CALLISTO

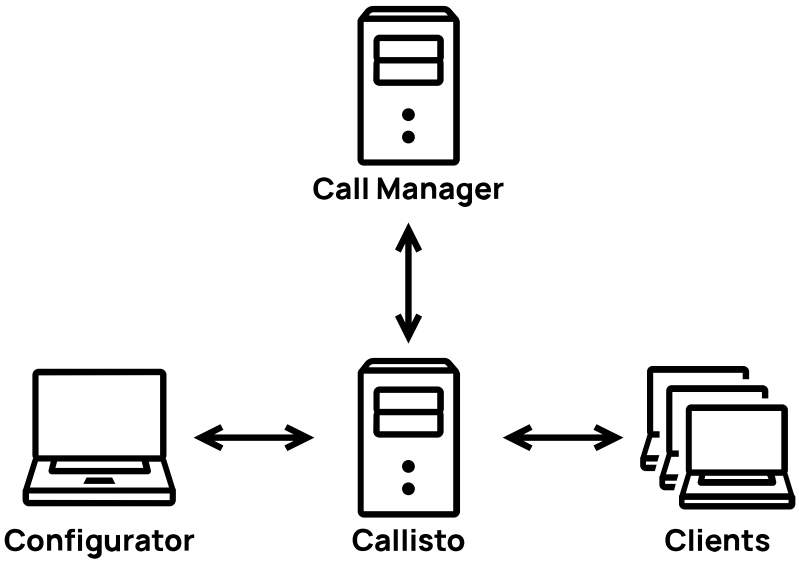
# CALLISTO OPERATOR CONSOLE

SETUP MANUAL

Table Of Contents

**Setup manual** ..... 3
- System overview ..... 3
- Installation ..... 4
- Call Manager configuration ..... 6
- NEC 3C configuration ..... 9
- Exchange configuration ..... 12
- Proxy licenses ..... 13
- Copyright Information, Disclaimer ..... 14

# System overview




COC Proxy UCM is part of Callisto. It is the software needed for communicating with the Call Manager, the COC Client and the COC Configurator.

The COC Configurator has to be installed on the administrator’s PC and the COC Client on the PCs of each end user.

# Installation

## Installing COC Configurator

The COC Configurator allows administrators to configure COC Proxy and the roles and permissions for the COC Client.

### System requirements

| | |
|---|---|
| Operating system | Windows 2008/10 Server, Windows 7 or higher |
| RAM | 2 GB or more |
| CPU | dual core or more |
| Cisco Call Manager | version 7 or higher |

To install the COC Configurator on a client PC, run COC_Configurator_Setup.exe and follow the installation wizard through the installation.

## COC Client

### System requirements

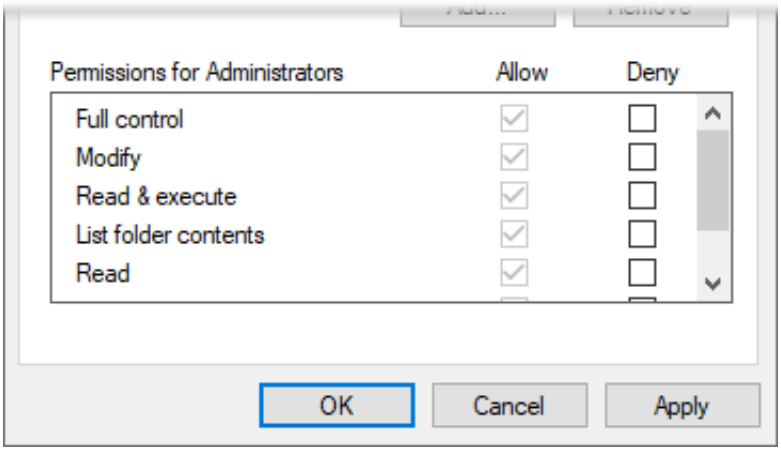
| | |
|---|---|
| Operating system | Windows 10 or higher |
| RAM | 2 GB or more |
| CPU | dual core or more |

To install the COC Client (i.e. the Operator Console itself) on a client PC, run COC_Client_Setup.exe and follow the installation wizard through the installation.

The COC Client setup requires an internet connection to download and install one of the required components. In case there is no internet connectivity on the PC, you need to download the WebView2 runtime standalone installer (available from the CTModule website) after installing COC.

Once this file is downloaded, unzip it and open WebView2InstallerX64.exe to start the installation. If COC is already installed on the PC, make sure COC has been shut down completely before installing WebView2.

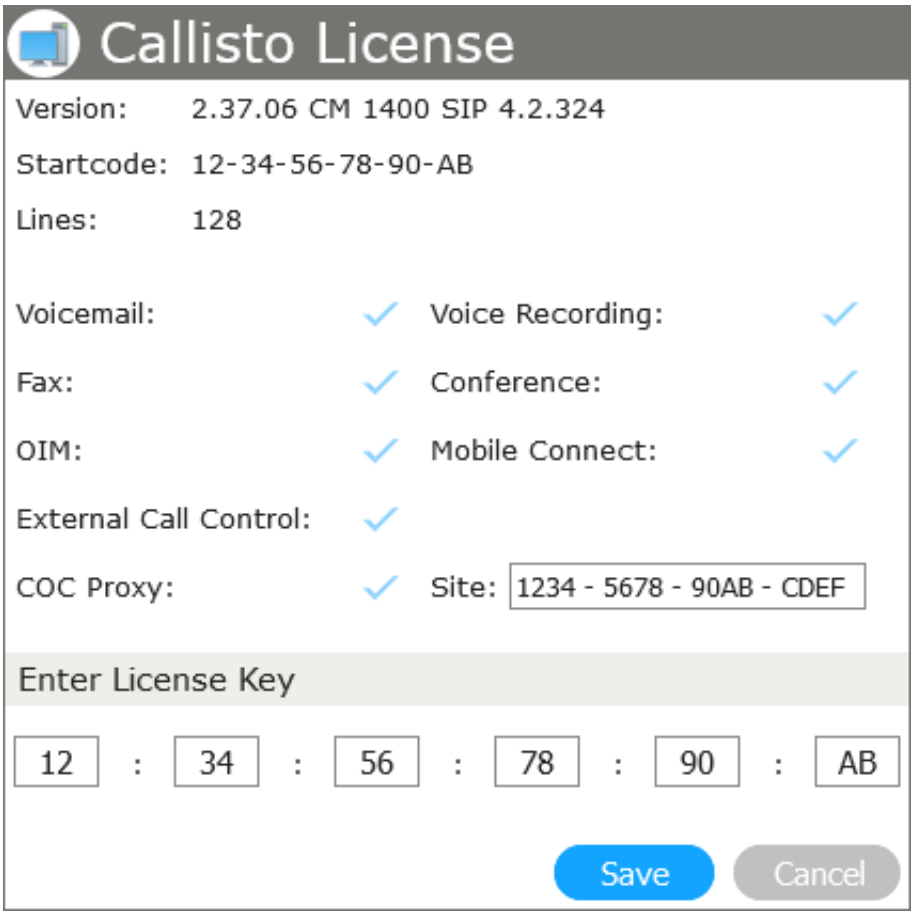
Once the WebView2 installation is finished, locate the directory <*user directory*>\Documents\CTModule\COC\ and check the permissions for the folder EBWebView by right-clicking it and choosing Properties > Security > Edit…. The currently logged-in user needs full permissions on this folder.




Once all permissions are granted, start the COC Client. It uses the Microsoft Edge WebView2 framework to display the HTML-based content.

## Product license

The software will be licensed through Callisto. Inside Callisto, choose System > Callisto License and verify that COC Proxy is enabled with the license entered in the Site field.



# Call Manager configuration

The COC Proxy UCM communicates with the Call Manager through AXL and JTAPI (CTI). For the communication with JTAPI (CTI), an application user must be created on the Call Manager.

## User group

Before configuring the Call Manager to work with COC, a user group must be created. This user group should include all the roles required when operating with COC. In the Call Manager, choose User Management > User Group, then click on Add New to add a new user group. Enter a name for the user group and click Save. Display the overview of user groups by choosing User Management > User Group, then select the name of the user group you just created. Certain roles must be assigned to this user group. Click on the *information* icon under Roles to assign roles to the user group.

The following roles must be assigned:

| Role | Description |
|---|---|
| Standard AXL API Access | This role only needs to be added if the credentials for the assigned application user and the administrator are the same, needed to allow access to the AXL database API. |
| 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. |
| 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 Enabled | Enables CTI application control |
| Standard CTI Allow Call Recording | Enables Call Recording |
| Standard CTI Allow Call Monitoring | Enables Call Monitoring |

## Application user

In the Call Manager, choose User Management > Application User. Then click on Add New to add a new application user, or click on the user name of an existing application user to edit it. When adding a new application user, enter and confirm a user password. Under Permissions, add the user group created above to this application user. Under Device Information, in the list box Available Devices, select all the devices that should be controlled by COC, then click on the *down arrow* button to move those devices to the Controlled Devices list box.

## Parking

To configure the parking functionality to work on COC, at least one *Call Park* number should be available. To create one, click on Call Routing, then click on Add New. On the Call Park Number Configuration dialogue, configure the respective parking numbers so that the calls can be parked on this parking slot. For details on configuring this page, please check the Cisco documentation about Call Park.

## Busy queue

To configure the Busy Queue functionality in order to work correctly on COC, at least one *CTIPort* device with directory number should be available. To create one, choose Phones and click on Add New. In the Phone Type menu, select CTIPort. After creating the phone, add a DN to it. In the Line configuration, locate

the fields Maximum Number of Calls and Busy Trigger; Set 200 calls for both.

## Call recording

Call recording functionality is available with CUCM version 9 and later.

To use call recording, the *Standard CTI Allow Call Recording* role needs to be added to the application user group (see above).

To add an application user to this group, choose User Management > Application User, click on the Find button and then click on your application user. In the Permissions Information section, click the Add to Access Control Group button. A new window will pop up. Click on the Find button and check the checkbox next to Standard CTI Allow Call Recording. Click on the Add Selected button on the bottom of the page.

Afterwards, call recording is enabled for your application user. The option Built-in Bridge must be enabled on the agent's phone.

## Silent monitoring and coaching

In order to enable the call monitoring feature, some configurations are needed on the CUCM.

1. The *Standard CTI Allow Call Monitoring* group must be added to the application user. Choose User Management > Application User, click on the Find button and then click on your application user. In the Permissions Information section, click the Add to Access Control Group button. A new window will pop up. Click on the Find button and check the checkbox next to Standard CTI Allow Call Monitoring. Click on the Add Selected button at the bottom of the page.
2. After adding this group, the Built-in Bridge option needs to be enabled. It should be enabled on both the supervisor's and the agent's phone.
3. Check the CSS/partition setting on the phones/lines. All phones involved in the monitoring and coaching feature should be reachable among each other.
4. Assign the desired CSS in the Monitoring Calling Search Space on the supervisor's phone line.

After these steps, the call Monitoring feature will be enabled for your application user.

## Presence (CUPS)

### Presence with REST

To enable REST API based presence in COC, follow these steps:

1. Specific roles need to be assigned to the application user. Choose User Management > Application User and select the application user which is used for Callisto. In the Permissions Information section, click the Add to Access Control Group button. A new window will pop up. Click on the Find button and check the checkbox next to Admin-3rd Party API.
2. The *End user* for presence needs to be enabled. Choose User Management > End User and choose any end user. In the Service Setting section, check the Enable User for Unified CM IM and Presence option. Repeat this for every user that is supposed to use presence.
3. If your CUPS is integrated with Exchange, enable Include meeting information in presence too.
4. The following ports should be opened:
    a. 8843 – incoming
    b. 8082 – incoming and outgoing
    c. 8083 – incoming and outgoing
5. If COC Proxy was running during the configuration above, restart COC Proxy.

### Presence with SIP

In order to use the SIP SIMPLE presence integration interface, you need to add the  Callisto IP to the

incoming ACL on CUPS:

1. Go to the CUPS administration page
2. Navigate to System > Security > Incoming ACL
3. Click on Add New
4. In the Address Pattern filed, enter the Callisto IP address

In order to enable end users for presence, follow steps 2 and 3 from the REST section. On the Callisto machine, make sure that port number 27865 is open.

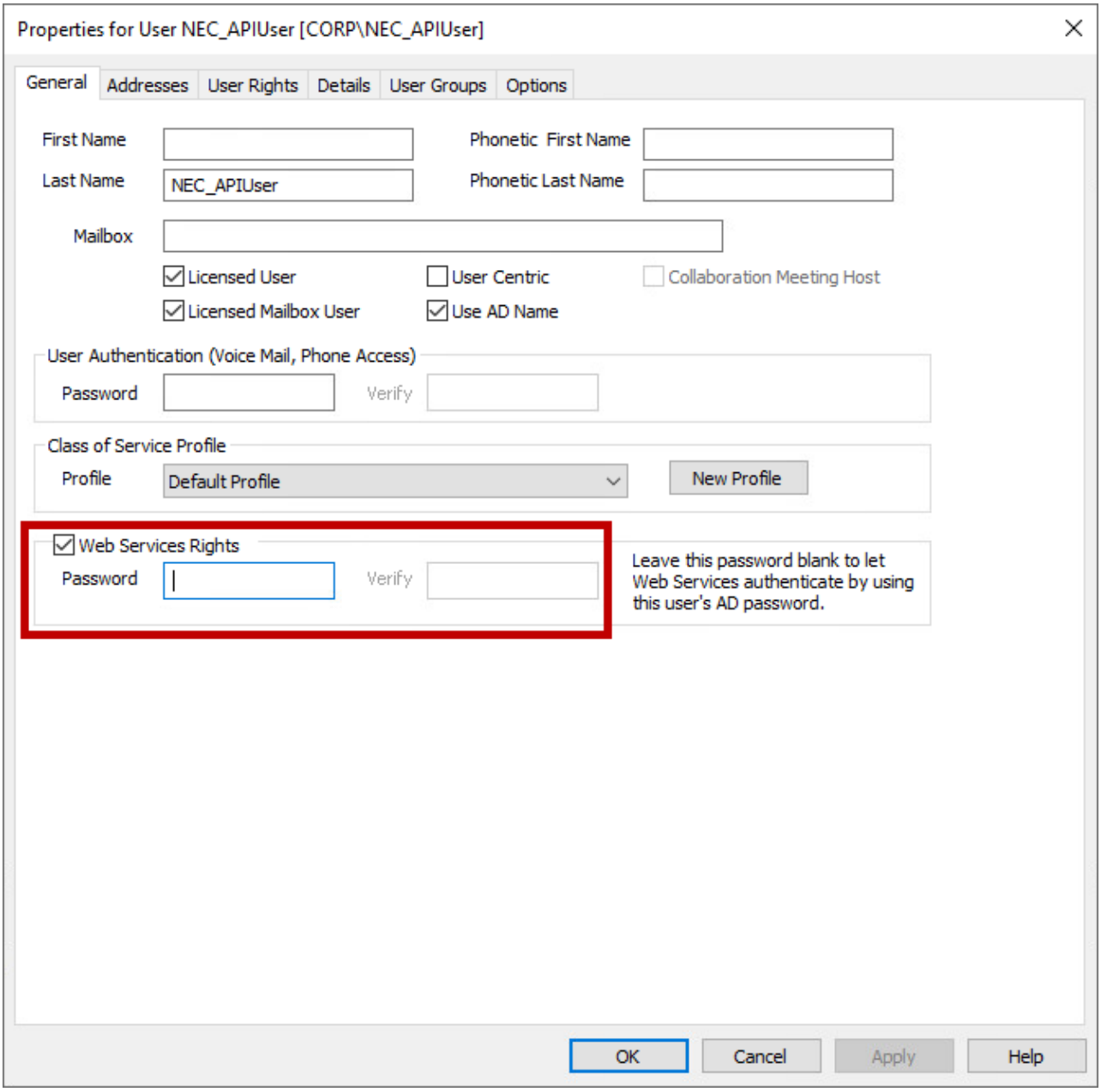
# NEC 3C configuration

The COC Proxy facilitates communication with the NEC 3C system through its SOAP API.

## Application user

To establish the communication channel, it’s necessary to create an application user on the NEC 3C server.

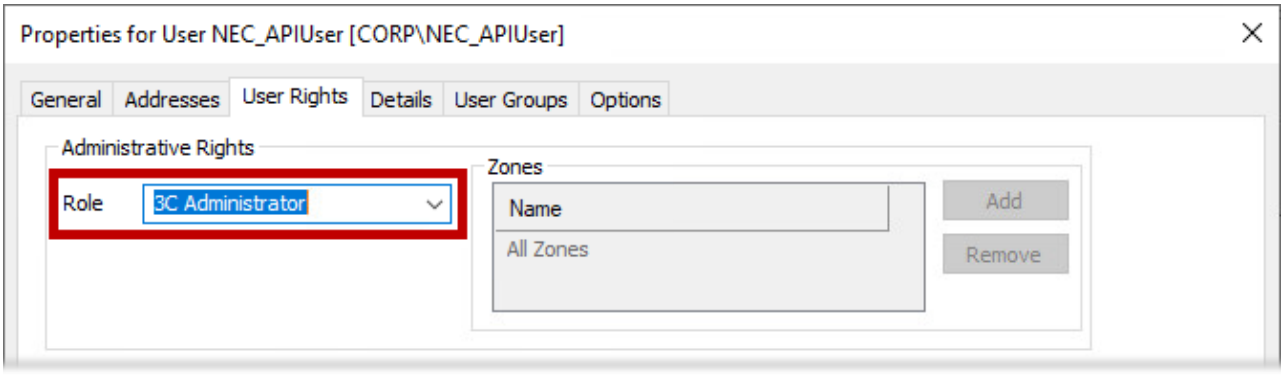
1. Access the 3C Administrator interface.
2. Navigate to the Users tab.
3. Look for an option to create a new user, labeled Add User.
4. Fill in the required details for the new user, such as username, password, and any other necessary information.
5. After creating the user, navigate to the General tab.
6. Ensure that the Web Services Rights option is checked.
7. Save the changes.




Your newly created application user can now be used in the NEC 3C system.

The following steps will show you how to grand administrator privileges to an application user.

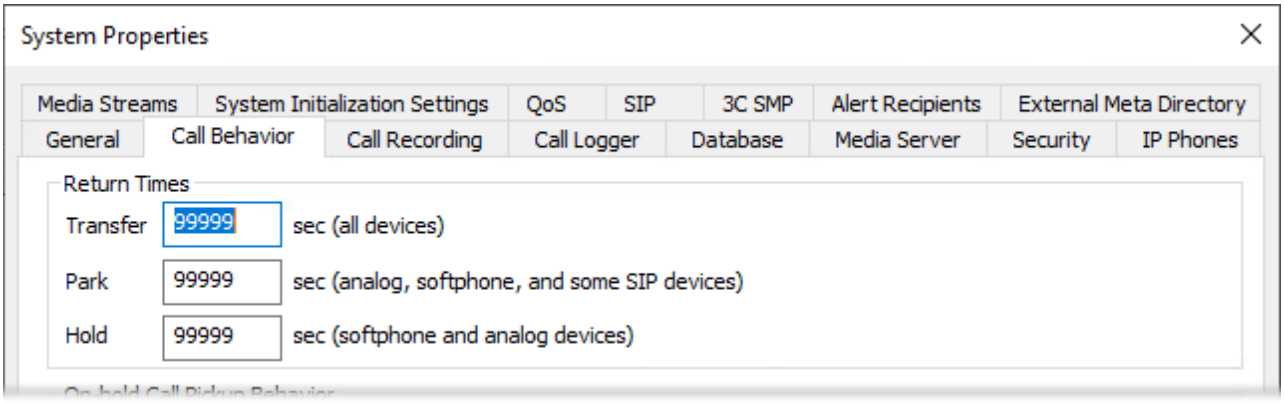
1. Navigate to the User Rights tab.
2. In the User Rights section, locate the Administrative Rights section.
3. From the Role drop-down menu, select 3C Administrator to assign administrator privileges to the user.
4. Save the changes.




## Call behavior return times

Return times are handled on the side of Callisto, so it's recommended to set the return times to the maximum value on the side of 3C for optimized operation.

1. Access the 3C Administrator interface.
2. Navigate to the General tab.
3. Open the System properties.
4. Navigate to the Call Behavior tab.
5. In the Return Times section, set the timeout settings to the maximum allowed value.



# Exchange configuration

COC allows the integration with Exchange to synchronize the presence states of the users with their Exchange availability. In order to do so, COC needs to connect to a specific Exchange user with the rights to observe the other users' calendars. The following steps lead you through . First, you'll have to create a new user (in this example named COC_Calendar) in Active Directory and create a mailbox in Exchange.

You also have to configure the rights on Exchange to configure what information can be seen by other users. You can set the same rights for all the users through the following shell command:

```
$users=Get-Mailbox -resultsize Unlimited
ForEach ($user in $users) {Add-MailboxFolderPermission -Identity
$user":\Calendar" -user COC_Calendar -AccessRights LimitedDetails}
```

You can also set the rights for each user individually through the following shell command:

```
Add-MailboxFolderPermission -Identity exchange-
user:\Calendar -User COC_Calendar -AccessRights LimitedDetails
```

:\Calendar is the location and name of the calendar folder. The name of the calendar folder is language dependent, so it might be different in the language your Exchange installation is set in. COC_Calendar is the name of the user that was added. exchange-user is the name of the user whose access rights you want to set.

In case the Exchange is reporting an error despite settings being set correctly, it is suggested to try accessing the WSDL file of the Exchange Web Service via your web browser. To do so, enter the following URL: https://<*Exchange IP*>/ews/Exchange.asmx, where <*Exchange IP*> is the Exchange address configured on the COC Configurator. Use the same credentials configured on the COC Configurator to access to this file. The COC Proxy should be able to access to this file in order to connect with Exchange.

# Proxy licenses

COC proxy works on user-based licensing, meaning one device will be associated with one user. For example, if you have 10 user licenses then you can incorporate 10 devices as well as 10 Callisto CTI lines. If you add more devices or CTI lines than available licenses, a warning message reading “License exceeded” will appear in the COC Configurator. To remove the warning message, remove any devices or CTI lines that exceed the number of licenses.

If you change the amount of devices, a restart of the proxy is required to make the new status active. If this is not possible, you can alternatively remove all devices from the device list and then assign the correct number of devices again.

If you need to use more devices or lines that your current amount of licenses allows, you can purchase additional license keys from CTModule.

# 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

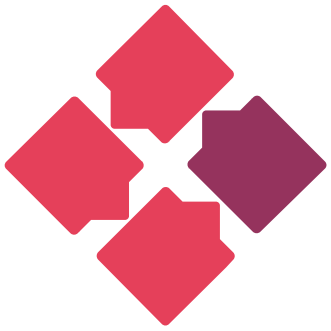
Changes are possible without notice.

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