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.