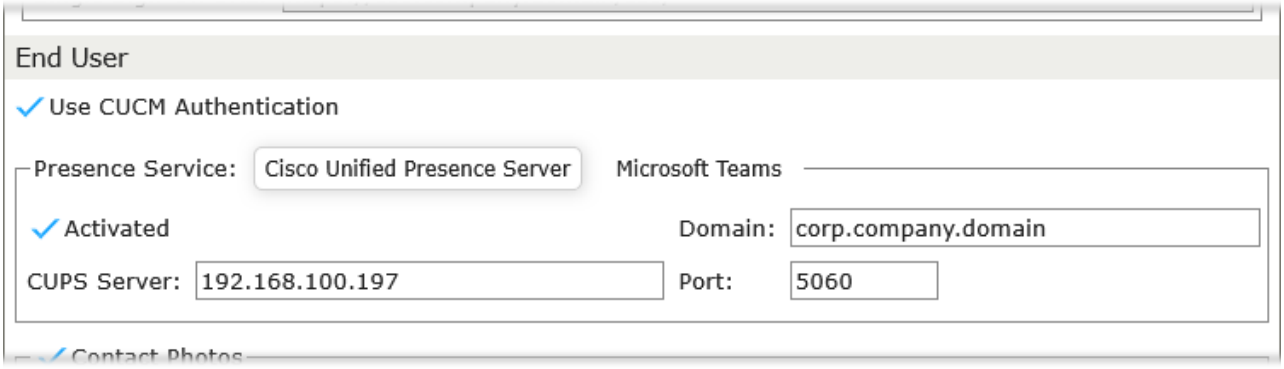
- When Passwords automatically expire after (days) is defined, users will be forced to change their password at the next login after the set expiration period.
- By clicking Now expired, all passwords from all existing users in Callisto will expire immediately. This only works if the parameter Passwords 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.

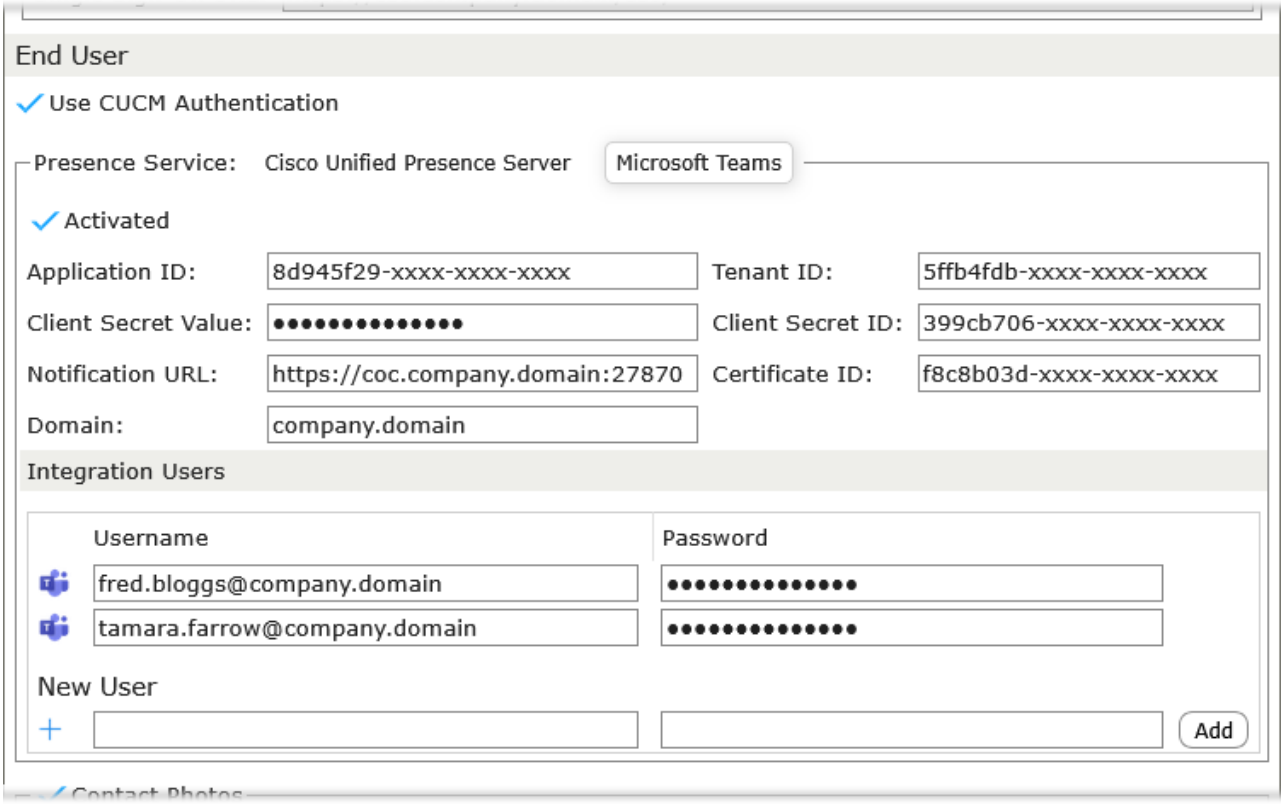
Authentication using Cisco Unified Presence Server



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.

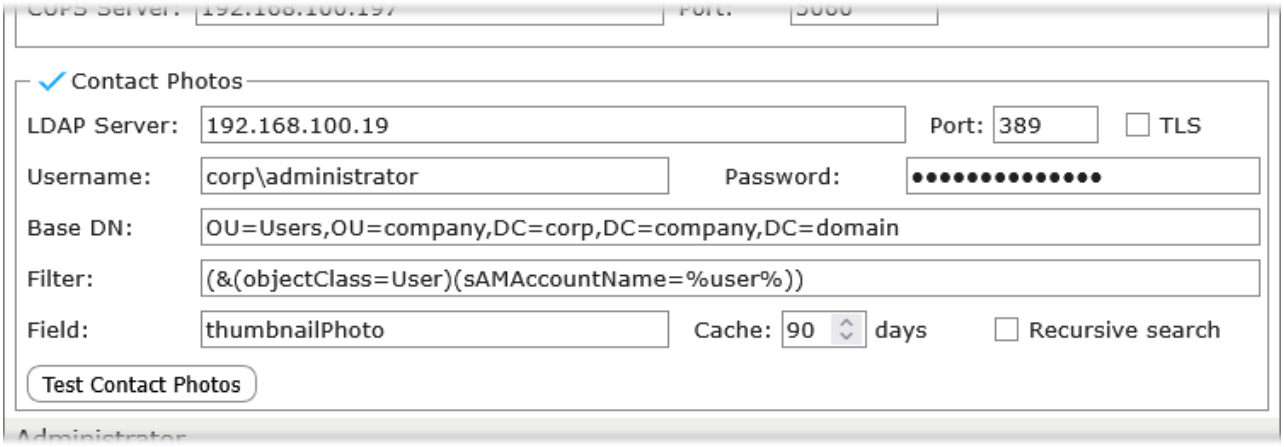
Activated	Check this box to enable CUPS integration. When activated, the system will connect to the specified CUPS server to retrieve and display user presence information.
CUPS Server	Enter the host name or IP address of your Cisco Unified Presence Server. This is the server that manages and distributes 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.

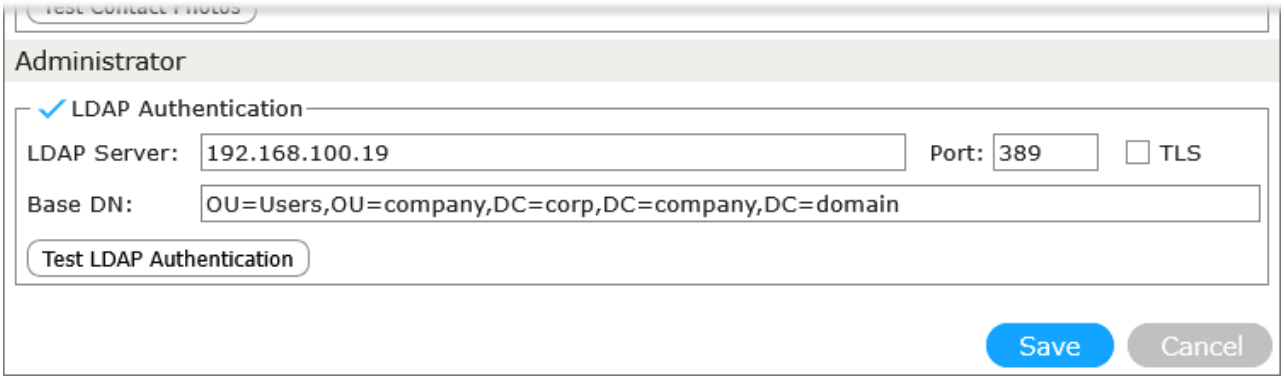
Contact Photos



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.

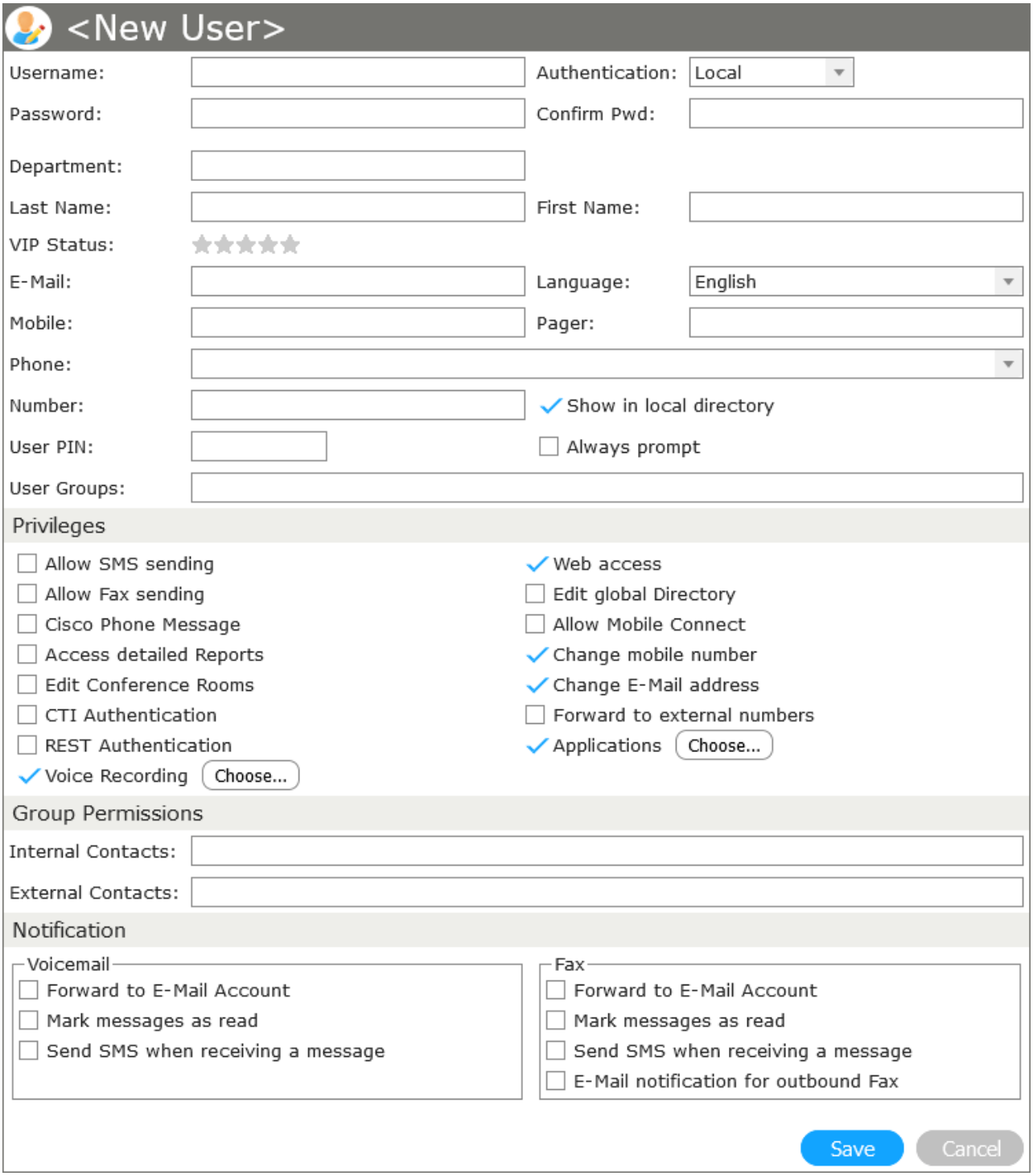
Administrator LDAP authentication



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

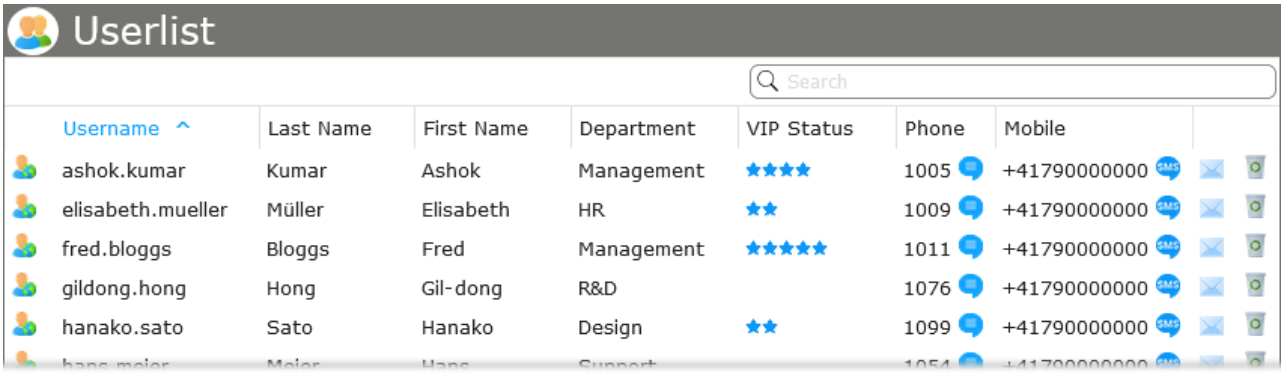
be checked.

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

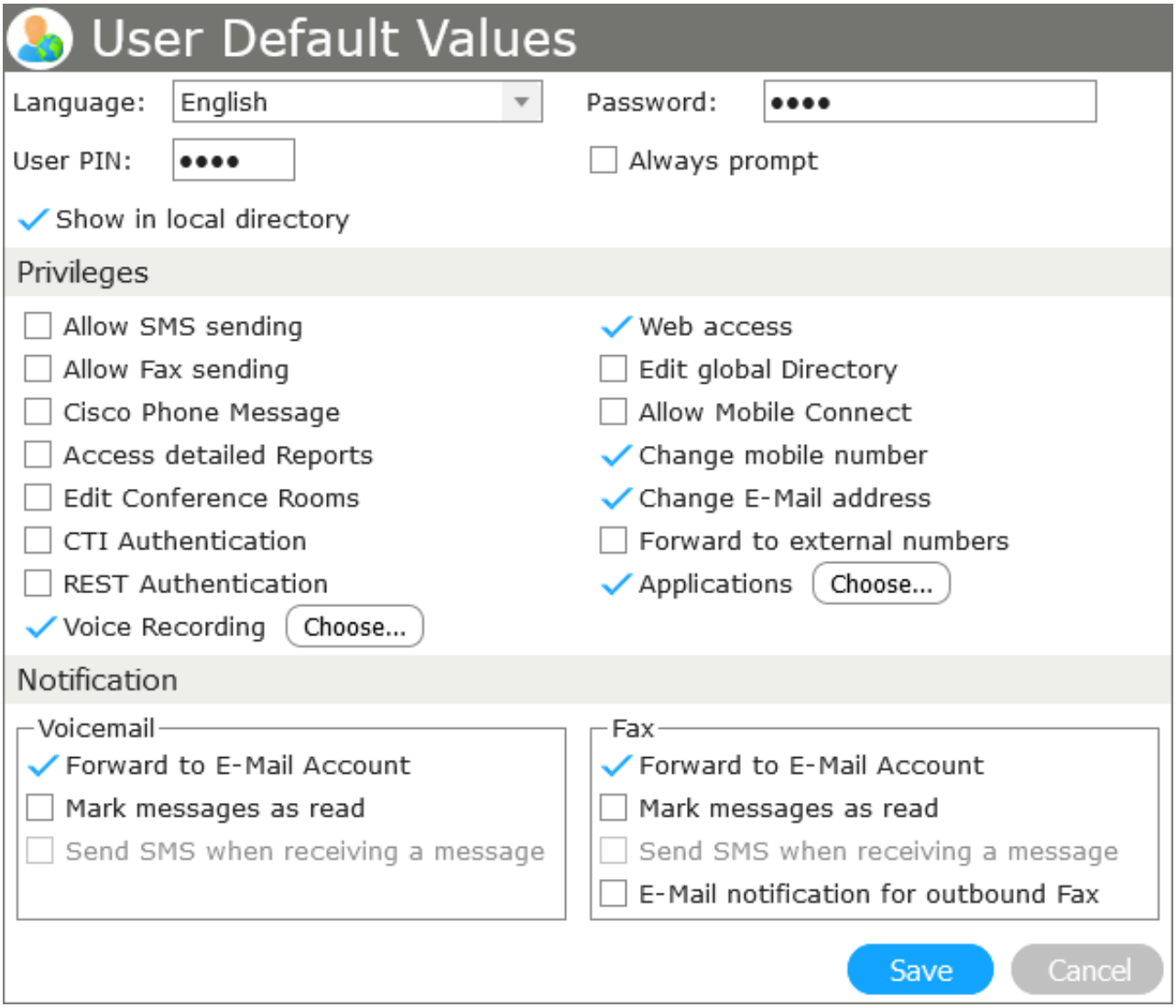
Phone message icon

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.

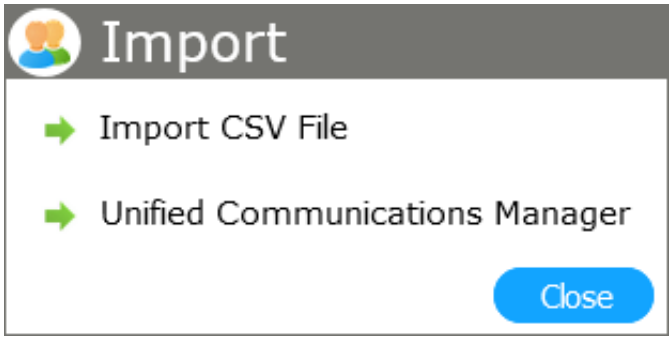
To add or remove a user from a group, choose User > Userlist, select the user you want to edit and choose all groups the user is a member of in the User Groups field.

Import users

Import with Unified Communications Manager

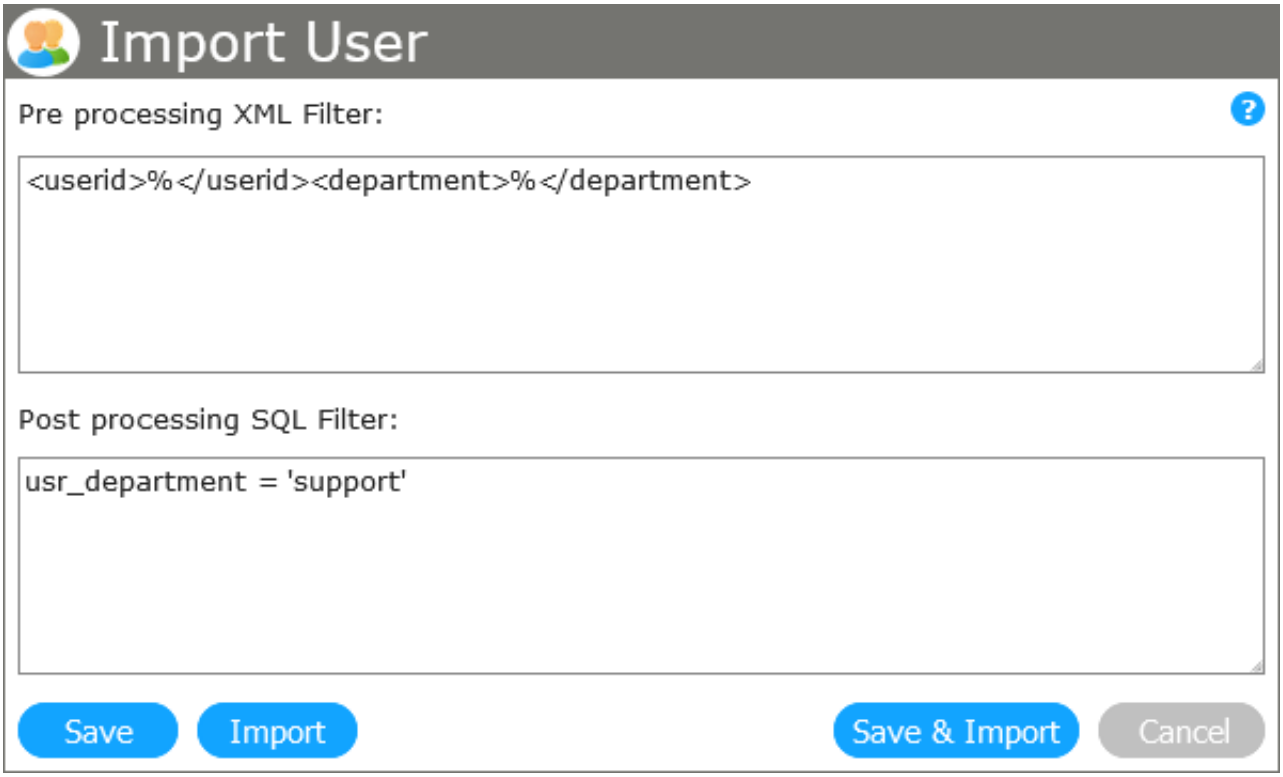
This option is only available on Callisto for UCM, HCS, Webex.

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')
```

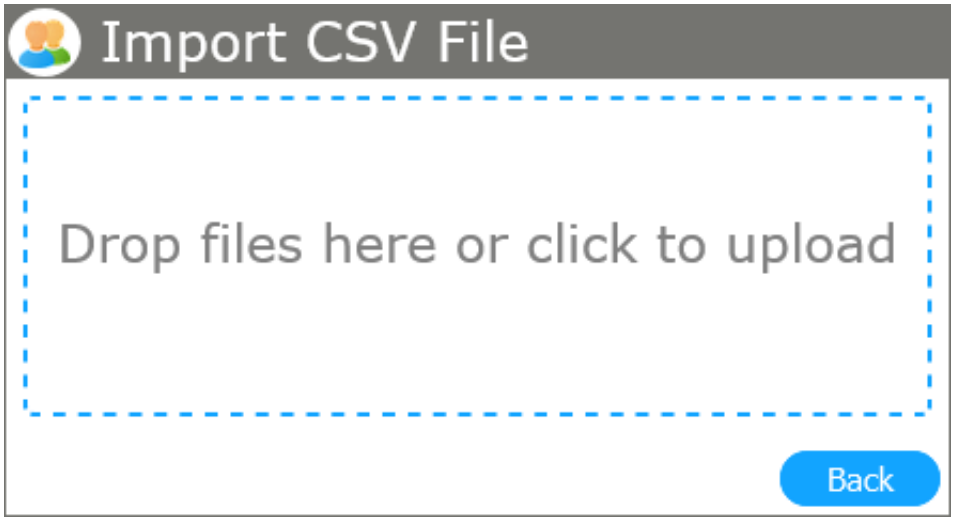
Additional SQL fields

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'

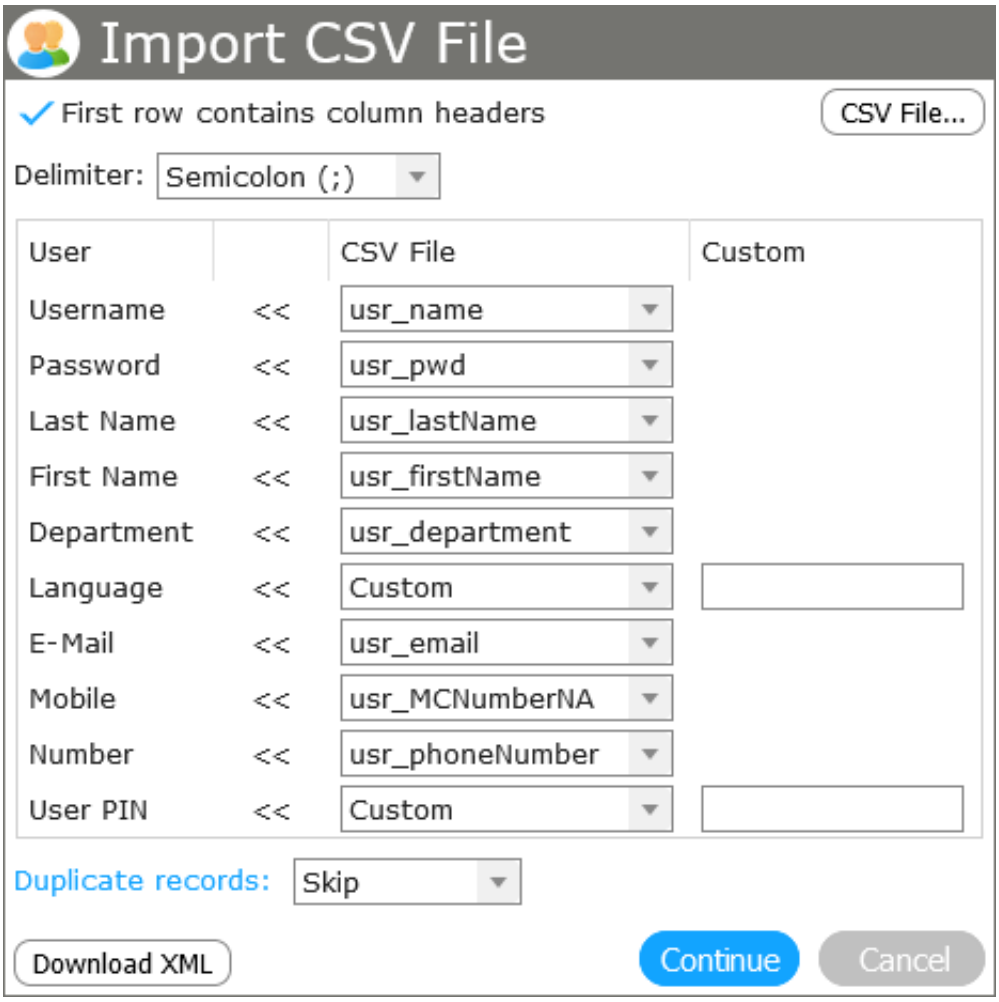
Name	Type	Example
usr_PhoneNumber	string	'1001'
usr_Department	string	'support'

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.



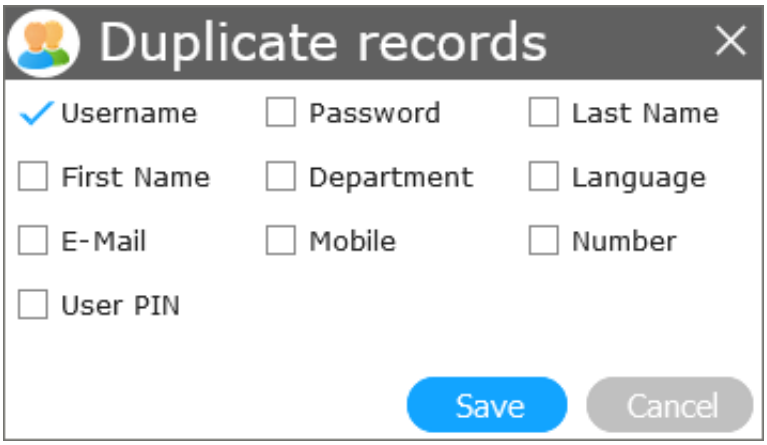
Select the proper Delimiter used in your CSV file. If the file's first row consists of a header record, check First row contains column headers.

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.



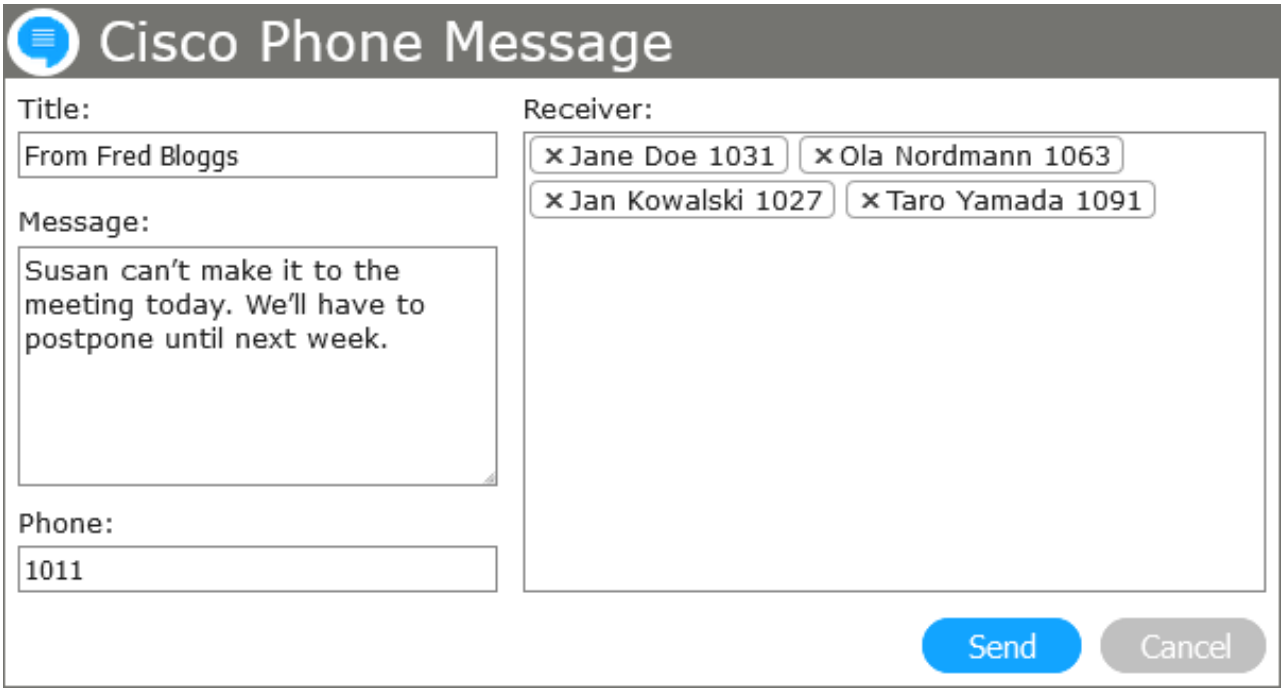
In the drop-down list to the right of Duplicate Records, you can decide how to handle duplicates.

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.

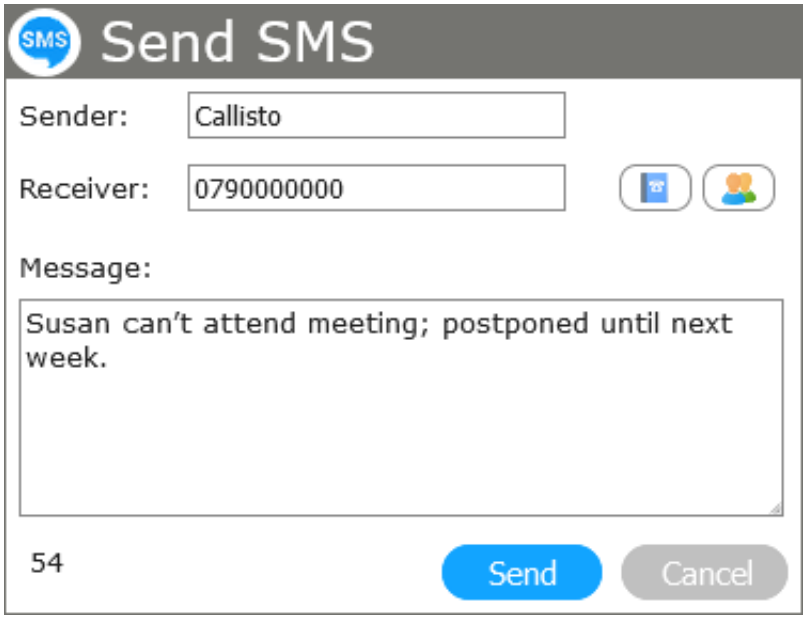
Type a title, the message and your phone number. The recipients can call back to the number you entered by the press of a button on their Cisco IP Phone.



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

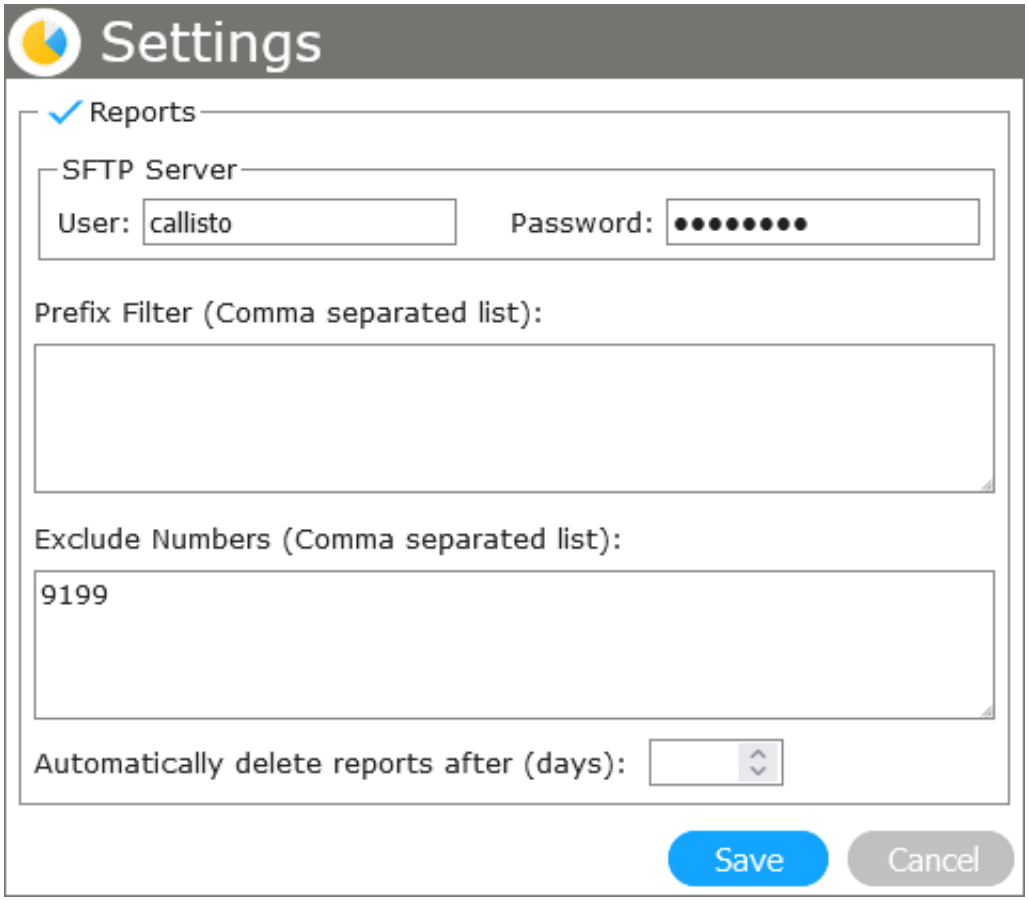
Enter the number or select a recipient from your directories. Open a directory, search the recipient, and confirm the number with a click on the *SMS* icon. To send the message, click Send.


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:

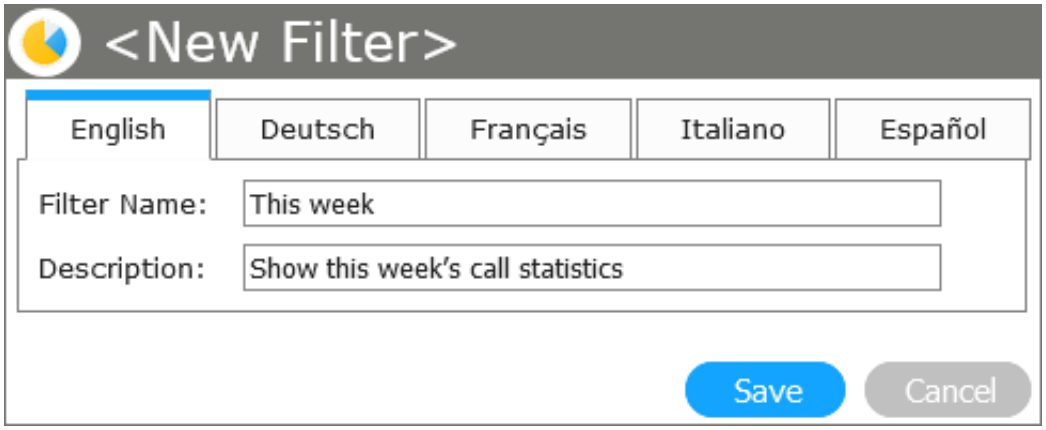
- Date/Time, Caller
- Called
- Duration
- Account Code
- SQL

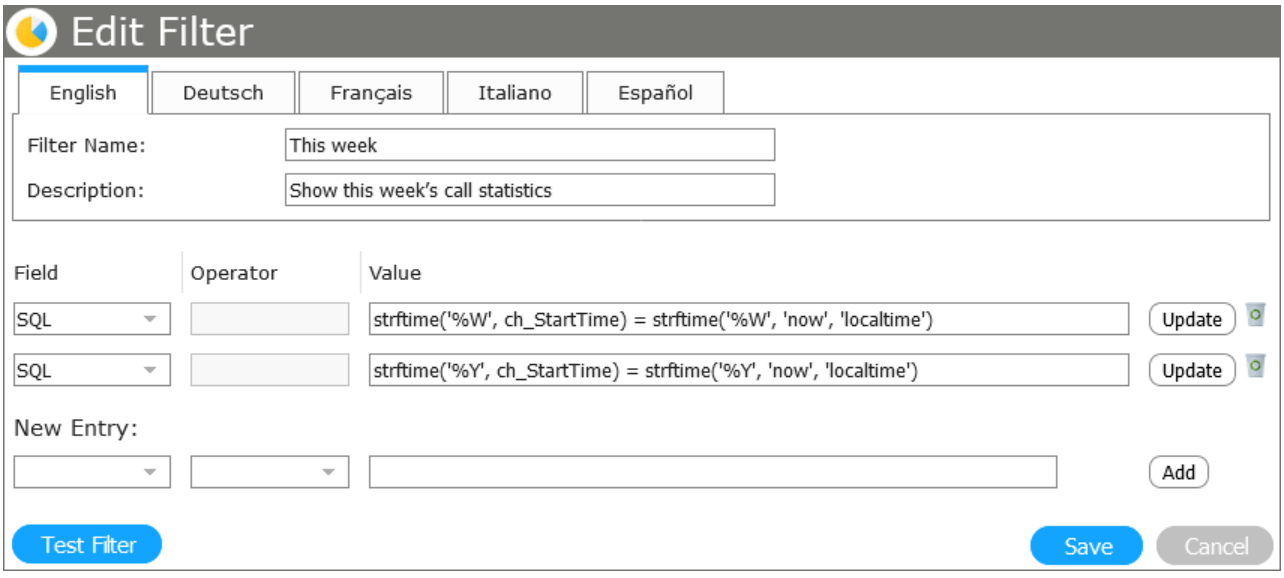
The following operators can be selected:

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

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

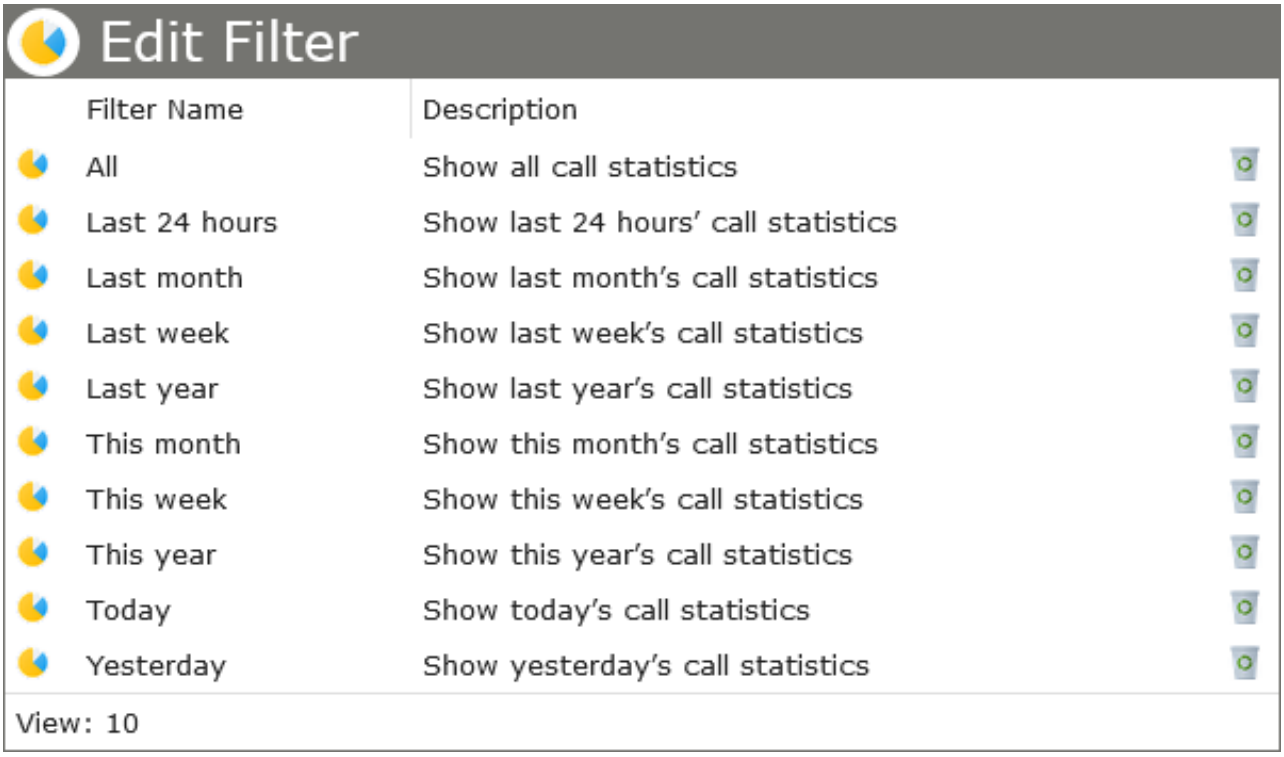
By clicking Add, the parameter will be added to the list. Only data entries that match *all* filter criteria will be included in the output (*AND relation*). Parameters can be deleted by clicking the *recycle* icon.





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

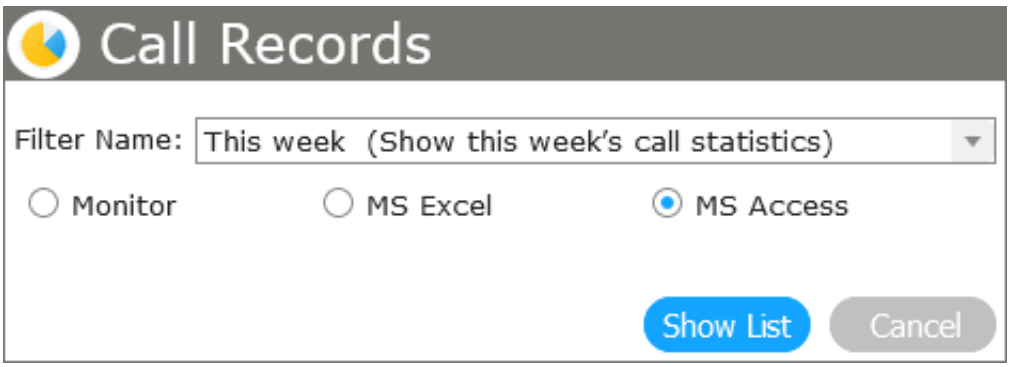
Clicking the button Save stores the new filter and makes it available to all authorized users.



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.



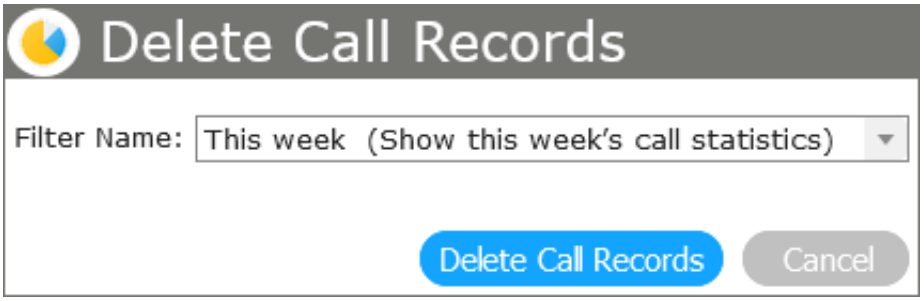
The following data will be listed:

- 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

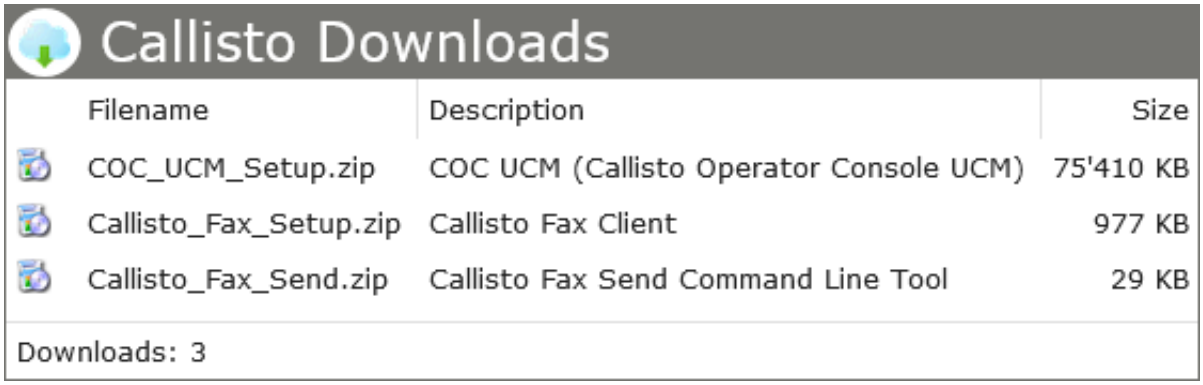
The Downloads menu provides access to all available Callisto downloads. Those can be installed on client PCs by administrators.

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

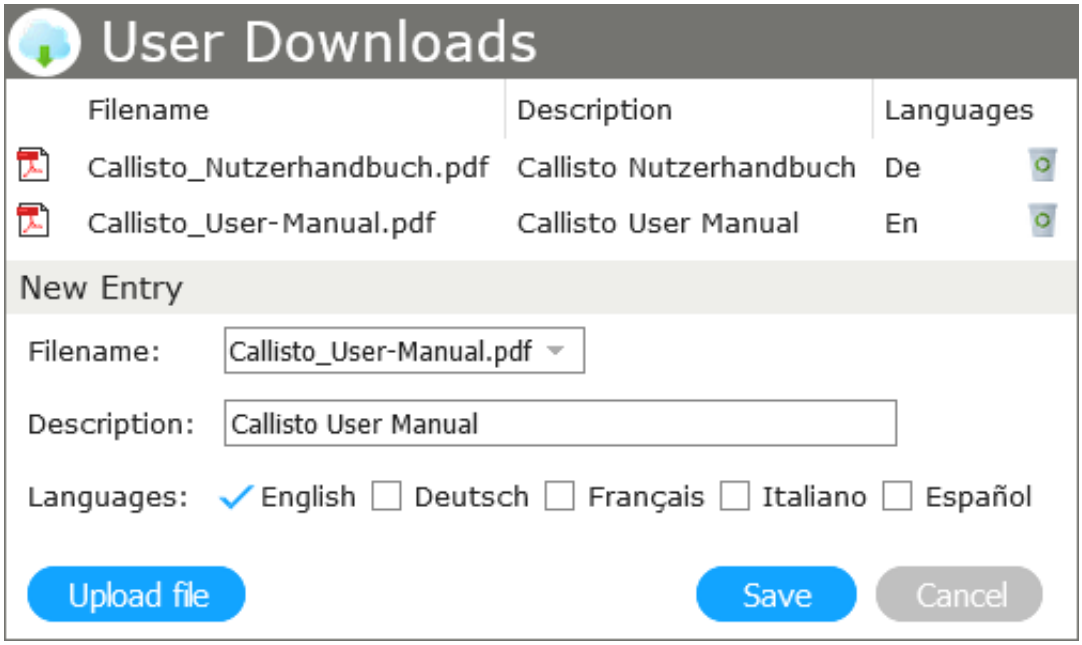


In the menu Downloads > Callisto Downloads, you'll find application installers, e.g. for the fax client or the Callisto Operator Console, depending on the edition of the Callisto Platform and what options are enabled.

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.

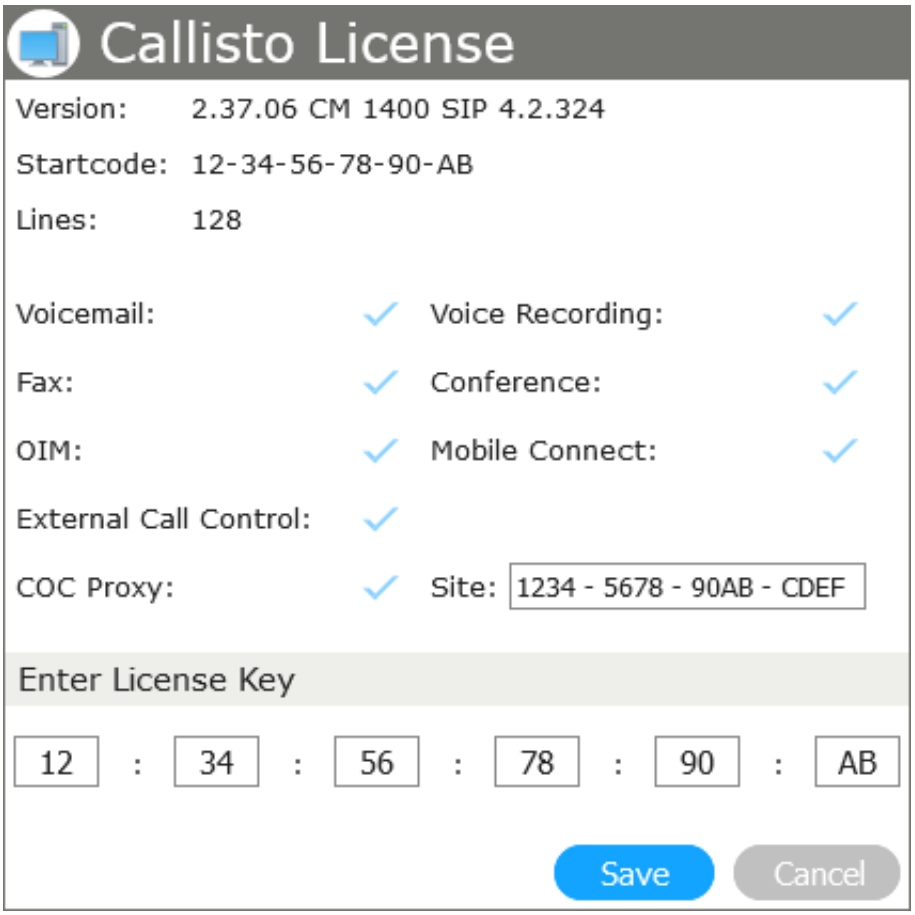
To upload a file, click on Upload File. After the upload is finished, select the file from the drop-down menu to set a Description and check the Languages the file is intended for. The file will only be visible to clients who set their web GUI in a language that you've enabled here.

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

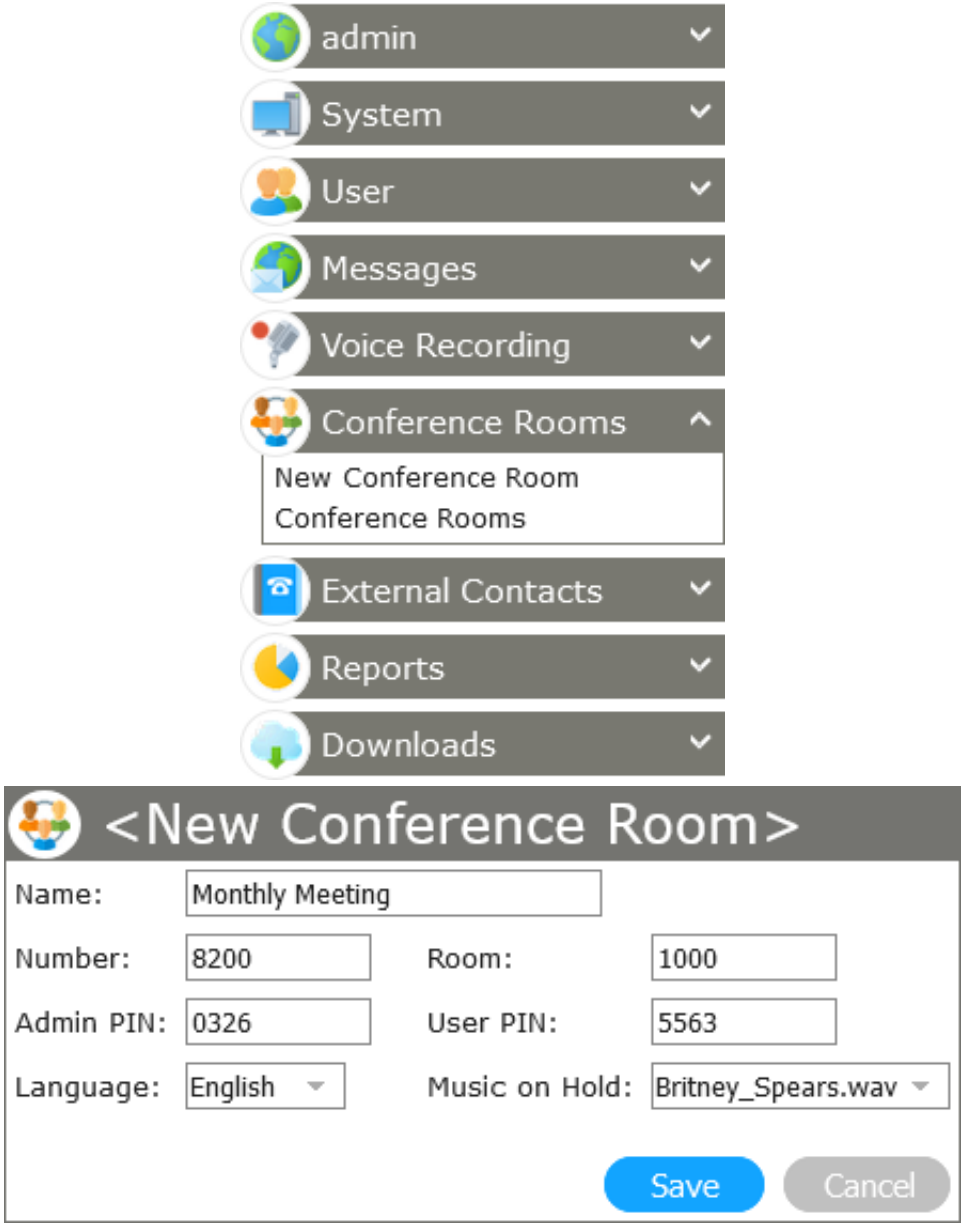
After activating the *COC Proxy Service* option,the configuration of COC Express needs to be updated: Instead of the Cisco UCME IP address, enter the IP address of the Callisto Platform.

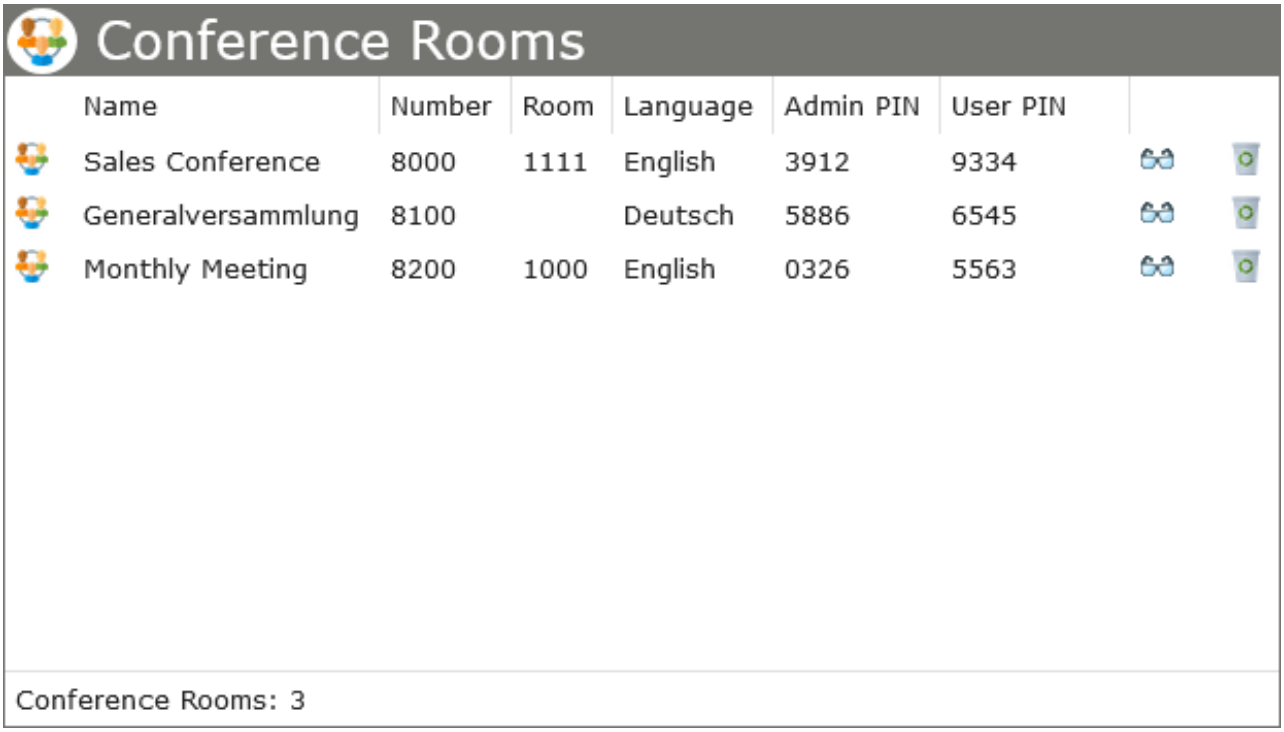
If you use a COC multi-user solution, the site license needs to be added to the Callisto configuration. This way, all installed workstations will be centrally activated through Callisto?eliminating the need for any additional or individual license registrations (see Option “COC Proxy Service”).

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.

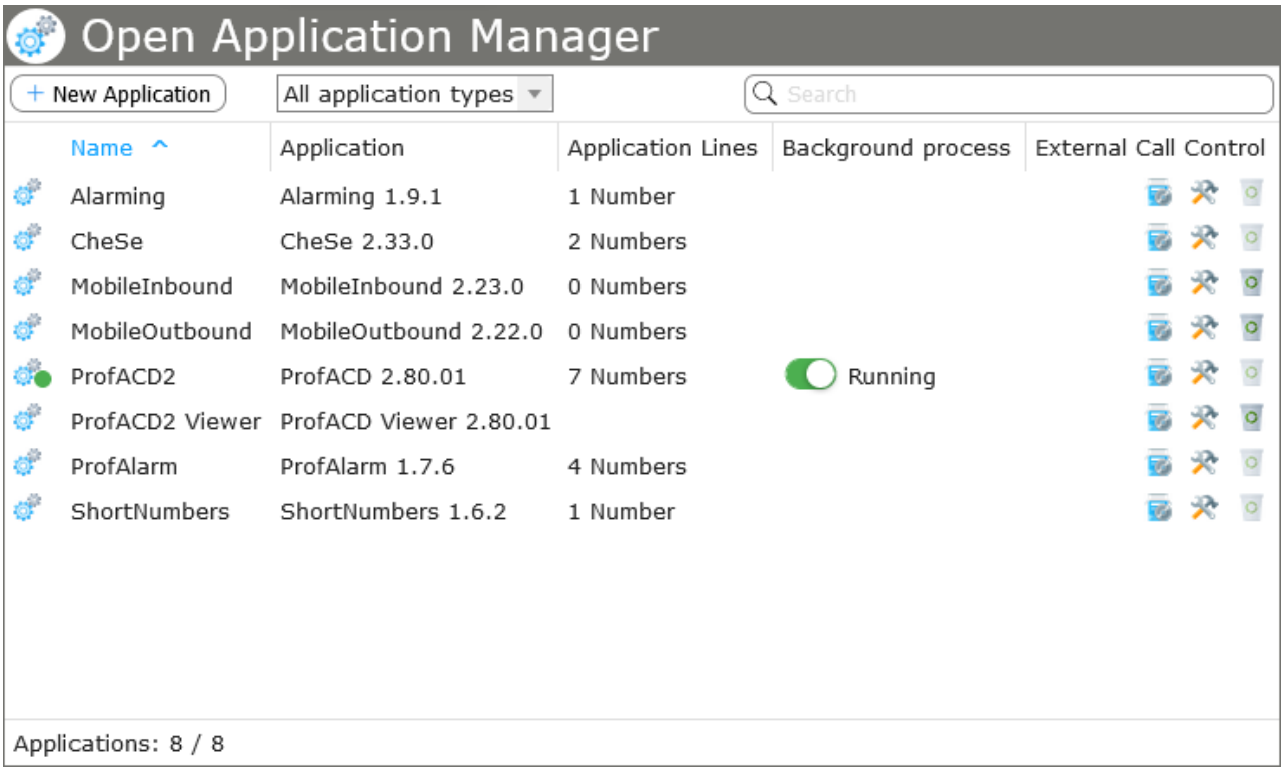
Option “Open Application Manager”

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

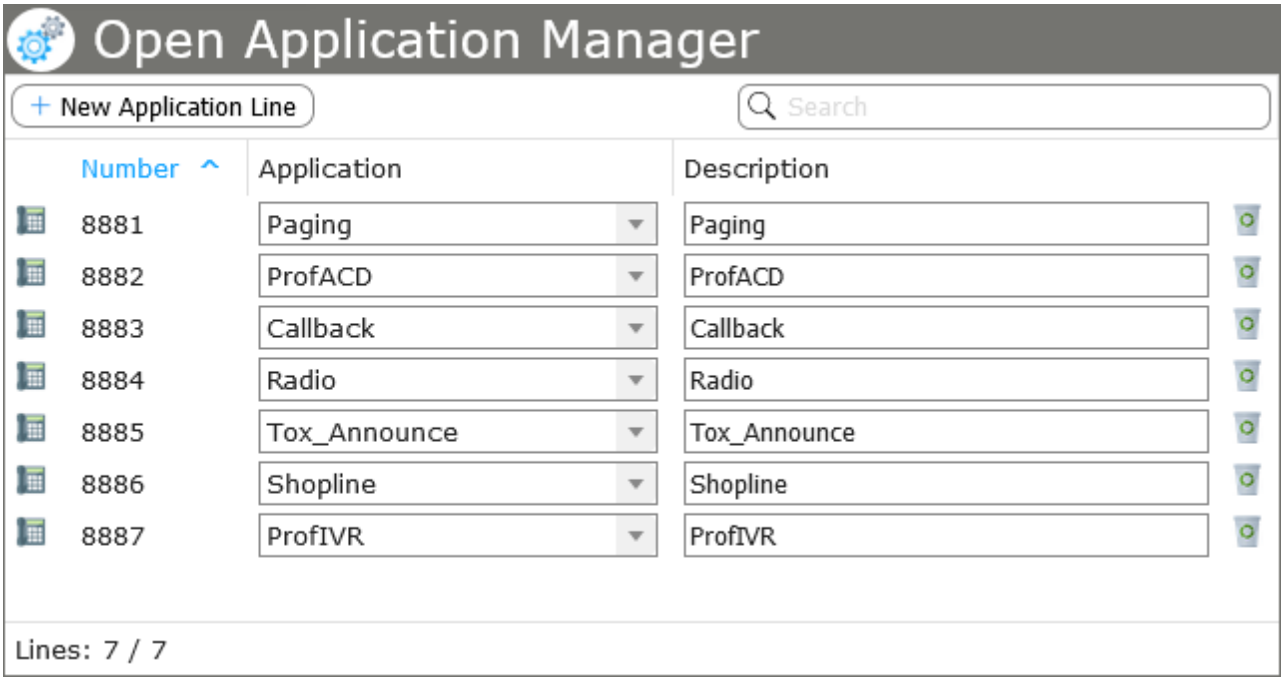
Configure

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.

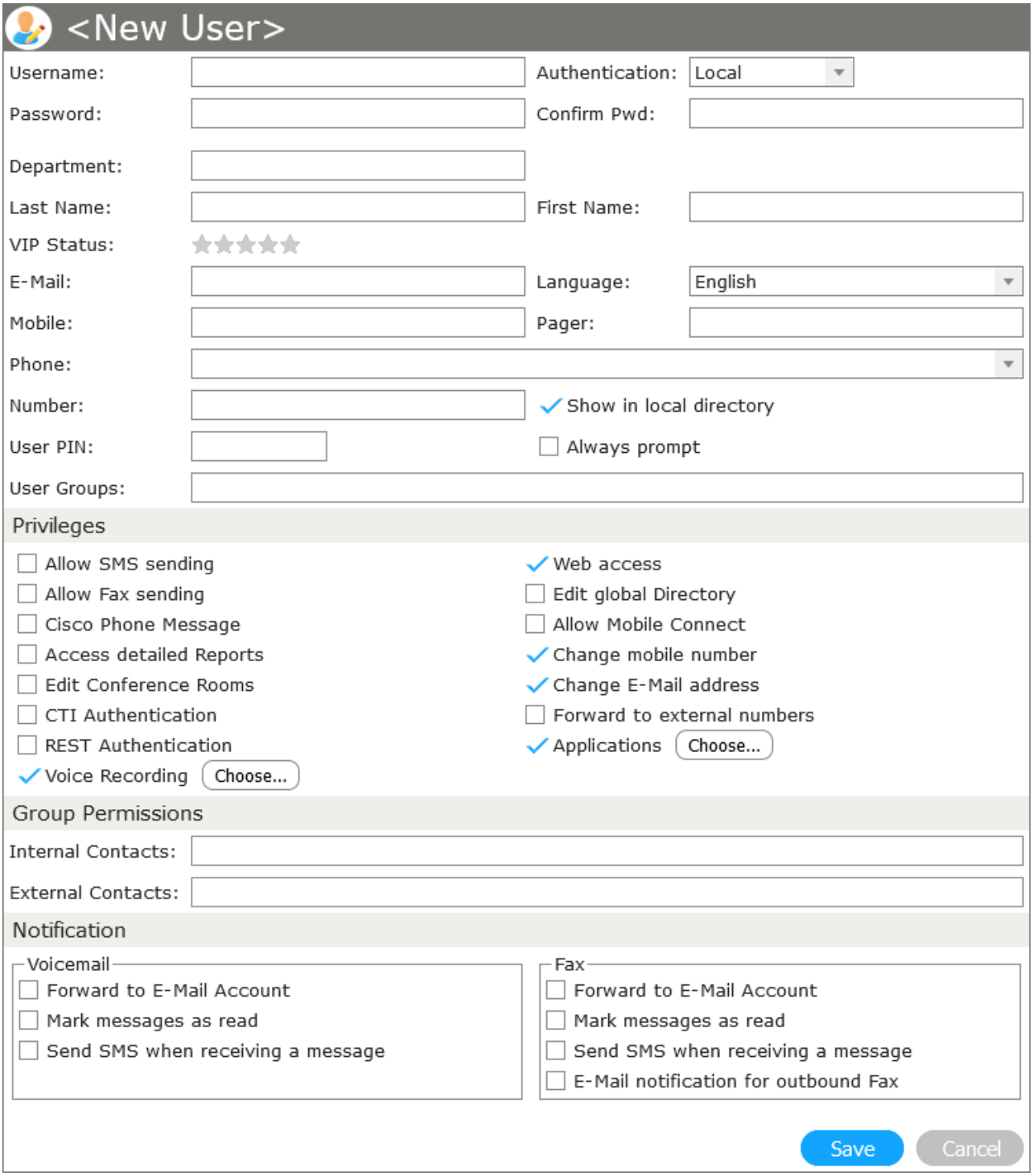
Option “Mobile Connect”

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”

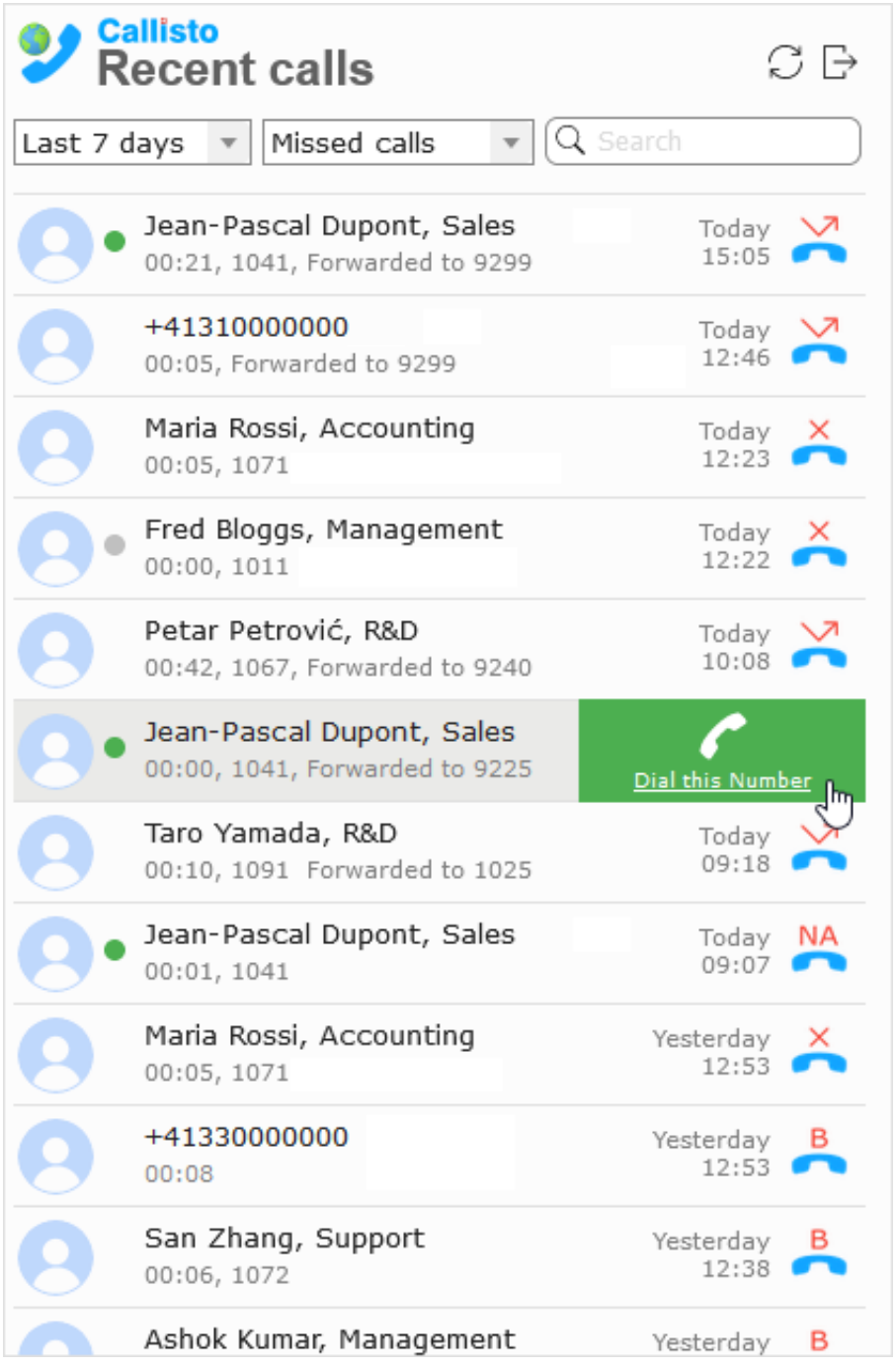
See the External Call Control administration manual.

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

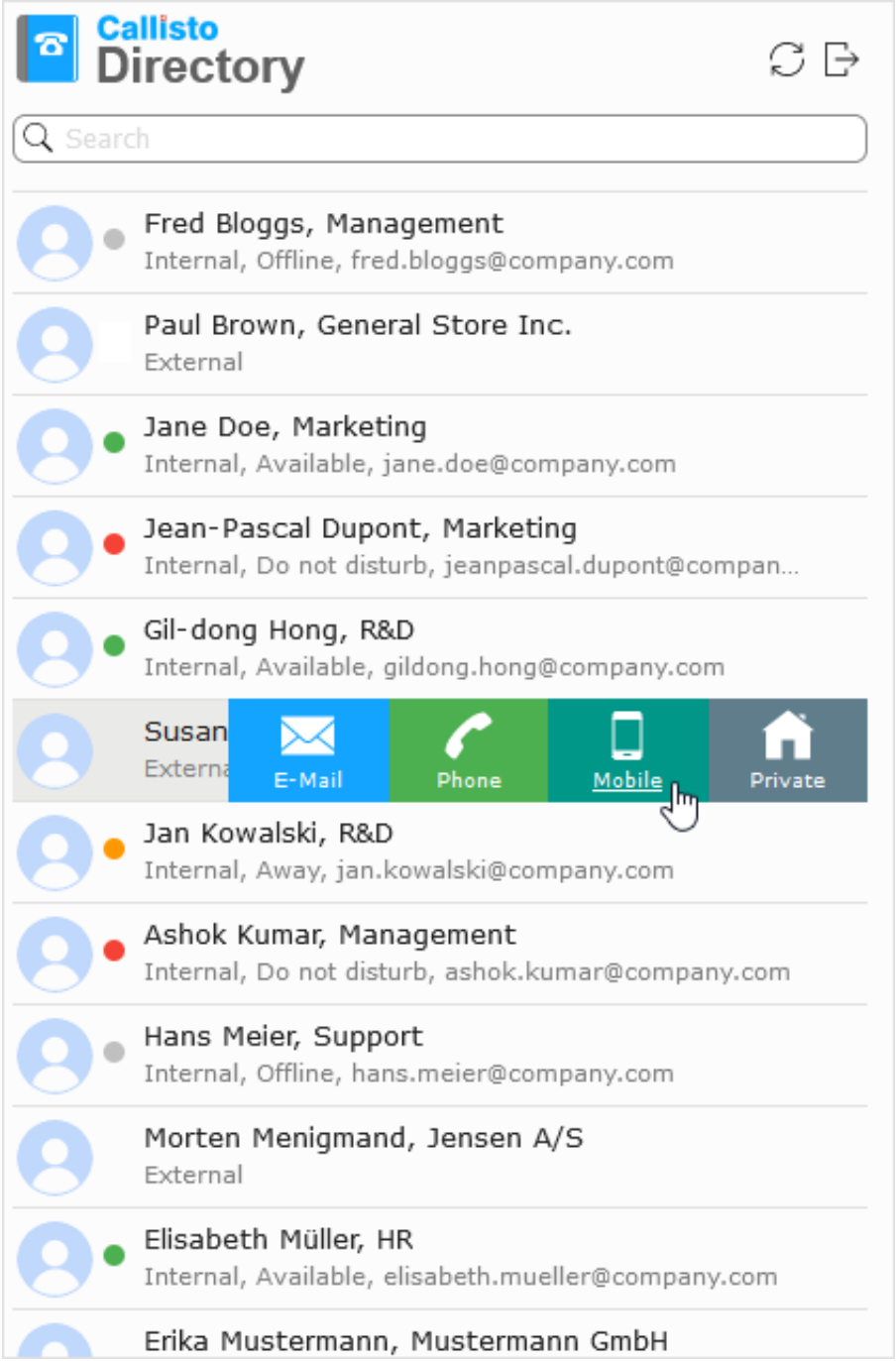


Recent calls shows the following call types:

	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

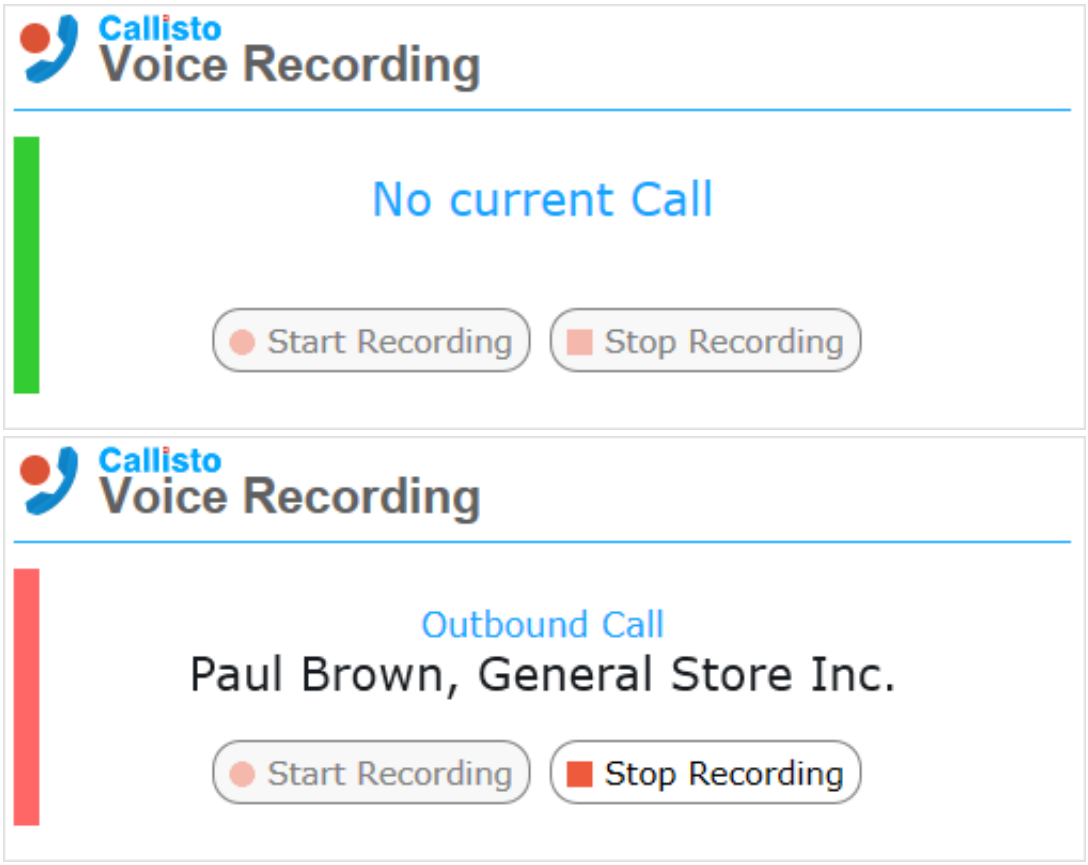


The search function will show results from both internal and external contacts saved in your Callisto directory. For more details on available search operators, refer to the quick reference.

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

Voice Recording

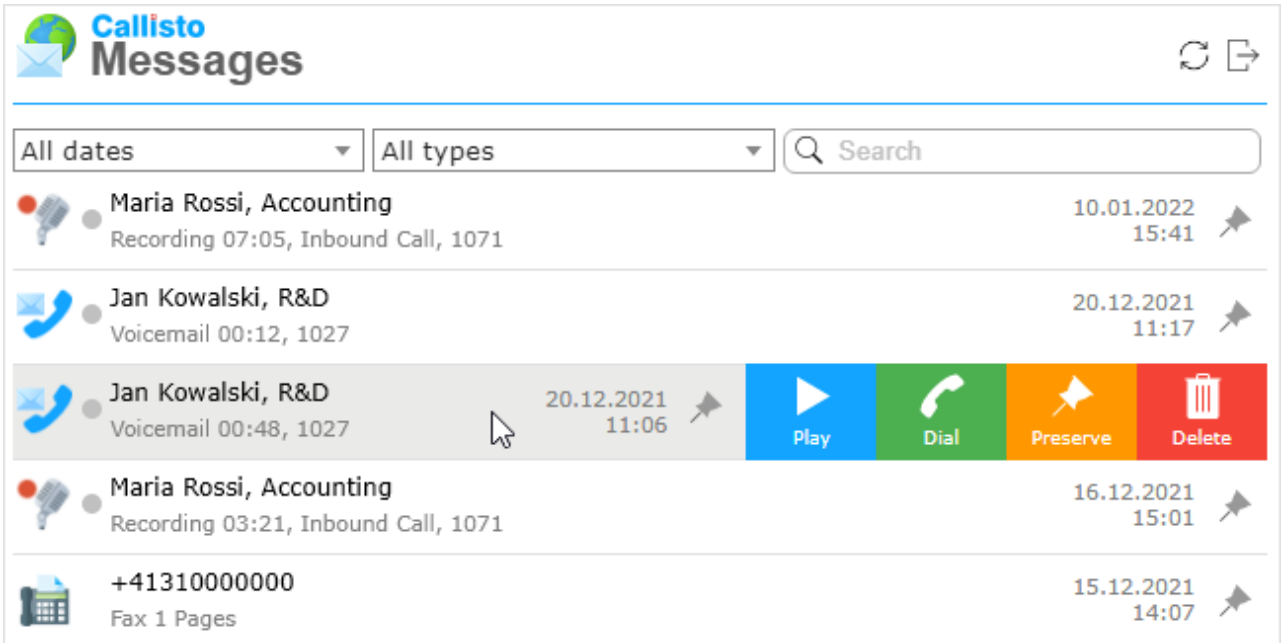
The URL of this gadget is: http://<*callisto*>/Jabber/Recording/Recording.asp



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.

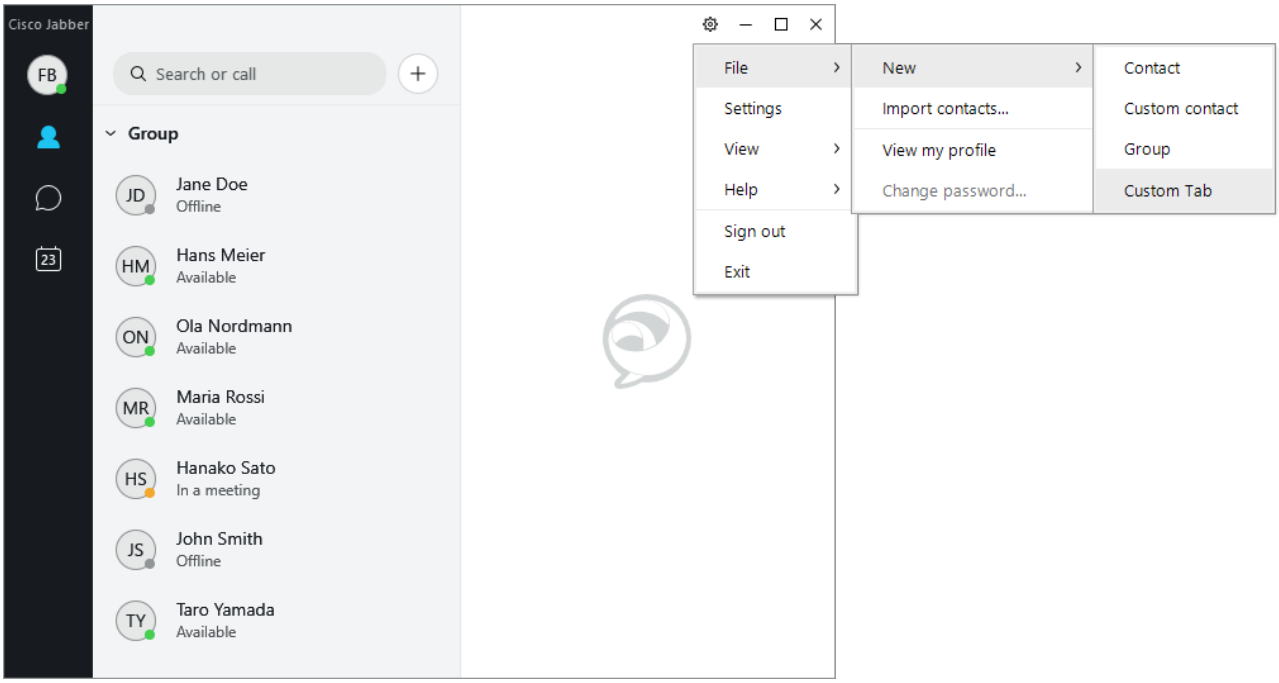
If you use one of the other two authenentication methods, the URLs to be used are identical to the ones described in the section Standalone page.

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

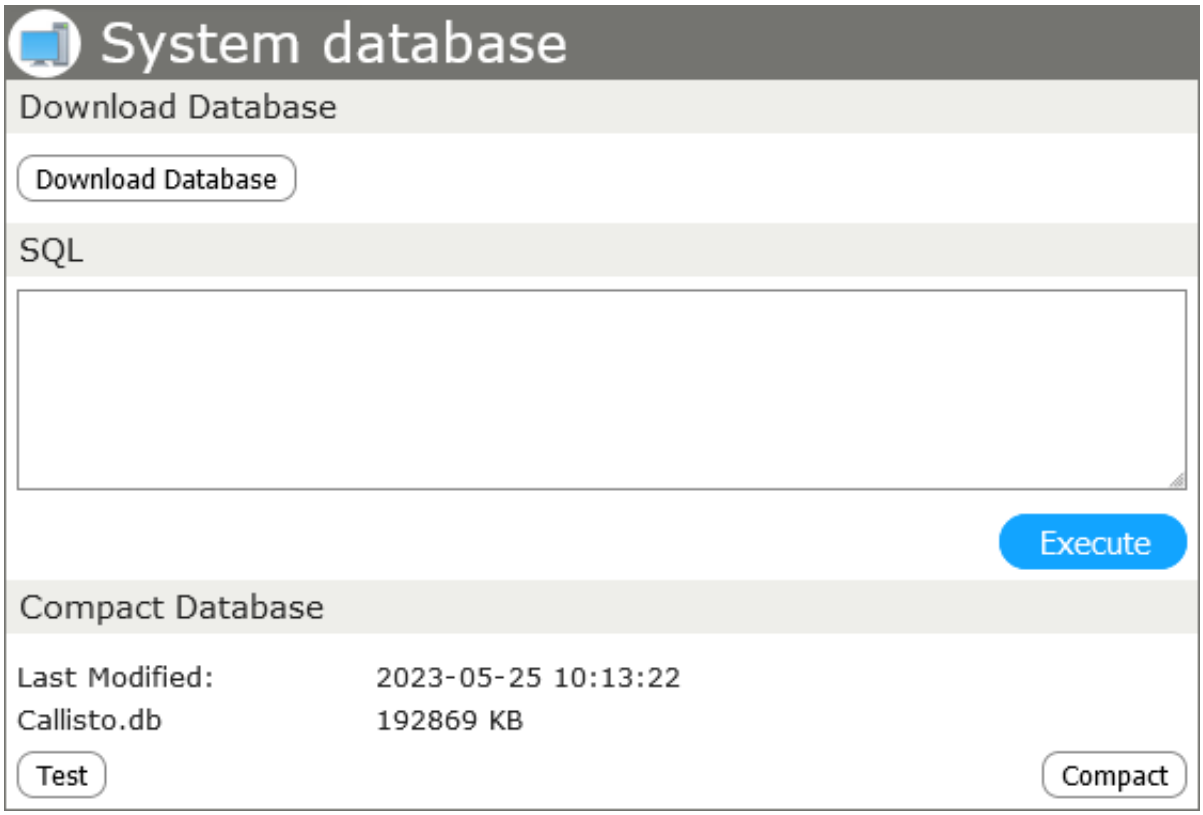
The Callisto concept ensures a maintenance-free system for years. In the unlikely event of a system failure, CTModule differentiates between services within a defined warranty period and those outside a defined warranty period.

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.

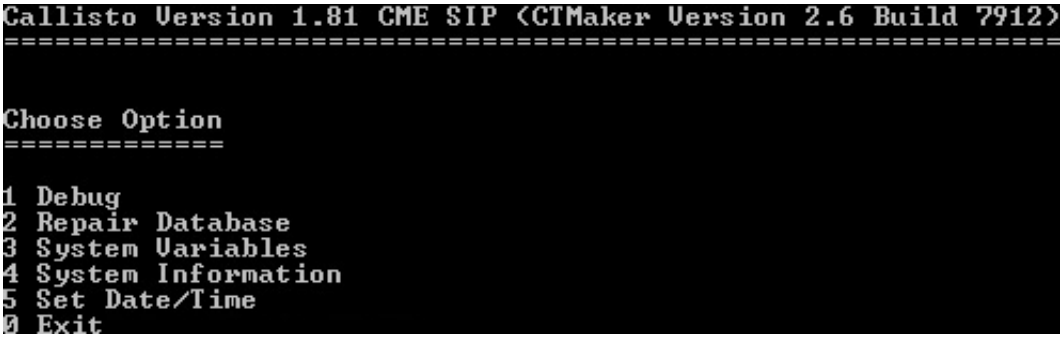
If you experience any problems, contact your Callisto dealer or follow the instructions according to the Callisto GTC and/or SLA. In case of software and/or configuration problems, you might be requested to activate trace logging, which is described in detail in the following section.

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.

Copyright

Copyright © 2026 CTModule AG; All Rights Reserved

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

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

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

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

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

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

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

Disclaimer

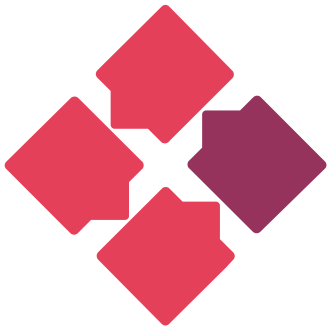
Changes are possible without notice.

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

All rights reserved.

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

www.ctmodule.com



CTMODULE

COMMUNICATION TECHNOLOGY MODULES

CTMODULE AG

Lehnweg 1

CH-3123 Belp/Berne

Switzerland

T: +41 (0)31 531 11 11

F: +41 (0)31 531 11 12

sales@ctmodule.com

OFFICE GERMANY

Frankfurter Straße 92

D-65760 Eschborn/Frankfurt

Germany

T: *+49 6196 2049173-0*

F: *+49 6196 2049173-9*

sales-d@ctmodule.com

OFFICE SERBIA

Gospodara Vučića 145

RS-11000 Belgrade

Serbia

T: +381 18 308076

sales@ctmodule.com