# Cisco Meeting Server

## Quick Reference Guide

### Using ActiveControl in Meeting Server conferences

03 March 2023

# Contents

# What's changed

| Version | Change |
| --- | --- |
| May 10, 2021 | Minor edit. |
| August 21, 2020 | Updated for 3.0 and web app. |

# 1 Introduction

Cisco Meeting Server offers meeting participants the ability to control their meeting experience directly from their conferencing endpoint through a feature called ActiveControl.

ActiveControl enables run-time meeting features for users, such as, meeting rosters (participant list), muting participants, dropping participants, changing video layout and more, directly from their endpoint.

To use ActiveControl requires the following in your deployment:

- The endpoint supports ActiveControl
- The call path between the endpoint and Meeting Server supports iX media end to end
- Appropriate permissions to be enabled in Meeting Server

This guide covers the configuration and dependencies for ActiveControl with Cisco Meeting Server.

In addition to ActiveControl, the Cisco Meeting Server web app has a set of meeting and space controls that are similar, but separate from the ActiveControl functionality in Meeting Server. Web app's functionality is described in the section, " Cisco Meeting Server web app controls" on page 14 of this guide.

## 1.1 About the ActiveControl Feature

ActiveControl is a set of features negotiated between the Call Bridge and Cisco endpoints to enable users to control their meeting experience without the need for external applications or operators. ActiveControl utilizes the iX media protocol in Cisco devices and is negotiated as part of SIP messaging of the call.

ActiveControl was originally launched for the Cisco TelePresence Server but has since been reworked for newer platforms such as Cisco Meeting Server (Meeting Server) and Webex Meetings. The specific functionality and configuration depend on the meeting service in use. This guide will focus only on the ActiveControl implementation for Meeting Server. For information on using ActiveControl with Webex Meetings, refer to this article.

The main features enabled by ActiveControl with Meeting Server are as follows:

- Viewing a list of all participants (known as roster list or participant list) connected to the meeting
- Muting or unmuting other participants
- Adding or removing another participant from the meeting
- Starting or Stopping Recording of a meeting

- Making a participant important
- Indicator for the participant who is the active speaker in the meeting
- Indicator for the participant who is currently sharing content or presentation in the meeting
- Locking or unlocking of the meeting
- Layout control

---

**Note:** The actual features available in your deployment can vary based on endpoint type and software versions in use.

---

**Note:** Participant list is also known as the roster list. It shows the names of all the people in the call.

---

# 2 Supported Endpoints

ActiveControl for Cisco Meeting Server is supported with the following endpoints:

- Cisco DX-Series, SX-Series, Room Kit, Room Kit Pro and all endpoints based on these codecs running software CE8.3 or later.
- Cisco Jabber release 12.5 and later.

Cisco Meeting Server web app has a set of in-meeting controls which are different to ActiveControl. For more information, see " Cisco Meeting Server web app controls" on page 14.

The following section details the feature support and requirements for the different endpoints.

## 2.1 Cisco Endpoints

This section applies to all Cisco Endpoints running CE software version 9.6.2, including the DX-Series, SX-Series, Room Kit, Room Kit Pro and all endpoints based on these codecs using the Touch10 controller. By default, ActiveControl is enabled in these endpoints.

To configure this setting from your endpoint, open **Configuration** > **Conference** > **ActiveControl Mode**.

ActiveControl features are accessed via the Touch10 controller or DX Touchscreen interface.

**Note:** The features supported with different versions of endpoint software may vary slightly, Cisco recommends using the latest version of endpoint software for the best experience.

### 2.1.1 List of features supported with software version CE9.6.2

| Feature | Support | Notes |
|---|---|---|
| Meeting Roster (Participant list) | Yes | |
| Mute Remote Party Audio | Yes | DTMF option available |
| Unmute Remote Party Audio | Yes | DTMF option available |
| Video Layout Control | Yes | DTMF option available |
| Add Participant | No | Available as an experimental feature |
| Drop Participant | Yes | |
| Record Meeting Controls | Yes | DTMF option available |
| Stream Meeting Controls | No | DTMF option available |

| Feature | Support | Notes |
|---|---|---|
| Record/Stream Indicator | Yes | Icon is displayed on screen. |
| Lock/UnLock Meeting | No | DTMF option available |
| Set/Unset Importance | No | |
| Roster Show Speaker Indicator (Active speaker indicator) | Yes | |
| Roster Show Content Contributor (Indicator to show who is sharing content) | Yes | |
| Participant Count | Yes | |
| Local Mute by ActiveControl | Yes | Server and Local Mute are coupled and follow each other |
| Local UnMute by ActiveControl | No | An on screen notification displays when user is no longer remotely muted. |
| Encrypted iX media support | Yes | Requires a TLS secured registration and call path end to end |
| Message Text | Yes | On screen message notifications are shown |

Note that availability of a particular feature may still be limited by the Meeting Server's configuration for a participant. See the " Cisco Meeting Server Configuration" on page 9 for more details.

## 2.2 Cisco Jabber

Support for ActiveControl in Jabber was introduced in Jabber version 12.5 on all supported platforms. Jabber requires Cisco Unified Communications Manager version 10.5 or later for ActiveControl support.

Jabber does not require any configuration on the client-side to enable ActiveControl, but iX media must be enabled in the SIP profile assigned to the user's device in Unified CM.

## 2.3 Features supported with Jabber 12.5

Table 1:List of features supported with Jabber 12.5:

| Feature | Support | Notes |
|---|---|---|
| Meeting Roster (Participant list) | Yes | |
| Mute/Unmute Remote Party Audio | Yes | DTMF option available |
| Video Layout Control | Yes | DTMF option available |
| Add Participant | Yes | |
| Drop Participant | Yes | |
| Record Meeting Controls | Yes | DTMF option available |
| Stream Meeting Controls | No | DTMF option available |
| Record/Stream Indicator | Yes | |
| Lock/UnLock Meeting | Yes | DTMF option available |
| Set/Unset Importance | No | |
| Roster Show Speaker Indicator (Active speaker indicator) | Yes | |
| Roster Show Content Contributor (Indicator to show who is sharing content) | Yes | |
| Participant Count | Yes | |
| Local Mute by ActiveControl | Yes | Server and Local Mute are coupled and follow each other |
| Local UnMute by ActiveControl | Yes | Server and Local Mute are coupled and follow each other |
| Encrypted iX media support | Yes | |
| Message Text | No | Meeting Server embeds as part of video stream |

Note that availability of a particular feature may still be limited by the Meeting Server's configuration for a participant. See " Cisco Meeting Server Configuration" on page 9 for more details.

# 3 Call Control and Trunks

To use ActiveControl, the full call path between the Meeting Server and the endpoint must support iX media in the SIP messages. Any proxy, firewall, or back-to-back user agent (B2BUA) in the path that blocks or interferes with the iX messaging will cause ActiveControl to not negotiate.

When enabling ActiveControl in your deployment, verify that the iX protocol is supported on trunks between the Meeting Server and endpoints.

The following sections detail the steps to enable ActiveControl for Cisco Expressway, Cisco VCS, and Cisco Unified Communications Manager. Please refer to the section appropriate for your deployment.

## 3.1 Cisco Unified Communications Manager

ActiveControl is compatible with Cisco Unified Communications Manager (Unified CM) versions 9.1.2 and later. iX protocol should be filtered or disabled on any trunks routing to instances running versions older than the supported versions.

The iX protocol may be disabled by default in Unified CM depending on the SIP profiles and Unified CM versions in use. Newer Unified CM versions have the iX protocol enabled by default in SIP profiles labeled for TelePresence use. Common profiles used for Jabber may have the setting disabled by default. iX media must be enabled in each of the SIP profiles used by your devices and all trunks that Telepresence calls will traverse.

Verify all SIP Profiles used by TelePresence Endpoints, Jabber Devices, and SIP trunks.

### 3.1.1 Enabling or verifying the SIP Profile iX media setting

To enable the iX media setting, follow these steps:

1. In the Unified CM Administration web interface, Choose **Device > Device Settings > SIP Profile**.
   The **Find and List SIP Profiles** window displays.
2. Locate the existing SIP profile in use for the trunk or device in question, enter the search criteria and click **Find**.
3. From the results, click the name of the SIP profile that you want to edit. The **SIP Profile Configuration window** displays.

4. Locate the **Allow iX Application Media** setting under **SDP Information** and ensure the checkbox is marked/enabled.


5. Click **Apply Config** to save your changes.

Restart any trunks or devices as necessary if changes to SIP profiles have been made

To filter or disable iX media on a trunk, edit the SIP Profile associated with the trunk and ensure the **Allow iX Application Media** setting is unchecked.

### 3.1.2 Encryption Considerations

Endpoints must use a secure SIP security profile to negotiate encrypted iX for calls. The call path must use TLS end-to-end for encrypted iX to negotiate. When not available, non-encrypted iX media can be negotiated.

### 3.1.3 MRA Considerations

Endpoints connected via Mobile Remote Access (MRA) will not support iX media and ActiveControl unless the Unified CM is in Mixed Mode security, and Unified CM uses a TLS connection to Expressway.

This limitation will be addressed in future releases of Unified CM and Cisco Expressway.

## 3.2 Cisco Expressway and Cisco Video Communication Server

ActiveControl is compatible with Cisco Expressway (Expressway) and Cisco Video Communication Server (Cisco VCS), version X7.2.3 and later. Support for iX is the same across both Cisco VCSand Expressway product variations. For simplicity, the term Cisco VCS refers to both Expressway and Cisco VCS in this document. iX protocol should be filtered/disabled on any trunks routing to instances running releases older than the supported versions.

In Cisco VCS, the iX protocol is allowed to pass through neighbor zones by default, unless it has been explicitly configured to be filtered with the SIP UDP/IX filter setting for the zone.

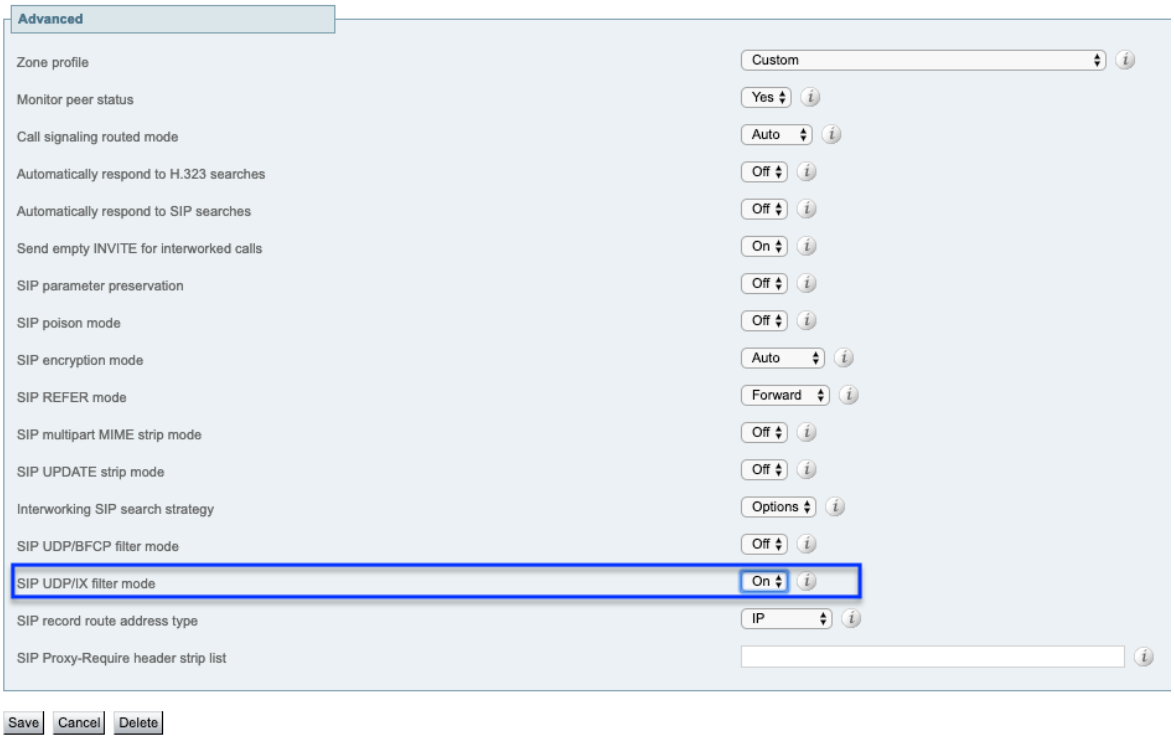
### 3.2.1 Verifying the iX Filter setting for Expressway

To configure the Cisco VCS to filter out the iX application line for a neighbor zone that does not support the protocol, the zone must be configured with a custom zone profile that has the SIP

UDP/IX filter mode advanced configuration option set to On.

To update advanced zone profile option settings:

1. In the Expressway web interface, navigate to **Configuration > Zones > Zones**.
2. Click on the name of the zone you want to view or edit.
3. Under the **Advanced** panel, if **Zone Profile** is set to **Default** or Cisco Unified Communications Manager, the SIP UDP/IX filter mode is assumed off and is not displayed.
4. To enable the filter, change the **Zone Profile** to **Custom** to view the advanced settings.
5. SIP UDP/IX filter mode controls filtering of iX media for this zone. Ensure it is set to **Off** to allow ActiveControl. Set to **On** if filtering iX to an incompatible neighbor.




   If you have changed the profile to custom and are saving changes, review the other **Advanced Settings** for applicability to the zone being edited.

6. Click **Save** to save the changes.

### 3.2.2 Encryption Considerations

Endpoints must register with TLS to negotiate encrypted iX for calls. The call path must use TLS end-to-end for encrypted iX. When not available, non-encrypted iX media can be negotiated.

## 3.3 Cisco Meeting Server Configuration

ActiveControl is supported in Cisco Meeting Server is enabled by default. While ActiveControl and negotiation is automatic; features available on an endpoint are still controlled by settings configured in Meeting Server's profiles. The profiles on Meeting Server must be configured before using ActiveControl features.

### 3.3.1 Meeting Server ActiveControl Features

Table 2:List of ActiveControl features for Cisco Meeting Server

| Feature | Support | Notes |
|---|---|---|
| Meeting Roster (Participant list) | Yes | |
| Mute/Unmute Remote Party Audio | Yes | DTMF option available |
| Video Layout Control | Yes | DTMF option available |
| Add Participant | Yes | |
| Drop Participant | Yes | |
| Record Meeting Controls | Yes | DTMF option available |
| Stream Meeting Controls | Yes | DTMF option available |
| Record/Stream Indicator | Yes | When supported, shown by endpoint, otherwise, shown in video stream by Cisco Meeting Server. |
| Lock/UnLock Meeting | Yes | DTMF option available |
| Set/Unset Importance | Yes | |
| Roster Show Speaker Indicator (Active speaker indicator) | Yes | |
| Roster Show Content Contributor (Indicator to show who is sharing content) | Yes | |
| Participant Count | Yes | |
| Local Mute by ActiveControl | Yes | |
| Local UnMute by ActiveControl | Yes | Endpoint controlled feature |
| Encrypted iX media support | Yes | |
| Message Text | Yes | When supported, shown by endpoint, otherwise, shown in video stream by Cisco Meeting Server. |

## 3.4 Cisco Meeting Server Profiles

By default, the participant permissions are generally disabled in Meeting Server. Before an ActiveControl feature is available to participants, the administrators must enable the feature through the API of the Meeting Server.

For SIP connected endpoints, permissions are controlled by the callLegProfiles setting in the API. A callLegProfile can be applied at the system-wide level, tenant level, space level, member or accessMethod level. The recommended best practice is to set the participant permissions you want as the baseline for your deployment at the system level. For more details on the Meeting Server API and how the object hierarchy is used, refer to the Cisco Meeting Server API reference guide.

The callLegProfile settings relevant to enable all ActiveControl features for SIP connected endpoints are listed below. To use a feature, the setting must be enabled for a participant. Alternatively, the settings can be applied to a system level callLegProfile so the settings apply by default to all participants.

Table 3:ActiveControl callLegProfile settings for SIP Participants

| callLegProfile Setting | Value to set | Notes |
|---|---|---|
| changeLayoutAllowed | true | Grants permission for changing layout for the participant themselves |
| disconnectOthersAllowed | true | Grants permission to Drop Participant from roster list (participant list) |
| addParticipantAllowed | true | Grants permission to Add Participant for ongoing call |
| muteOthersAllowed | true | Grants permission for Mute/Unmute Audio in roster list (participant list) |
| muteSelfAllowed | true | Grants permission for Server-side mute for themselves |
| callLockAllowed | true | Grants permission to lock/unlock the ongoing call |
| setImportanceAllowed | true | Grants permission to set/unset Importance for a participant in the roster list(participant list) |
| recordingControlAllowed | true | Grants permission for recording controls if recording is available for call |
| streamingControlAllowed | true | Grants permission for streaming controls if streaming is available for call |

## 3.5 Other Relevant Dependencies

### 3.5.1 Recording/Streaming

For recording or streaming controls to be available for participants, the following prerequisites must be met:

- recording or streaming must be configured for the Call Bridge
- the space must have an associated callProfile with the **`recordingMode`** set to **`manual`**.

### 3.5.2 Add Participant

ActiveControl can enable a participant to dial out to a new participant for the ongoing call, but for that call to be successful, the Outbound Call table in Meeting Server must be configured correctly with call control that can successfully connect to the requested URI.

### 3.5.3 Encrypted iX

To negotiate encrypted iX media, the Meeting Server must have SIP Media encryption enabled for the participant. When not available, Meeting Server will attempt to negotiate non-encrypted iX media which may impact the security status reported for a participant or conference.

SIP Media Encryption can be disabled in the Call Bridge settings from the Web Admin interface (From **Configuration > Call Settings**), or from the callLeg settings applied to a participant. Ensure that the SIP Media Encryption is not disabled for participants if encrypted iX is desired.

# 4 ActiveControl Feature Matrix

Table 4 provides a summary of ActiveControl features per device type. For more details on a device type, refer to the corresponding section in this guide.

Table 4:ActiveControl feature matrix

| | DX,SX,RK Endpoints CE9.6.2 | Cisco Jabber 12.5 | Meeting Server setting for ActiveControl | Notes |
|---|---|---|---|---|
| Meeting Roster (Participant list) | Yes | Yes | N/A - Automatic | |
| Mute/Unmute Remote Party Audio | Yes | Yes | muteOthersAllowed | DTMF option available |
| Video Layout Control | Yes | Yes | changeLayoutAllowed | DTMF option available |
| Add Participant | No | Yes | addParticipantAllowed | |
| Drop Participant | Yes | Yes | disconnectOthersAllowed | |
| Record Meeting Controls | Yes | Yes | recordingControlAllowed | DTMF option available |
| Stream Meeting Controls | No | No | streamingControlAllowed | DTMF option available |
| Record/Stream Indicator | Yes | Yes | N/A - Automatic | |
| Lock/UnLock Meeting | No | Yes | callLockAllowed | DTMF option available |
| Set/Unset Importance | No | No | setImportance | |
| Roster Show Speaker Indicator | Yes | Yes | N/A - Automatic | |
| Roster Show Content Contributor | Yes | Yes | N/A - Automatic | |
| Participant Count | Yes | Yes | N/A - Automatic | |

| | DX,SX,RK Endpoints CE9.6.2 | Cisco Jabber 12.5 | Meeting Server setting for ActiveControl | Notes |
|---|---|---|---|---|
| Local Mute by ActiveControl | Yes | Yes | muteSelfAllowed | |
| Local UnMute by ActiveControl | No | Yes | N/A - Automatic | |
| Encrypted iX media support | Yes | Yes | N/A - Automatic | |
| Message Text | Yes | No | N/A - Automatic | |

# 5 Cisco Meeting Server web app controls

Cisco Meeting Server web app offers in-meeting controls for participants to manage their meetings. A few of the meeting control options are similar to the features provided by ActiveControl for SIP. The key differences are as follows:

- web app's features and controls are not managed in the same way as ActiveControl for SIP participants.
- web app does not use iX media for its meeting controls.

The permissions that govern the meeting features in web app are a combination of the following:

- userProfile settings – The profile assigned to a user which controls more general user behaviors.
- space member permissions – The permissions assigned to the user within a particular space.
- callLegProfiles – Permissions applied to the participant as a combination of member, space, tenant, or system profiles.

## 5.1 Comparison of Meeting controls

Table 5 compares the ActiveControl options and settings to the meeting control features available in web app. The table also includes a columns for Meeting Server's callLegProfile settings relevant to a meeting feature, and a column to note any differences for a web app user joining as a guest user (not authenticated or joining spaces they are not members of).

Table 5: Meeting controls comparison

| Feature | Meeting Server's ActiveControl setting | web app equivalent? | Setting to control web app behavior | web appGuest user experience |
|---|---|---|---|---|
| Meeting roster (Participant list) | N/A - Automatic | Yes | Automatic | |
| Mute/Unmute Remote Party Audio | muteOthersAllowed | Yes | muteOthersAllowed | |
| Mute/Unmute Remote Party Video | Not Available | Yes | videoMuteOthersAllowed | |

| Feature | Meeting Server's ActiveControl setting | web app equivalent? | Setting to control web app behavior | web appGuest user experience |
|---|---|---|---|---|
| Video Layout Control | changeLayoutAllowed | Yes | Layout setting is local to Meeting App | |
| Add Participant | addParticipantAllowed | Yes | addParticipantAllowed | Not available to guests users |
| Drop Participant | disconnectOthersAllowed | Yes | disconnectOthersAllowed | Not available to guests |
| Record Meeting Controls | recordingControlAllowed | Yes | recordingControlAllowed | |
| Stream Meeting Controls | streamingControlAllowed | Yes | streamingControlAllowed | |
| Record Meeting Indicator | N/A - Automatic | Yes | N/A - Automatic | |
| Lock/UnLock Meeting | callLockAllowed | Yes | callLockAllowed | |
| Set/Unset Importance | setImportance | Yes | setImportance | |
| Active speaker (Roster Show Speaker) Indicator | N/A - Automatic | Yes | N/A - Automatic | |
| Roster Show Content Contributor | N/A - Automatic | Yes | N/A - Automatic | |
| Participant Count | N/A - Automatic | Yes | N/A - Automatic | |
| Local Mute by ActiveControl | muteSelfAllowed | Yes | N/A - Automatic | |
| Local UnMute by ActiveControl | N/A - Automatic | No | N/A – Local unmute controlled by client only | |
| Encrypted iX media support | N/A - Automatic | N/A | N/A | |
| Message Text | N/A - Automatic | No | N/A – web app does not support Message Text feature | |

| Feature | Meeting Server's ActiveControl setting | web app equivalent? | Setting to control web app behavior | web appGuest user experience |
|---|---|---|---|---|
| Manage guest access to a space | N/A – Not supported in ActiveControl | Yes | Guest access to a space can be managed through the user portal | Not available to guests |

# 6 Configuration Examples

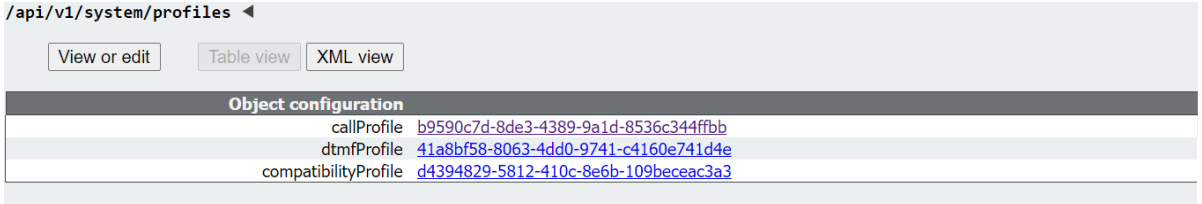
## 6.1 Enable ActiveControl Permissions in Meeting Server

This section gives an example of how to configure a system wide profile in Meeting Server to enable all ActiveControl features for participants.

Using the Web Admin interface of the Meeting Server, select **Configuration**>**API**:

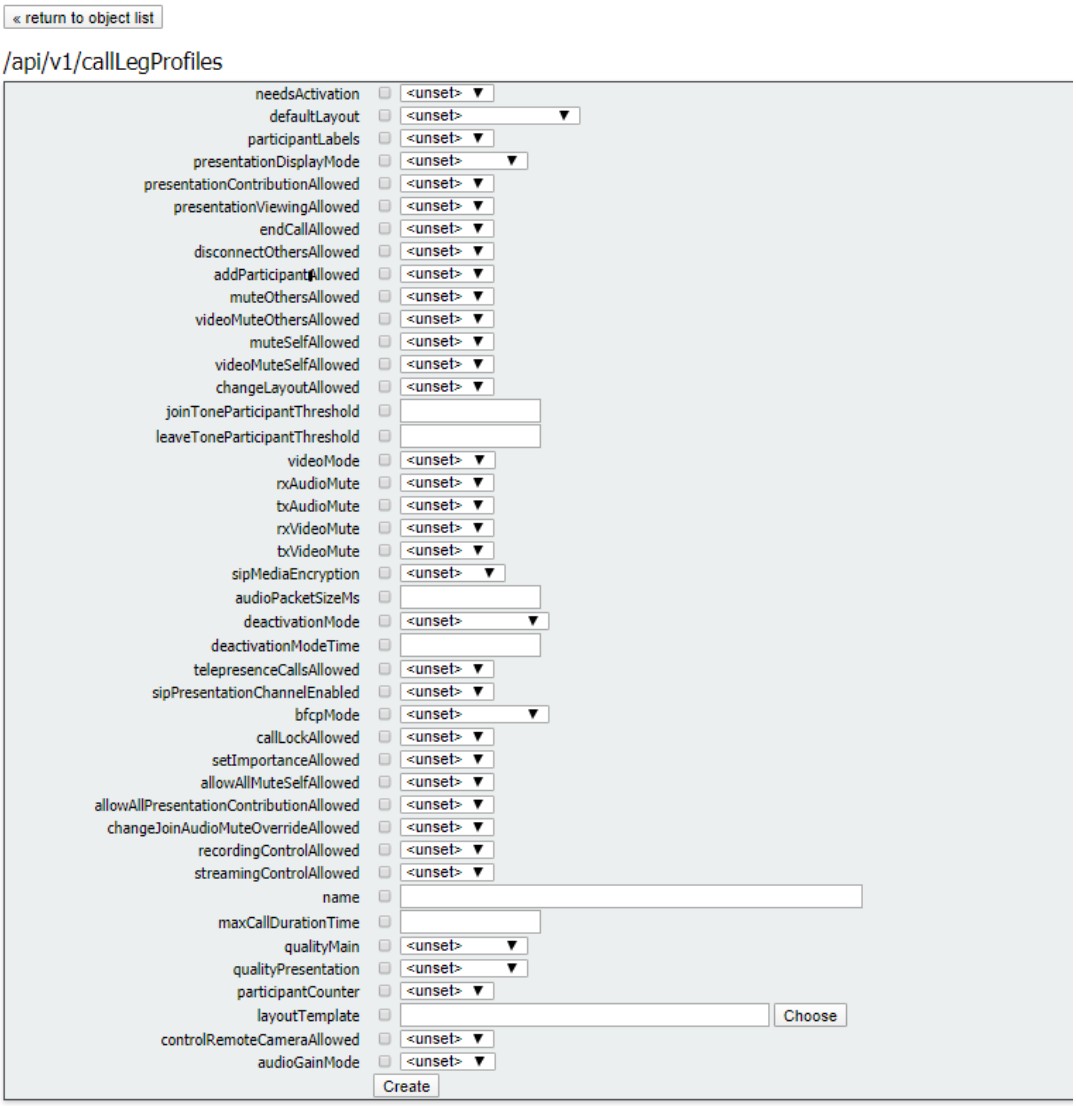
1. Check if there are any existing callLegProfiles applied at the system level – from the list of API objects, tap the ▶ after **/api/v1/system/profiles**

   Example output:

   The output in this example shows no callLegProfile listed, therefore a new callLegProfile can be created and applied.

2. Return to the list of API objects and from the list, tap the ▶ after **/callLegProfiles**
   a. Create a callLegProfile:
      i. Click the **Create new** button
      ii. Set the following parameters to **true** (includes all the permissions to enable ActiveControl on callLegProfile settings for SIP Participants as outlined in Chapter 3.4):
         - changeLayoutAllowed
         - **disconnectOthersAllowed**
         - **addParticipantAllowed**
         - **muteOthersAllowed**
         - **muteSelfAllowed**
         - **callLockAllowed**
         - **setImportanceAllowed**
         - **recordingControlAllowed**
         - **streamingControlAllowed**

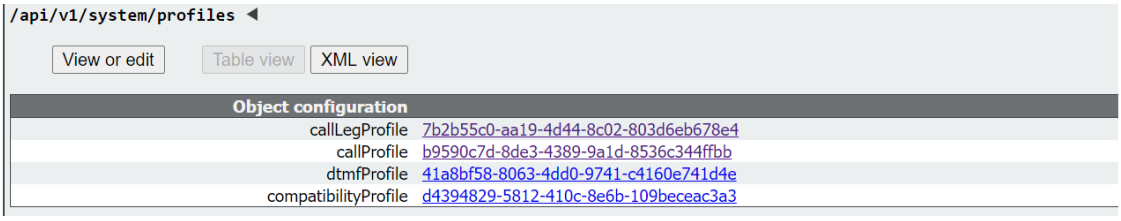



iii. Click **Create**

Retain a note of the **object id** of the newly created callLegProfile which you now need to apply at the system profile level.

3. Return to the list of API objects and from the list, tap the ▶ after **/api/v1/system/profiles**
4. Click **View or edit**, scroll down the parameters to **callLegProfile** and click **Choose**.
5. Select the **object id** of the new callLegProfile to use from the resulting dialog.
6. Return to the Web Admin page and click **Modify**.
7. The newly created callLegProfile should now be applied at the system/profiles level. To check, from the list of API objects, tap the ▶ after **/api/v1/system/profiles**

   Example output:

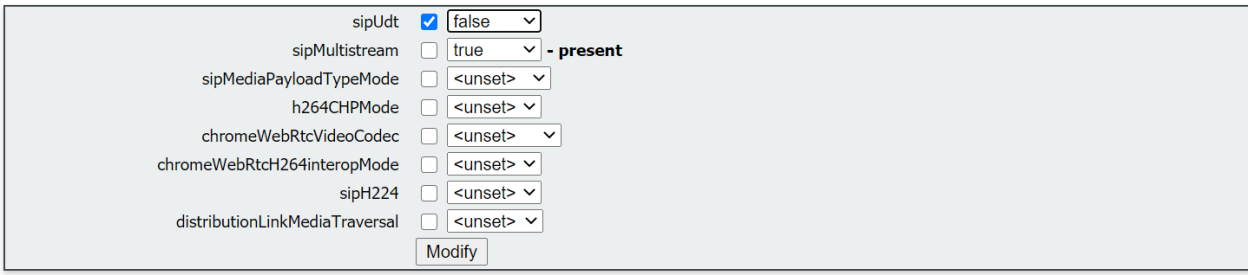



## 6.2 Turn off ActiveControl in Meeting Server

To turn off Active Control completely, set the **sipUdt** parameter to **false** in the active compatibilityProfile.

1. From the list of API objects, tap the ▶ after **/api/v1/compatibilityProfiles**
2. Select the **object id** of the active compatibilityProfile.
3. Set the the **sipUdt** parameter to **false** and click **Modify**.

/api/v1/compatibilityProfiles/84d4a889-da90-4384-9005-92a9435c76d7



# 7 ActiveControl Troubleshooting

## 7.1 General ActiveControl limitations:

Listed below are some ActiveControl limitations:

- ActiveControl is a SIP-only protocol and is not supported for inter working scenarios.
- Older SIP devices may not handle the iX SIP messages gracefully and may cause call failures if seen. Trunks to the following should have iX disabled to avoid interoperability issues:
    - Trunks to Unified CM servers running releases older than version 9.1.2
    - Trunks to VCS/Expressway servers running releases older than X7.2.3
    - Trunks to any external network or 3rd party call control device where call failures have been traced to iX protocol handling

## 7.2 Verifying ActiveControl negotiation in Meeting Server

If negotiated, ActiveControl will be shown in the following places:

- The call details of Status/Calls for the participant
- The callLeg API object for the participant

### 7.2.1 Meeting Encryption Status

When a participant negotiates ActiveControl and if iX is not encrypted, Meeting Server will report the participant as unencrypted. This non-encrypted user can lower the encryption status of the conference as seen by other endpoints.

## 7.3 Disabling iX in Meeting Server

ActiveControl uses the UDT transport protocol for certain features, for example sending roster lists (participant lists) to endpoints, allowing users to disconnect other participants while in a call, and inter deployment roster lists (participation lists). UDT is enabled by default. You can disable UDT for diagnostic purposes, for example if your call control does not use UDT, and you believe this is the reason the call control does not receive calls from the Meeting Server.

If necessary, disabling ActiveControl in Meeting Server can be done by disabling UDT in Meeting Server via the API. To disable UDT, follow these steps:

1. Create a compatibility profile with the parameter **`sipUdt`** set to *false* using the POST method (or modify an existing with PUT method) to **`/api/v1/compatibilityProfiles setting sipUdt=false`**.
2. Apply the newly created compatibility profile by setting the newly created profile at the system level. Use PUT method with **`compatibilityProfile=<compatibility profile id>`** to **`/api/v1/system/profiles.`**

## 7.4 iX troubleshooting

Table 6: Call handling summary for calls that contain an iX header

| Scenario | Outcome |
|---|---|
| Unified CM 8.x or earlier | Calls fail |
| Unified CM 9.x earlier than 9.1(2) | Calls handled normally but no ActiveControl |
| Unified CM 9.1(2) | Calls handled normally plus ActiveControl |
| Endpoint - no support for iX and no SDP implementation | Endpoint may reboot or calls may fail |

# Cisco Legal Information

# Cisco Trademark