



# Cisco Meeting Server Webinar Session 2

January, 2018

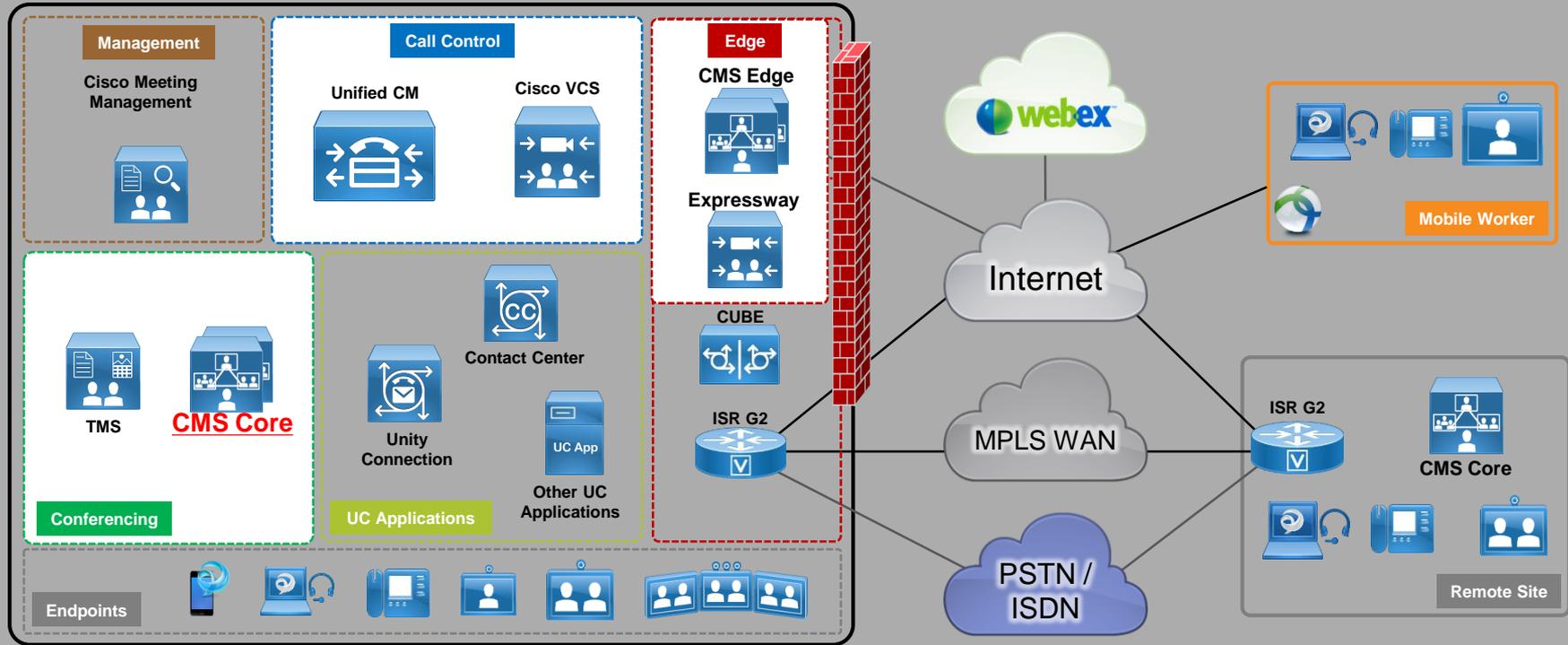
Vikram Dutta

# Agenda

- API Overview
- Branding and Customization
- CMS WebRTC Proxy via Expressway ( Single Edge Solution)
- Recording
- TMS Integration

# General Overview

# Collaboration Architecture



# API Overview

# API (Application programming interface)

Cisco Meeting Server can be configured in 3 ways:

- Web interface of call bridge
  - MMP via ssh
  - API using API tools like PostMan or Poster
- 
- Command are pushed to CMS via API over https:
  - Important API methods we use on CMS are GET, POST, PUT, DELETE
- 
- GET is to fetch status of configuration
  - POST is to do new configuration
  - PUT is to modify existing configuration.
  - DELETE is to Delete configuration

# API Request and Response

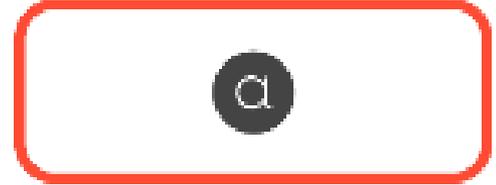


# HTTP POST

- Creates new object



POST /api/v1/coSpaces  
Content-Type: application/x-www-form-urlencoded  
name=APICoSpace&uri=9000&CallID=9000



200 OK  
Location: /api/v1/coSpaces/f11f1c23-ff75-49d1-af8c-384a404f1f26

Filter

<input type="checkbox"/>	Name	URI user part	Secondary URI user part	Additional access methods	Call ID
<input type="checkbox"/>	APICoSpace	9000			9000

# HTTP GET

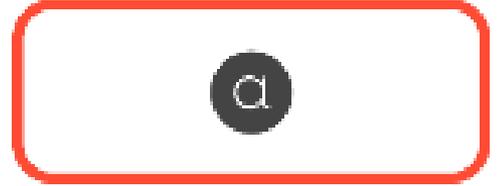
- Retrieves existing information
- No Content in Body



GET /api/v1/calls HTTP/1.1

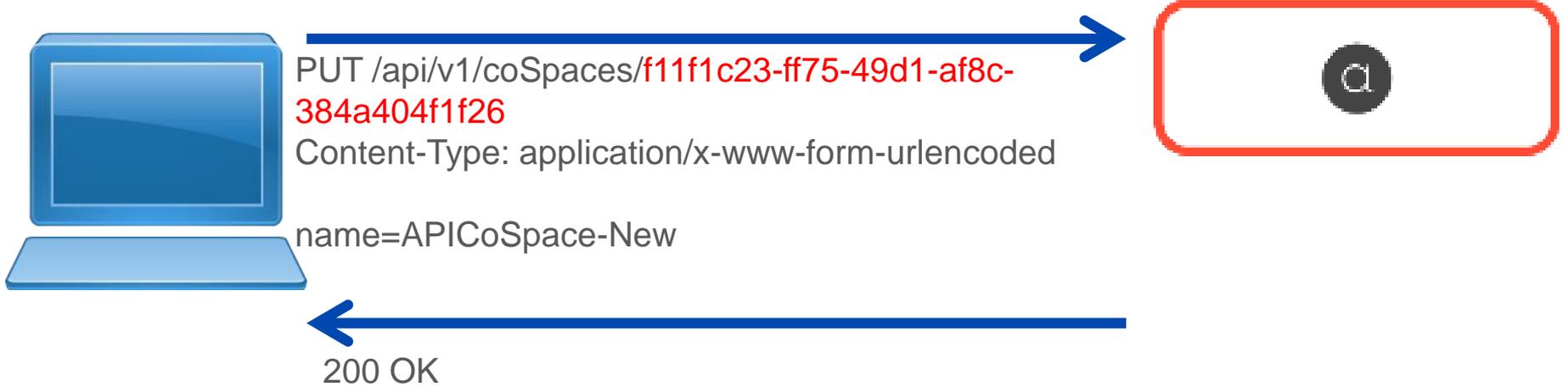
200 OK

```
<?xml version="1.0"?>
<calls total="1">
<call id="527089d6-6581-4331-8417-
971c05c9e274">
<name>Sales coSpace</name>
<coSpace>2dcf2b7a-3410-4066-b638-
46273698d469</coSpace>
</call>
</calls>
```



# HTTP PUT

- Modifies existing object



Filter

<input type="checkbox"/>	Name	URI user part	Secondary URI user part	Additional access methods	Call ID
<input type="checkbox"/>	APICoSpace-New	9000			9000

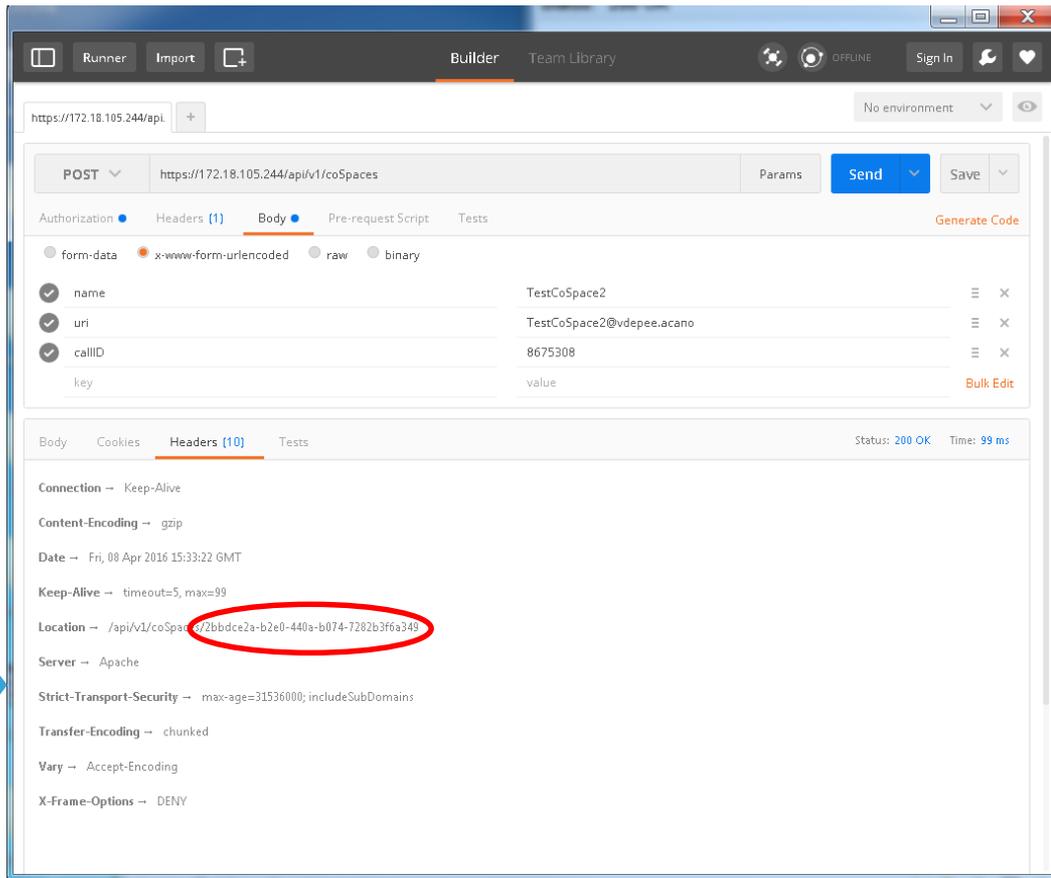
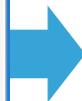
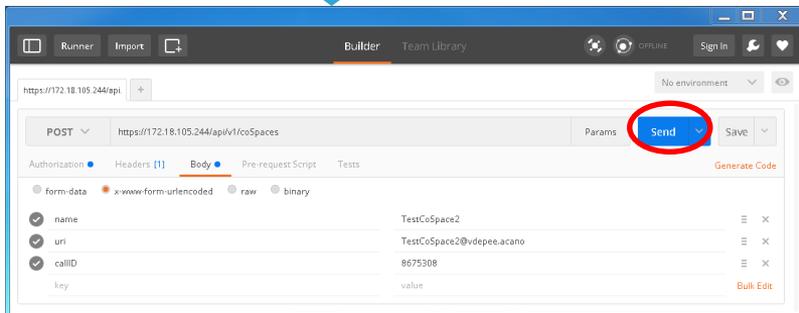
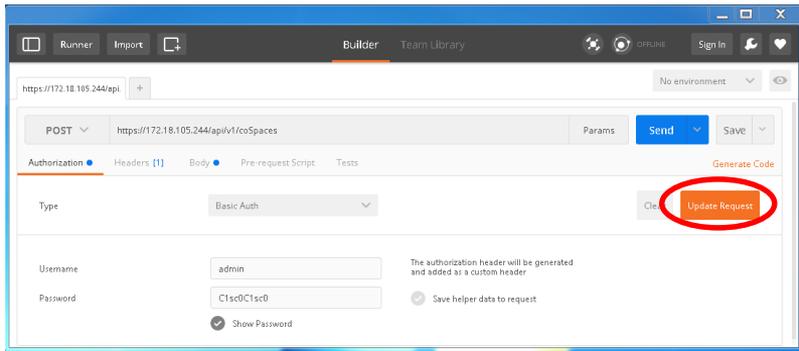
# HTTP DELETE

- Destroys an object

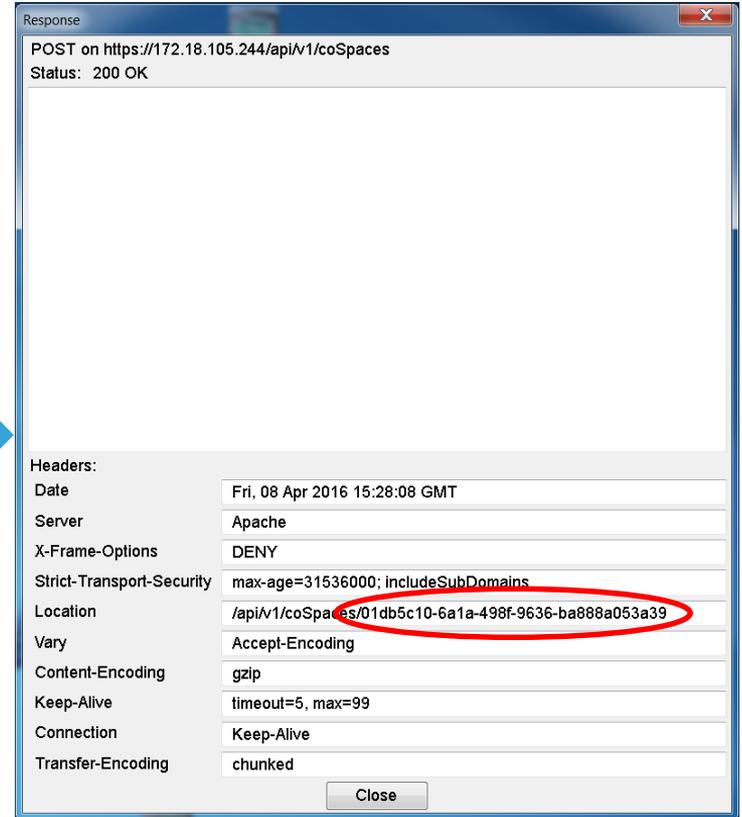
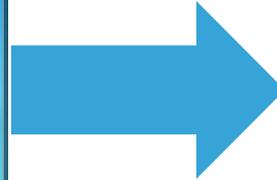
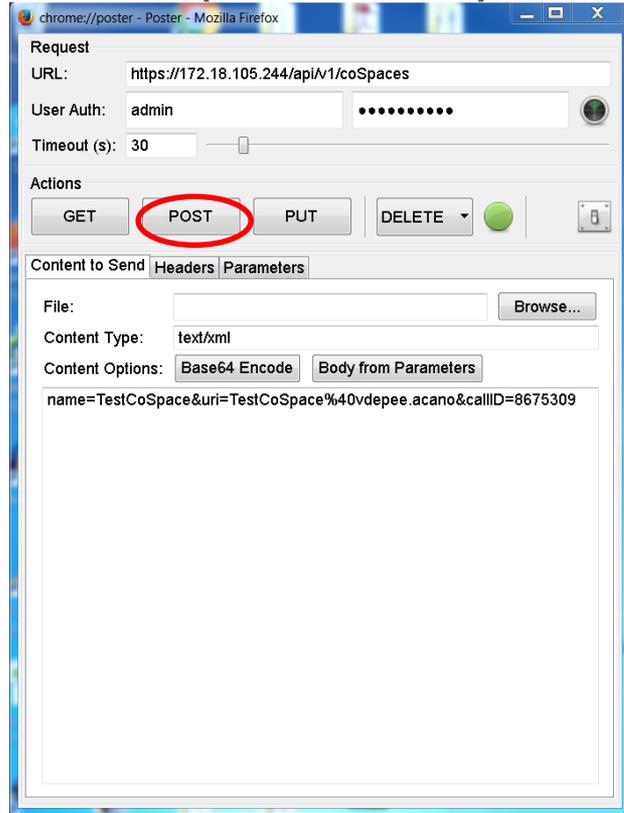


<input type="checkbox"/>	Name	URI user part	Call ID
<input type="checkbox"/>			

# Postman (Chrome)



# Poster (Firefox)



# Branding and Customization

# Branding and Customization

-Branding & customization in Cisco Meeting Server is a way to rebrand the end user WebRTC landing page, voice prompts ,IVRs etc. Enterprises and Service provider can benefit from Branding and customization. They can rebrand the product interfaces, prompts and introduce it to audience.

-Customization on CMS requires an Option key.

## Licenses Types:

- **No Branding license** : Control of the background images and logo on the WebRTC landing page of a single Web Bridge via the Web Admin Interface.

NOTE\*\*\*\* From 2.3 version, It is not possible to do customization from web interface.

- **Single brand via API**: only a single set of resources can be specified/customised Eg (1 WebRTC page, 1 set of voice prompts ,1 invitation text etc). These resources are used for all spaces, IVRs and Web Bridges.
- **Multiple brand via API**: Different resources can be used for different Spaces, IVRs and Web Bridges. These resources can be assigned at the system, tenant, space or IVR level.

# Branding and Customization

What is needed?

- Web Server is required (Windows server with IIS will be enough)
- Create directories on webserver in which all branding files will be placed.  
(.wav, jpg, png or archive (e.g. zip) files can be stored)
- Web server should be reachable from call bridge and there should be no http authentication enabled.
- We need to download branding files from cisco.com (shown in slide ahead)

## WebRTC Client Customization:

We recommend customization of Webrtc client via API

Below fields can be customised:-

- **sign in background image,**
- **sign in dialog box – icon displayed,**
- **sign in dialog box – colours used.**

# Branding and Customization

How to do webbridge branding?

Create a “Branding” folder under wwwroot

Zip all webrtc branding files and place the zip file inside Branding folder we just created.

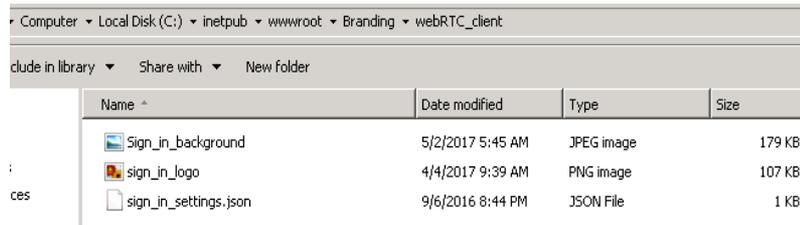
**C:\inetpub\wwwroot\Branding**

Then we need to run a POST method on **/webBridges**

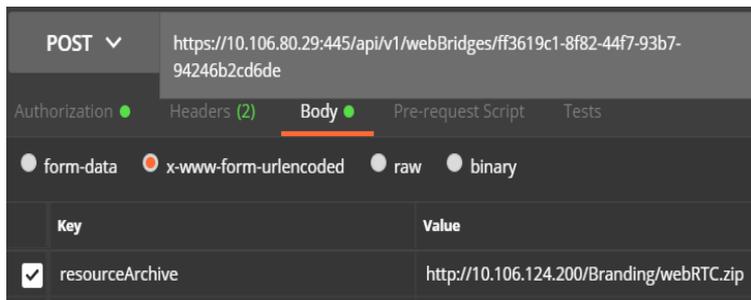
We define the location of files under parameter “resourceArchive” = <http://10.106.124.200/Branding/webRTC.zip>

\*\* There are specific file properties for branding files. Properties of files can be found in below link.

<https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Customisation/Version-2-2/Cisco-Meeting-Server-2-2-Customization-guidelines.pdf>



Name	Date modified	Type	Size
Sign_in_background	5/2/2017 5:45 AM	JPEG image	179 KB
sign_in_logo	4/4/2017 9:39 AM	PNG image	107 KB
sign_in_settings.json	9/6/2016 8:44 PM	JSON File	1 KB

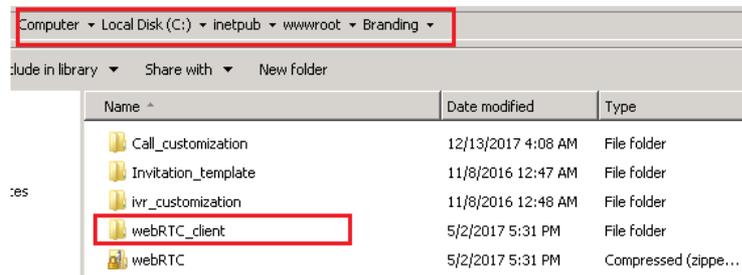


POST <https://10.106.80.29:445/api/v1/webBridges/ff3619c1-8f82-44f7-93b7-94246b2cd6de>

Authorization  Headers (2) **Body** Pre-request Script Tests

form-data  x-www-form-urlencoded  raw  binary

Key	Value
<input checked="" type="checkbox"/> resourceArchive	<a href="http://10.106.124.200/Branding/webRTC.zip">http://10.106.124.200/Branding/webRTC.zip</a>

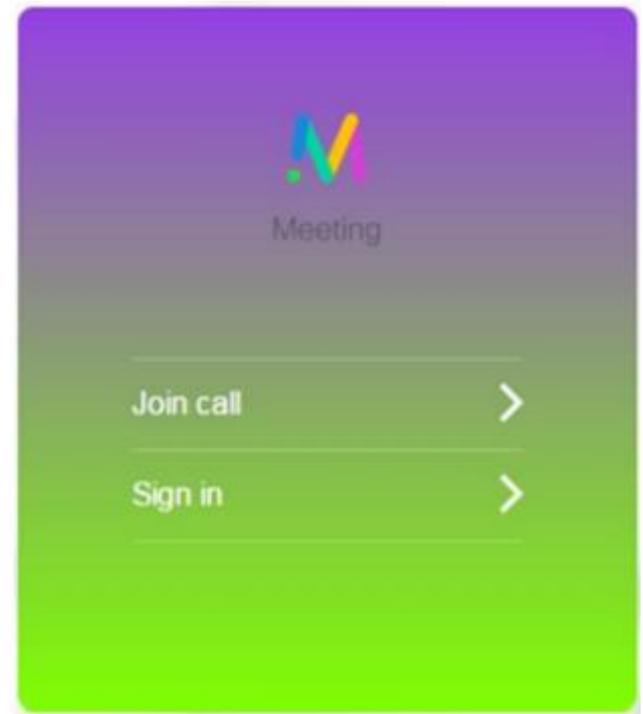


Name	Date modified	Type
Call_customization	12/13/2017 4:08 AM	File folder
Invitation_template	11/8/2016 12:47 AM	File folder
ivr_customization	11/8/2016 12:48 AM	File folder
webRTC_client	5/2/2017 5:31 PM	File folder
webRTC	5/2/2017 5:31 PM	Compressed (zippe...

# Branding and Customization

Colours of “Join Call Pane” can also be changed. This is controlled by .json file.

Upto 4 colour can be used. If not configured correctly, default white background will be used.



# Branding and Customization

## Call Customization

There are 2 types of call customizations:

**IVR call customization** and **Sip call customization** (both needs branding license)

## How to do IVR customization

IVR customization enables us to modify the IVR voice prompt which user hears when call connects to CMS IVR.

Messages shown in the screen shot can be customized. >>>>>>>

IVR background images can also be customised

Text of message	Filename to use (filenames are case sensitive)	Played when .....
Please enter the call ID, followed by the '#'(pound) key.	ivr_id_entry.wav	dialling via IVR to enter a specific space
Unable to recognize that call ID. Please try again.	ivr_id_incorrect_try_again.wav	the incorrect call ID is entered to join the space
Please try again: this is your last attempt.	ivr_id_incorrect_final_attempt.wav	two incorrect pins/call ID's have been entered to join the space
Unable to recognize that call ID. Goodbye.	ivr_id_incorrect_goodbye.wav	entering three incorrect call ID's to join the space
Welcome to a Cisco meeting.	ivr_welcome.wav	joining a space
Unable to connect you. Goodbye.	ivr_timeout.wav	after dialling via IVR and not entering the call ID, the call times out

# Branding and Customization

## How to do IVR Customization

Create a folder named “**ivr\_customization**” at below location

**C:\inetpub\wwwroot\Branding**

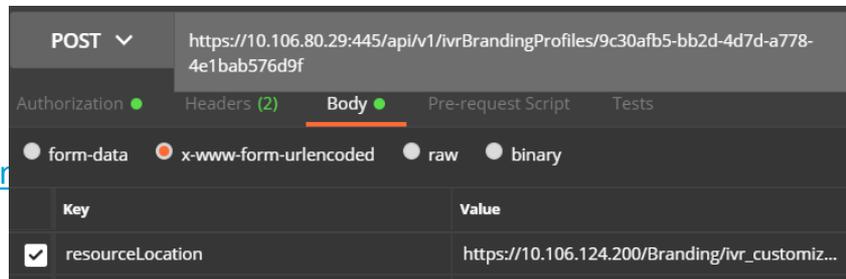
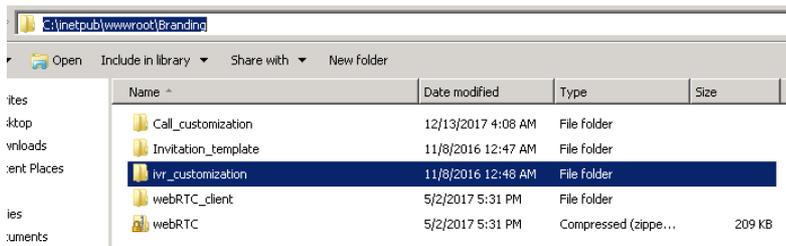
Custom IVR files can be downloaded from [cisco.com](https://www.cisco.com).

<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html>

Place all custom files in the **ivr\_customization** folder.

Using API client, create a **/ivrBrandingProfiles** and specify the **resourceLocation** = [https://10.106.124.200/Branding/ivr\\_customization](https://10.106.124.200/Branding/ivr_customization)

Apply the **ivrBrandingProfile** at system level (global parameter)



# Branding and Customization

## SIP/Lync Call Message Customization

### How to customize calls initiated from Sip Endpoints or Lync clients?

There are tons on messages which can be customized. Here are few mentioned in screenshot. All messages can be seen in url mentioned.

<https://www.cisco.com/c/dam/en/us/td/docs/conferencing/ciscoMeetingServer/Customisation/Version-2-2/Cisco-Meeting-Server-2-2-Customization-guidelines.pdf>

SIP Call Branding sample wav files can be downloaded from below link.

<https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html>

Text of message	Filename to use (filenames are case sensitive)	Repeats for audio calls	Played when .....
Welcome to a Cisco meeting	welcome.wav	No	joining a call
I haven't been able to connect you. Goodbye.	timeout.wav	No	after dialling via an IVR and not entering the call id, the call times out
Press '1' to join the call.	call_join_confirmation.wav	No	
You are joining the call now.	call_join.wav	No	
Hello. You are invited to a Cisco call.	call_outgoing_welcome.wav	No	
Press '1' to enter the meeting.	cospace_join_confirmation.wav	No	calling a phone number from a space

# Branding and Customization

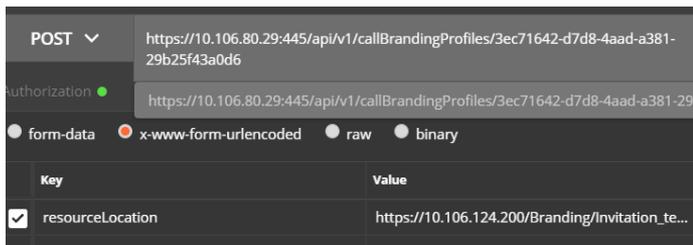
How to do sip/lync call customization

Create a folder “Call\_customization” at below location and place your wav files in the folder.

**C:\inetpub\wwwroot\Branding**

**Create a /callBrandingProfiles** by doing a POST with resourceLocation mentioned.

resourceLocation= [https://10.106.124.200/Branding/Invitation\\_template.txt](https://10.106.124.200/Branding/Invitation_template.txt)

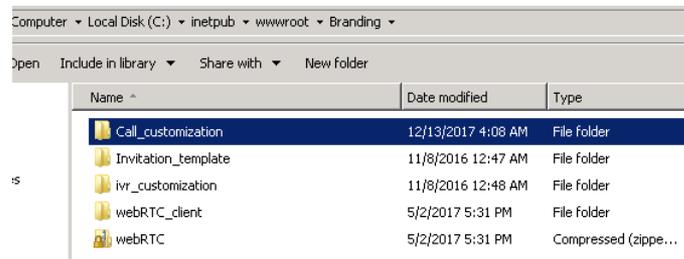


POST  <https://10.106.80.29:445/api/v1/callBrandingProfiles/3ec71642-d7d8-4aad-a381-29b25f43a0d6>

Authorization  <https://10.106.80.29:445/api/v1/callBrandingProfiles/3ec71642-d7d8-4aad-a381-29b25f43a0d6>

form-data  x-www-form-urlencoded  raw  binary

Key	Value
<input checked="" type="checkbox"/> resourceLocation	<a href="https://10.106.124.200/Branding/Invitation_te...">https://10.106.124.200/Branding/Invitation_te...</a>



Name	Date modified	Type
Call_customization	12/13/2017 4:08 AM	File folder
Invitation_template	11/8/2016 12:47 AM	File folder
ivr_customization	11/8/2016 12:48 AM	File folder
webRTC_client	5/2/2017 5:31 PM	File folder
webRTC	5/2/2017 5:31 PM	Compressed (zippe...)

# Branding and Customization

## SIP/Lync Call Message Customization

Apply the **/callBrandingProfiles** to system level.

The screenshot shows a REST client interface for a POST request to `https://10.106.80.29:445/api/v1/system/profiles`. The request body is set to `x-www-form-urlencoded` and contains a single key-value pair:

Key	Value
<input checked="" type="checkbox"/> callBrandingProfiles	3ec71642-d7d8-4aad-a381-29b25f43a0d6
<input type="text" value="New key"/>	<input type="text" value="Value"/>

# Branding and Customization

## Customizing the invitation text on CMA clients

CMA users can send out join invitations to other users.

These invitations can be customized and sent out with contact information. We can include webrtc join URLs, PSTN phone numbers, Space ids etc. in the invitation.

## Invitation example below

You're invited to Join My OnLine Meeting of lyncadmin.space

To join from a PC/Mac, click here: <https://bharat.tptac9.com/invited.sf?secret=2D5Ha5d48t9ptkjbSznFsw&id=776655>

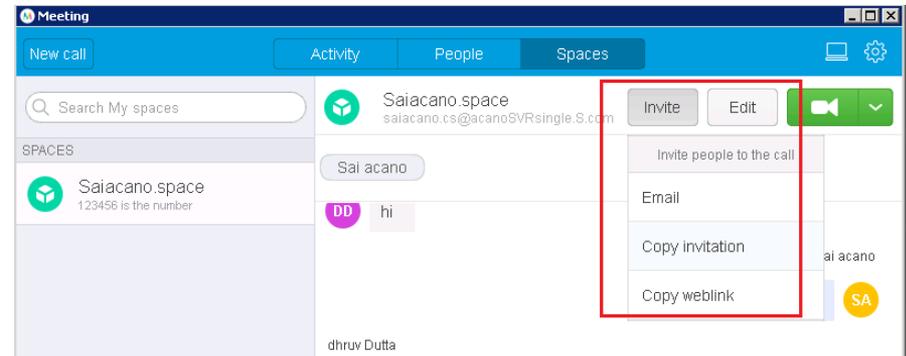
To join from an Android Device, click here: <https://bharat.tptac9.com/invited.sf?secret=2D5Ha5d48t9ptkjbSznFsw&id=776655>

To join from an Apple Device, download the app: <https://itunes.apple.com/us/app/acano/id680581809?mt=8>  
After downloading, then click, here: <https://bharat.tptac9.com/invited.sf?secret=2D5Ha5d48t9ptkjbSznFsw&id=776655>

Room-Based Video System, Dial: [776655@tptac9.com](tel:776655@tptac9.com)

Jabber or Lync Client, Dial: [776655@tptac9.com](tel:776655@tptac9.com)

If you are unable to dial a URI, Dial: 1.1.1.1  
At the prompt, Enter: 776655#



The screenshot shows a Cisco Meeting application window titled "Meeting". The interface includes a top navigation bar with "New call", "Activity", "People", and "Spaces" tabs. Below this is a search bar labeled "Search My spaces". The main content area displays a meeting space named "Saiacano.space" with a green icon and the text "123456 is the number". A chat window is open on the right, showing a message from "Sai acano" with the text "hi". A red box highlights the "Invite" button in the top right corner, which has opened a dropdown menu with the following options: "Invite people to the call", "Email", "Copy invitation", and "Copy weblink".

# Branding and Customization

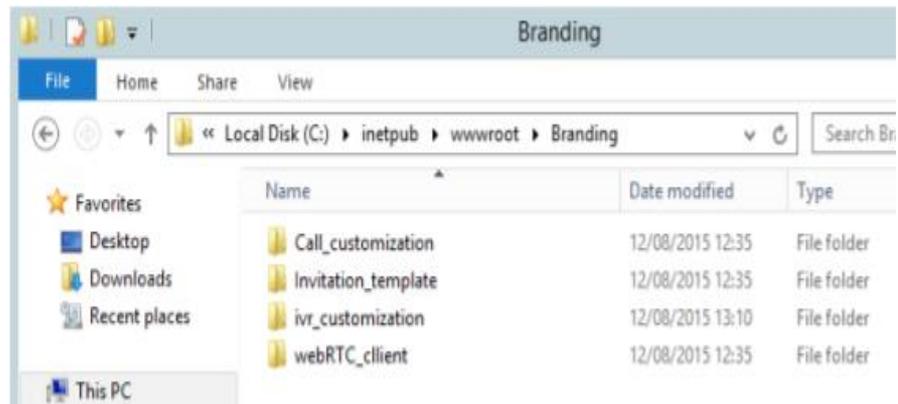
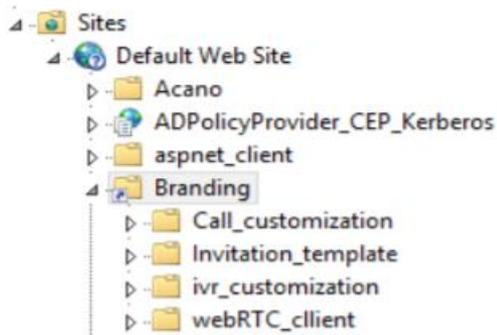
## Branding Summary:

Make sure IIS is running on windows webserver with no authentication enabled.

Create relevant Branding folders under Default IIS directory (**c:\inetpub\wwwroot**)

Make sure relevant files are placed correctly in folders.

Check IIS manager, all folders should be visible there.



# Branding and Customization

- Create /callBrandingProfile , /ivrBrandingProfile, /webBridges
- Specify the resourceLocations under each object.
- place the GUID under system level profiles.
- Branding should work.

Check output.

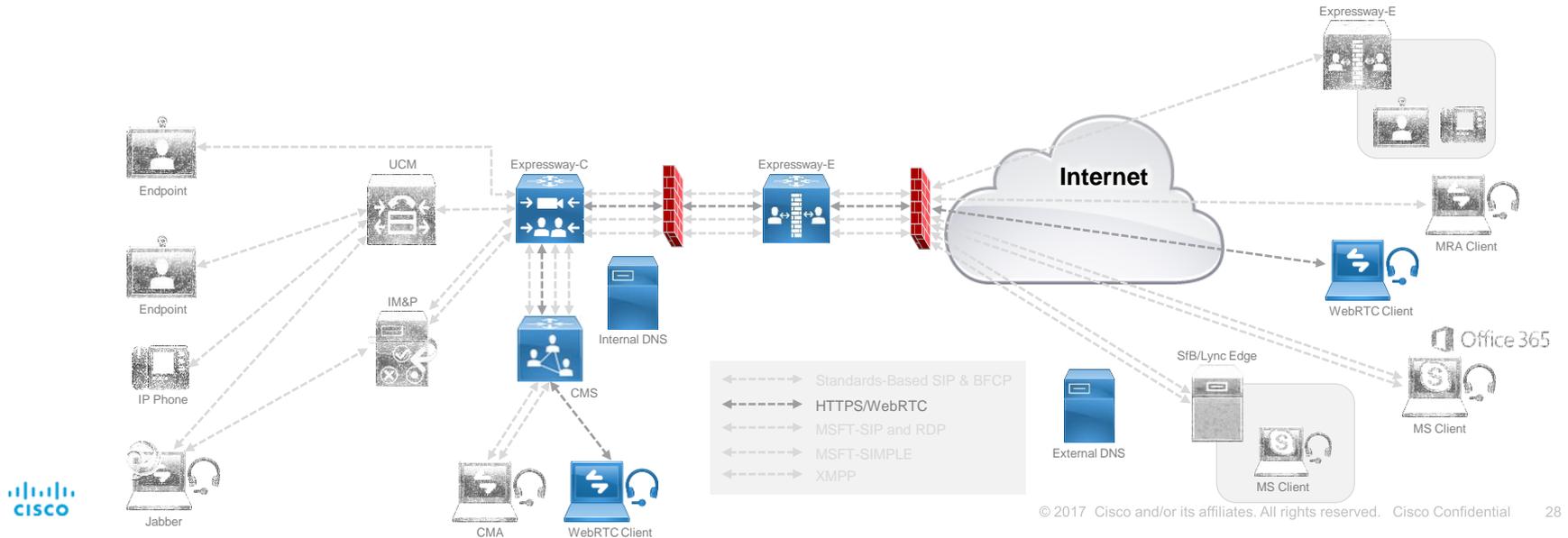
# Expressway proxy for WebRTC

# Single Edge Solution

- **Single Expressway Edge for Cisco Meeting Server deployments**

- WebRTC Clients (CMS Web Proxy)

- Enables external users to join CMS spaces using browser. (chrome only)
- External users would only need Join URL and passcode (if configured) to connect to CMS space.

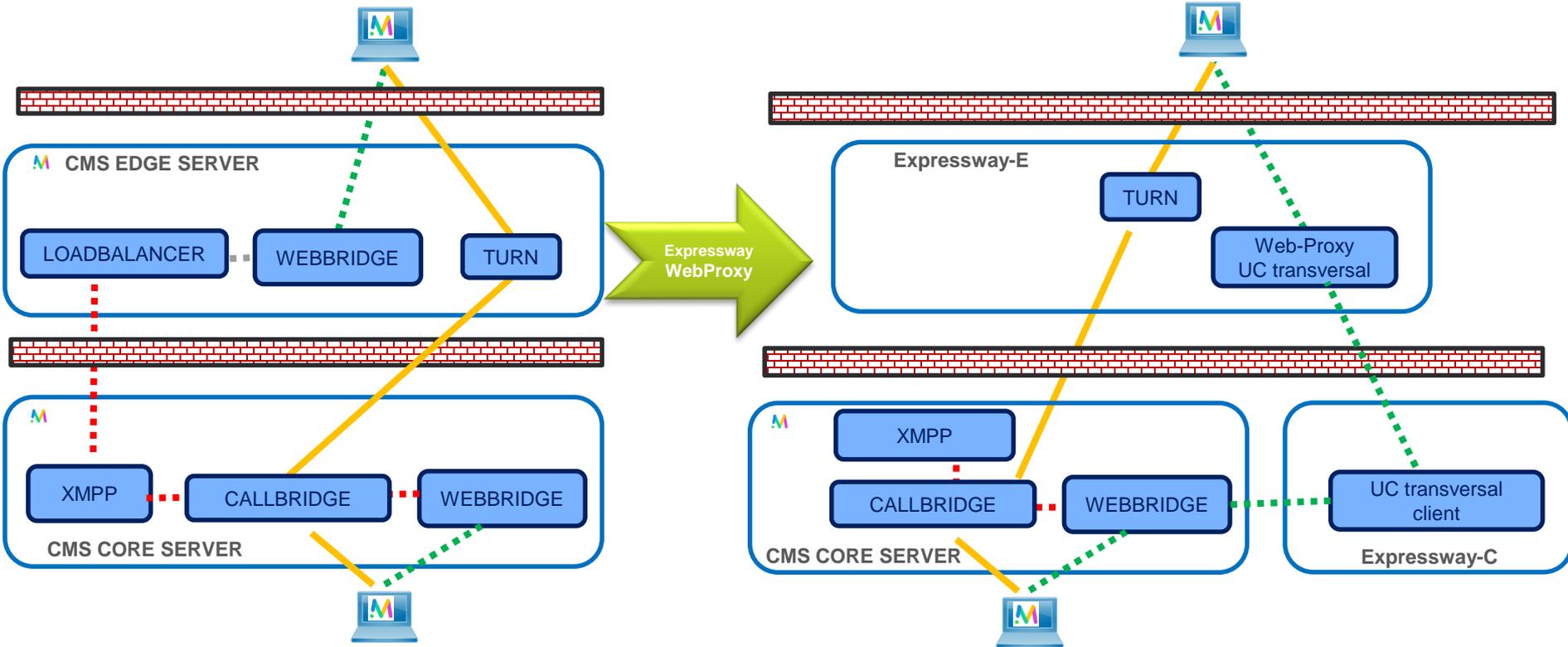


# Single Edge Solution

- Cisco Flagship product Expressways can act as entry point for Webrtc clients to join meetings server spaces.
- Expressways “**Reverse Proxy**” feature helps in traversing “Https” traffic securely through corporate firewall and enables webrtc clients to join cms spaces.
- CMS utilizes “**Turn**” feature on Expressway to latch media from outside and vice versa.
- CMS web proxy can coexist with MRA, B2B, Registrar, IMP federation but not with **Jabber-Guest or MS Interop**.
- **Solution Components defined below:**
- Join.s.com is webrtc url hosted on Internal and external network.



# From legacy CMS Edge to Expressway Web-Proxy



XMPP  
.....

HTTPS / WEBRTC  
.....

Media ; TURN  
.....

# Single Edge Solution

## High level configuration overview on CMS

- We assume that basic CMS configuration like **Webbridge**, **Call bridge**, **Xmpp** etc have been done already.
- Make sure webrtc works internally.
- Webadmin port on cms should be changed to 445 (or any other port)
- Configure guest url and domain on cms web bridge settings.

Web bridge settings

Guest account client URI	https://join.S.com
Guest account JID domain	S.com
Custom background image URI	
Custom login logo URI	
Guest access via ID and passcode	legacy: passcode entry after call ID resolution
Guest access via hyperlinks	allowed
User sign in	allowed
Joining scheduled Lync conferences by ID	not allowed

- To enable external access for join url make sure **external access** is enabled on cms.

```
acanoSVRsingle> webadmin
Enabled : true
TLS listening interface : a
TLS listening port : 445
Key file : webadmin.key
Certificate file : webadmin.cer
CA Bundle file : UCTPROOTCA.cer
HTTP redirect : Disabled
STATUS : webadmin running
```

External access

Web Bridge URI	https://join.S.com
IVR telephone number	

# Single Edge Solution

## High level configuration overview on CMS

- Make sure xmpp component is configured on cms and active.

### System status

Uptime	16 days, 22 hours, 28 minutes
Build version	2.2.7
XMPP connection	connected to 10.106.80.29 (secure) for 16 days, 22 hours, 28 minutes

```
acanoSVRsingle> xmpp
Enabled : true
Clustered : false
Domain : s.com
Listening interfaces : a
Key file : xmpp.key
Certificate file : xmpp.cer
CA Bundle file : UCTPROOTCA.cer
Max sessions per user : unlimited
STATUS : XMPP server running

acanoSVRsingle> xmpp callbridge list
***
Callbridge : acanoSVRsingle
Domain : s.com
Secret : BehkqHRAPV1mRdkiAb1
***
```

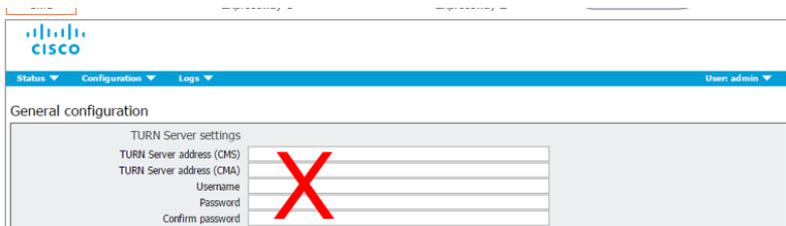
- Make sure Call id is configured on CMS space. (passcode not mandate)

joey's space	joey.meet		754893669		not set
prkapur's space	prkapur.meet		624700180		not set
user1's space	user1.meet		182879137		not set

# Single Edge Solution

High level configuration overview on CMS

- Turn server configuration need to be done via API not web interface.



DO NOT configure TURN parameters from Web GUI

- Below is important Turn configuration which need to be done via API.

Parameter	Value
<u>serverAddress</u>	TURN Server's FQDN/IP Address (Expressway-E Private IP Address, i.e. address of LAN1)
<u>clientAddress</u>	TURN Server's FQDN/IP Address (Expressway-E Public IP Address, i.e. NAT address of LAN2)
<u>username</u>	TURN Authentication realm
<u>password</u>	TURN Authentication password
<u>type</u>	expressway
<u>tcpPortNumberOverride</u>	3478

IMPORTANT: Configure TCP/TURN port to "3478"

# Single Edge Solution

## High level configuration overview on CMS

- On CMS API client, Do a POST on `/turnServers` with below parameters in Body.

Parameter	Value
<code>serverAddress</code>	TURN Server's FQDN/IP Address (Expressway-E Private IP Address, i.e. address of LAN1)
<code>clientAddress</code>	TURN Server's FQDN/IP Address (Expressway-E Public IP Address, i.e. NAT address of LAN2)
<code>username</code>	TURN Authentication realm
<code>password</code>	TURN Authentication password
<code>type</code>	expressway
<code>tcpPortNumberOverride</code>	3478

IMPORTANT: Configure TCP/TURN port to "3478"

- Example configuration results should look like below.

(Note My ExpresswayE is single nic, thus client/server ip are same)

```
1 <?xml version="1.0"?>
2 <turnServer id="998e5f32-2e6e-4c04-baaa-20dcc0b5d53f">
3   <serverAddress>10.106.80.17</serverAddress>
4   <clientAddress>10.106.80.17</clientAddress>
5   <numRegistrations>0</numRegistrations>
6   <username>turn</username>
7   <type>expressway</type>
8   <tcpPortNumberOverride>3478</tcpPortNumberOverride>
9 </turnServer>
```

# Single Edge Solution

High level configuration overview on Expressway C

- **Configure Unified Traversal Zone on Expressway C.**

The screenshot shows the configuration interface for a Unified Traversal Zone. It is divided into two sections: 'Configuration' and 'Connection credentials'.  
In the 'Configuration' section:  
- Name: UçZONE217  
- Type: Unified Communications traversal  
- Hop count: 15  
In the 'Connection credentials' section:  
- Username: admin  
- Password: [masked]

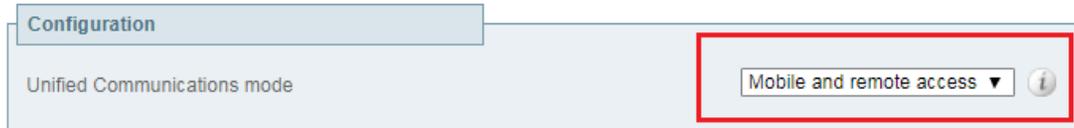
- **Sign expressway C certificate and make sure client/server attributes are present.**

```
X509v3 extensions:  
X509v3 Key Usage: critical  
    Digital Signature, Key Encipherment  
X509v3 Extended Key Usage:  
    TLS Web Server Authentication, TLS Web Client Authentication  
X509v3 Subject Alternative Name:  
    DNS:VCS8C.s.com, DNS:VCS8Master.S.com, DNS:federation.com, DNS:acanoSVRsingle.S.com  
X509v3 Subject Key Identifier:  
    79:B3:8F:47:D7:C1:5E:DE:C3:D8:C5:63:1D:63:E2:B1:F1:AA:CF:4D  
X509v3 Authority Key Identifier:  
    keyid:28:19:A2:11:1B:92:61:1C:3F:2B:46:34:73:88:78:D1:82:0C:DC:97
```

# Single Edge Solution

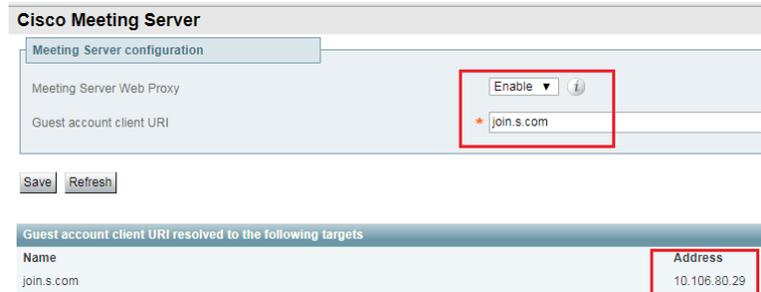
## High level configuration overview on Expressway C

- Enable MRA on Expressway C



The screenshot shows the 'Configuration' tab of the Expressway C interface. The 'Unified Communications mode' is set to 'Mobile and remote access', which is highlighted with a red rectangular box. An information icon is visible to the right of the dropdown menu.

- Add CMS on Expressway C.



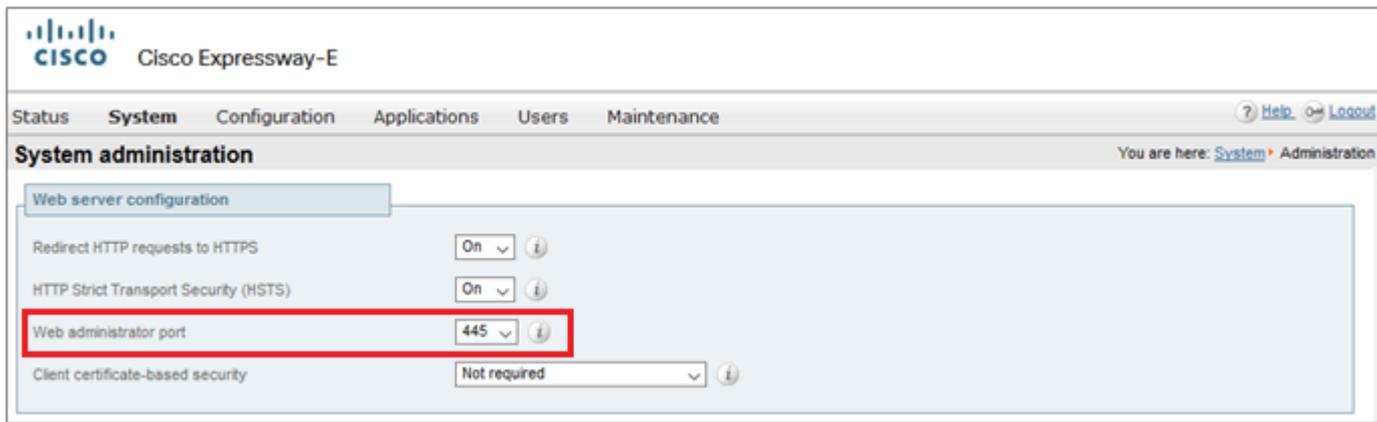
The screenshot shows the 'Cisco Meeting Server' configuration page. The 'Meeting Server configuration' tab is active. The 'Meeting Server Web Proxy' dropdown menu is set to 'Enable' and the 'Guest account client URI' field contains 'join.s.com'. Both the dropdown menu and the text input field are highlighted with a red rectangular box. Below the configuration fields are 'Save' and 'Refresh' buttons. At the bottom, a table shows the resolved targets for the 'Guest account client URI'.

Name	Address
join.s.com	10.106.80.29

# Single Edge Solution

High level configuration overview on Expressway C

- **Change administration port on Expressway C. You can change the port from CLI to any other port.(gui only support 445 or 443)**

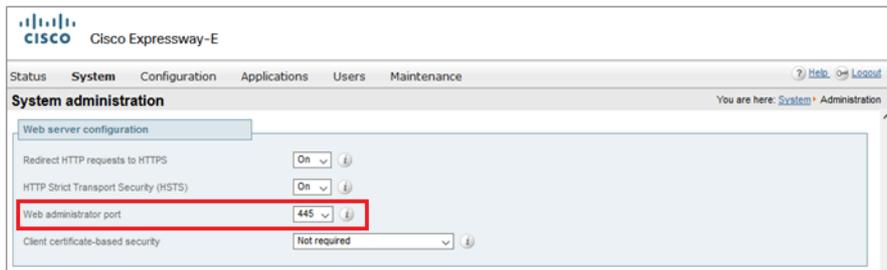


The screenshot displays the Cisco Expressway-E web administration interface. At the top left is the Cisco logo and the text 'Cisco Expressway-E'. Below this is a navigation bar with tabs for 'Status', 'System', 'Configuration', 'Applications', 'Users', and 'Maintenance'. The 'System' tab is selected. In the top right corner, there are links for 'Help' and 'Logout'. The main content area is titled 'System administration' and shows a breadcrumb trail 'You are here: System > Administration'. Under the 'Web server configuration' section, there are four configuration items: 'Redirect HTTP requests to HTTPS' (set to 'On'), 'HTTP Strict Transport Security (HSTS)' (set to 'On'), 'Web administrator port' (set to '445'), and 'Client certificate-based security' (set to 'Not required'). The 'Web administrator port' row is highlighted with a red rectangular box.

# Single Edge Solution

## High level configuration overview on Expressway E

- Change administration port on Expressway E. you can change the port from CLI to any other port.(gui only support 445 or 443)



- Install certificate on Expressway E. **(Imp Expressway E certificate should have external webRTC join Url as SAN name)**

```
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Subject Alternative Name:
  DNS:VCS8Master.s.com, DNS:Edgeinternal.federation.com, DNS:Edgeexternal.federation.com, DNS:FE.federation.com, DNS:federation.com, DNS:acanoSVRSing1e.s.com, DNS:s.com, DNS:acanolab.com, DNS:join.s.com
X509v3 Subject Key Identifier:
  3E:67:7D:10:72:0E:89:34:27:60:C9:08:70:AD:69:09:C9:BF:E2:28
```

If Join URL is not present in san, a certificate warning will always appear on browser while accessing webrtc link



# Single Edge Solution

## High level configuration overview on Expressway E

- Create Unified traversal zone on Expressway E

**Configuration**

Name	* UCZONE249	
Type	Unified Communications traversal	
Hop count	* 15	

**Connection credentials**

Username	* admin	
Password	<a href="#">Add/Edit local authentication database</a>	

Enabled Mobile and Remote Access mode

Cisco Expressway-E

Status System **Configuration** Applications Users Maintenance Help Logout

**Unified Communications** You are here: Configuration > Unified Communications > Configuration

**Configuration**

Unified Communications mode	Mobile and remote access	
-----------------------------	--------------------------	--

**Single Sign-On**

Single Sign-On support	Off	
------------------------	-----	--

# Single Edge Solution

## High level configuration overview on Expressway E

- Configure and enable Turn server.
- Note\*\* : Turn relay licenses should be installed on expressway E.

**TURN**

Server

TURN services: On

TURN requests port: 3478

Delegated credential checking: Off

Authentication realm: turn

Media port range start: 24000

Media port range end: 29999

-

- On External DNS server, resolve join.s.com to resolve to Expressway E public ip-address

Device	FQDN	IP Address
Guest Account URL	Join.s.com	point to Exp-E 10.106.80.17

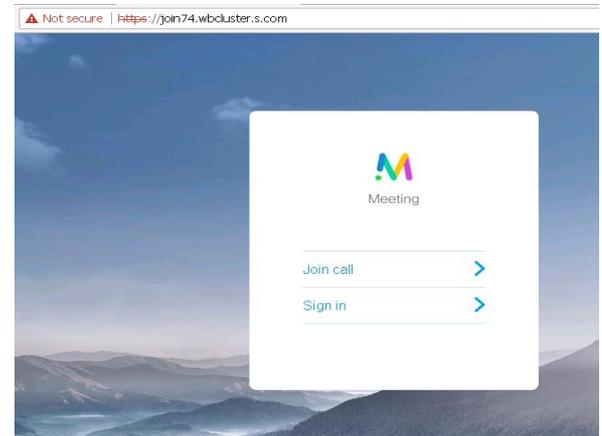
# Single Edge Solution

## High level Call flow:



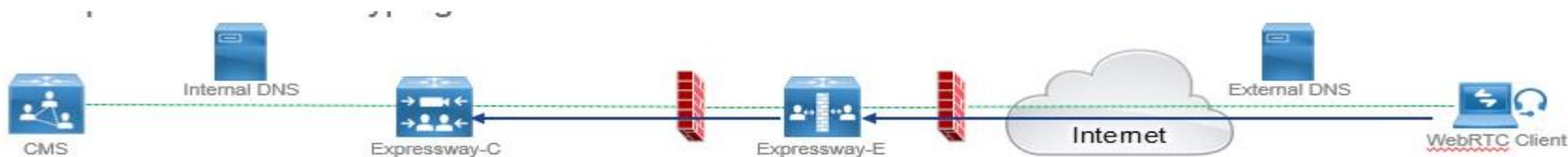
- User open browser and type guest access client URL. Browser connects to Expressway E on port 443
- Traverses inside via Expressway C to CMS and fetches all web browser headers.

```
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/ HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/bundle.min.js HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/graphics/logo_cma_a.svg HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/app.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/common.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/animations.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/extension.js HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/typography.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/palettes.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/defaults.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/utilities.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/headings.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/layers.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/effects.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/contexts.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/modules.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/coApps.css HTTP/1.1
GET http://vcs_control.uc.ciscotp.com:8443/LUNNUyO/css/guest.css HTTP/1.1
```

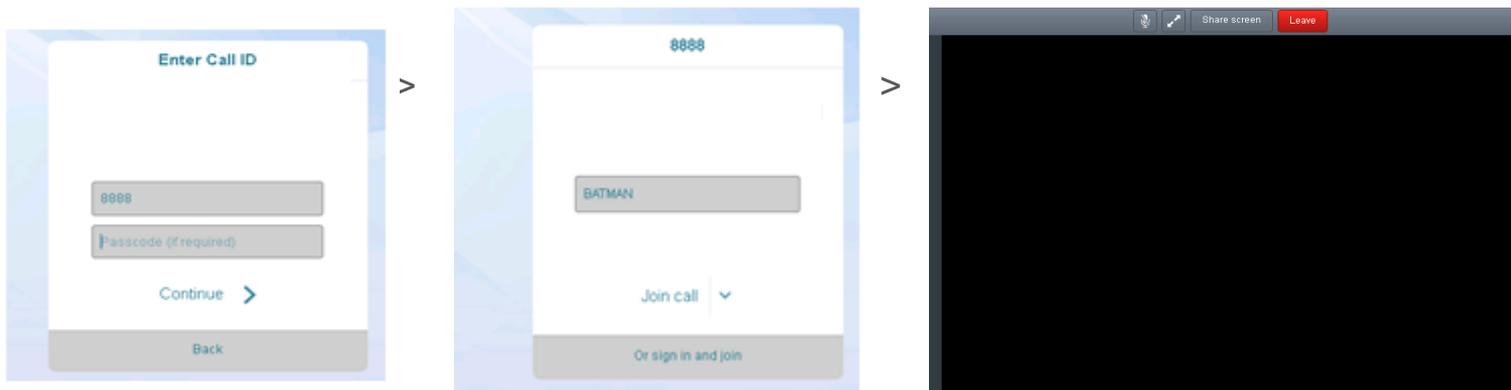


# Single Edge Solution

High level Call flow:



- Once “join” tab appears . Please enter “call Id” (passcode if configured on cms) next.
- Enter a friendly name
- Join the call.

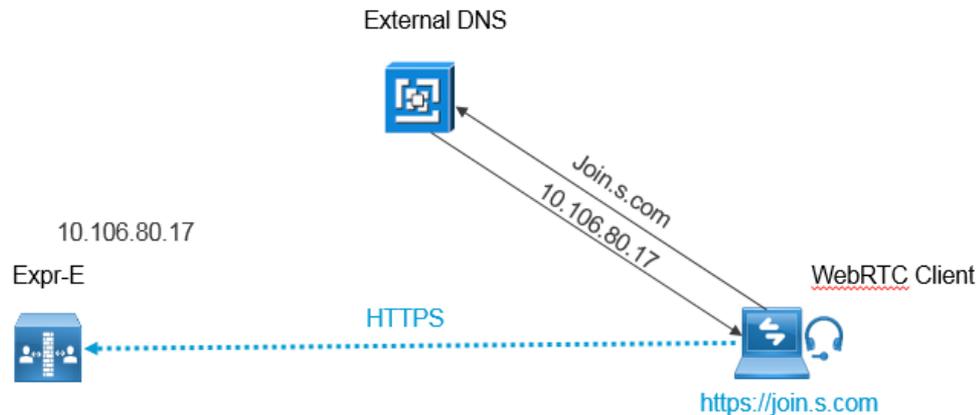


# Single Edge Solution

## High level Call flow:

- Webrtc client resolves the external join URL and gets the expressway E ip address.
- Browser connects on Expressway E on 443.
- Expressway E presents its certificate.

## Configuration

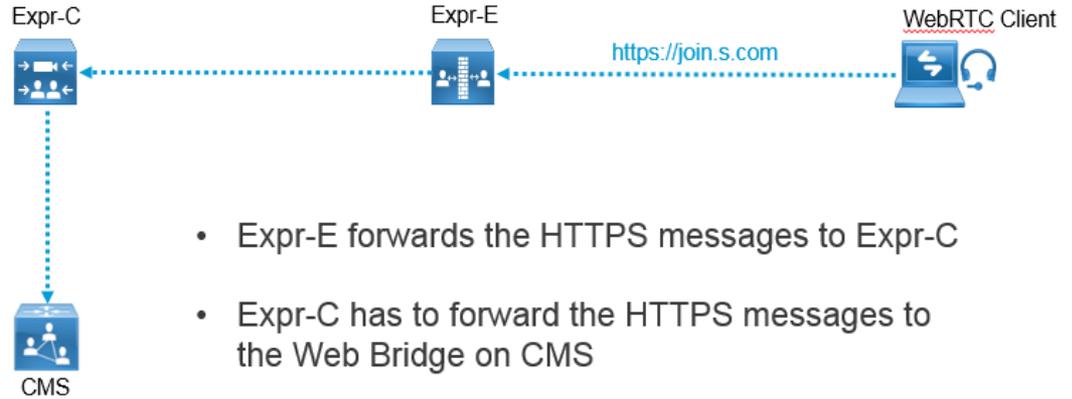


# Single Edge Solution

High level Call flow:

**IMP\*\*\***

Expressway C should be able to resolve  
Join URL into CMS webbridge ip address  
Internally.

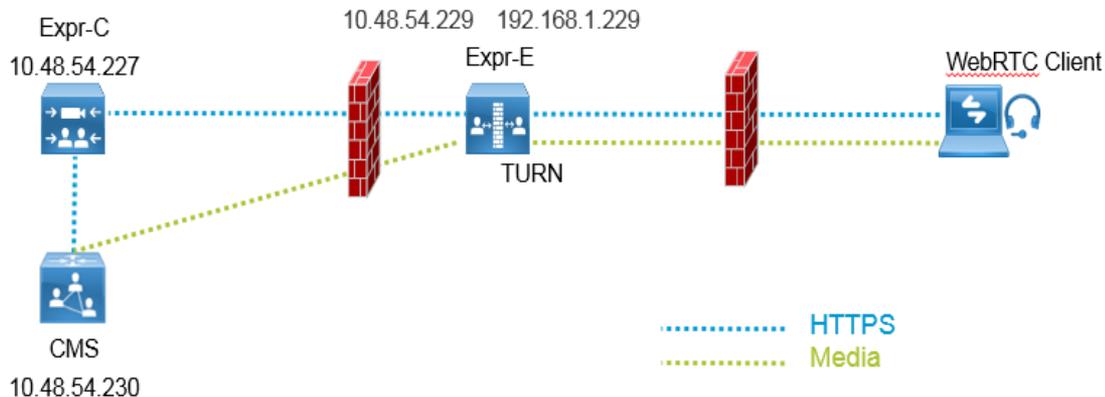


# Single Edge Solution

High level Call flow:

Media flow:

- Webrtc uses Ice "TURN" component to latch media to Expressway E.
- Since Expressway E provides TURN services , Turn component on Expressway Binds itself to CMS and Webrtc clients, and latches media for both sessions.

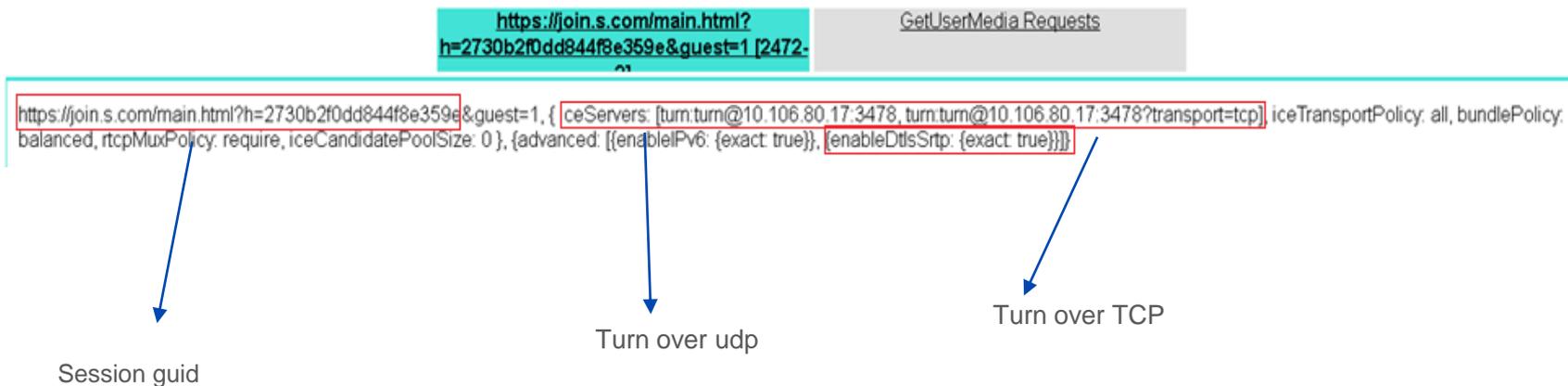


# Single Edge Solution

Using browser inbuilt tools, we can troubleshoot webrtc calls.

**chrome://webrtc-internals/** is one such tool.

-



# Single Edge Solution

High level Call flow:

Continue.....

Using browser inbuilt tools, we can trouble shoot webrtc calls.

**chrome://webrtc-internals/**

**Digging further we see relay candidates offered.**

```
10/01/2018, 17:59:55  setLocalDescriptionOnSuccess
                      ▼ icecandidate (relay)
10/01/2018, 17:59:55  sdpMid: audio, sdpMLineIndex: 0, candidate: candidate:3079937280 1 udp 16785151 10.106.80.17 24002 typ
                      ▼ icecandidate (relay)
10/01/2018, 17:59:55  sdpMid: audio, sdpMLineIndex: 0, candidate: candidate:4179091952 1 udp 33562623 10.106.80.17 24005 typ
                      ▼ icecandidate (relay)
10/01/2018, 17:59:55  sdpMid: video, sdpMLineIndex: 1, candidate: candidate:3079937280 1 udp 16785151 10.106.80.17 24004 typ
                      ▼ icecandidate (relay)
10/01/2018, 17:59:55  sdpMid: video, sdpMLineIndex: 1, candidate: candidate:4179091952 1 udp 33562623 10.106.80.17 24006 typ
```

# Single Edge Solution

High level Call flow:

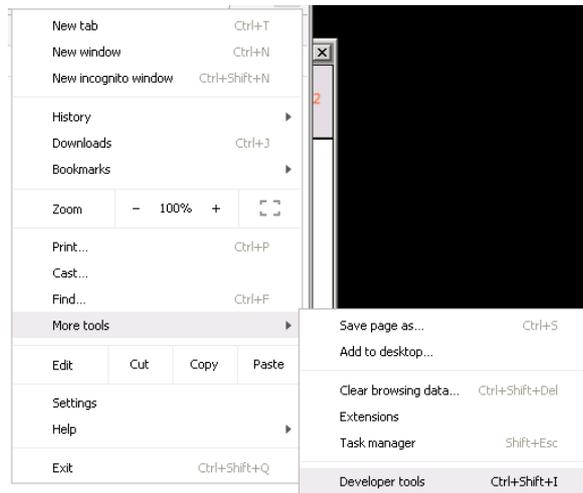
Continue.....

Using browser inbuilt tools, we can troubleshoot webrtc calls.

You can navigate to

**Chrome> more tools > developer tools> Console view**

**Logs captured on console shows us turn servers presented to client.**



script\_booter.js?h=2730b2f0dd844f8e359e:5 12:44:27 : webrtc configuration updated - **using turn server "10.106.80.17"**

script\_booter.js?h=2730b2f0dd844f8e359e:5 12:44:27 : Configure Peer Connection

# CMS Recorder

# Cms Recorder

Recorder solution on CMS provides capability to enterprises to record meetings.

-Components needed for Recorder :

-Call bridge

-NFS file server.

-Xmpp component on call bridge server

-CMS server should be on or above 1.9

-Recorder is a licensed feature. Licenses is needed to enable it.

# Cms Recorder

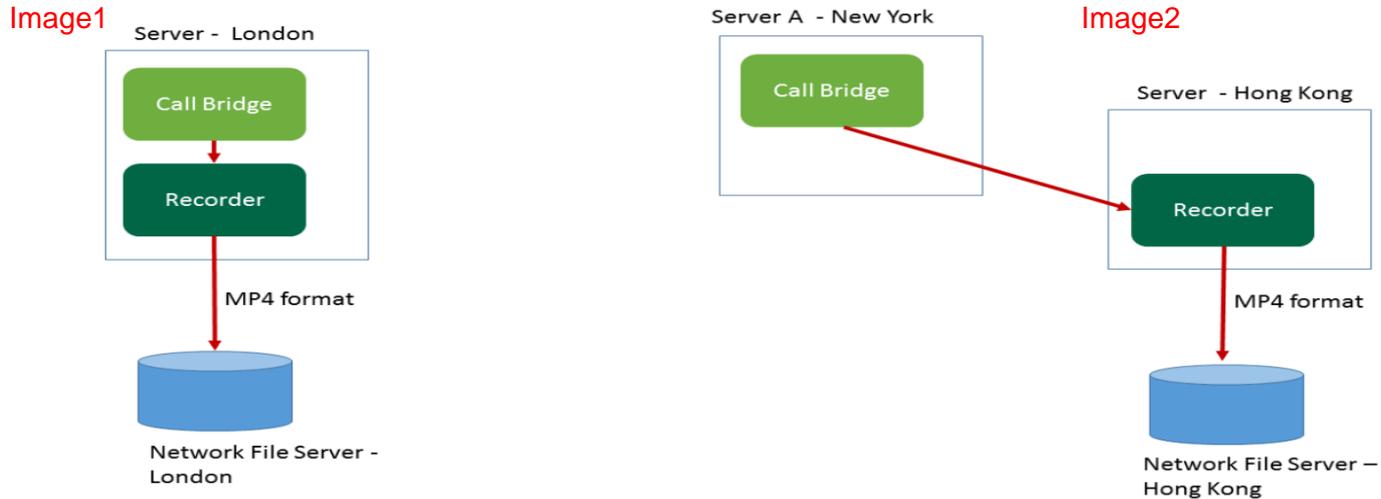
## Recorder can be deployed in 2 ways.

- Recorder can **co-locate** along with call bridge on same box. (Such deployment is not recommended for productions)
- Recorder component can exist on a **separate server** which should be reachable by call bridge.
- You can have a **redundant** setup for recorders and call bridges.
- Recorder and NFS server should be on **same physical network**. This ensures low latency/loss
- A typical recording for 1 hr on 720p30 resolution , creates a file of 300-800 mb
- When recording ends, recorder converts the file in MP4 format and places it on NFS directory path.
- Recorder secretly acts as a xmpp client.
- Make sure xmpp is configured and xmpp SRVs are in place on call bridge.

# Deployment models

Deployment shown in **image1** should be used for testing purposes only

Deployment shown in **image2** includes single call bridge and recorder.



# Deployment models

Below 2 are redundant deployments

Recordings will be load balanced between all recorders.  
(If you have a call bridge cluster ) Then every call bridge will use every recorder.  
You need to license all your boxes with Recorder license.

Image3

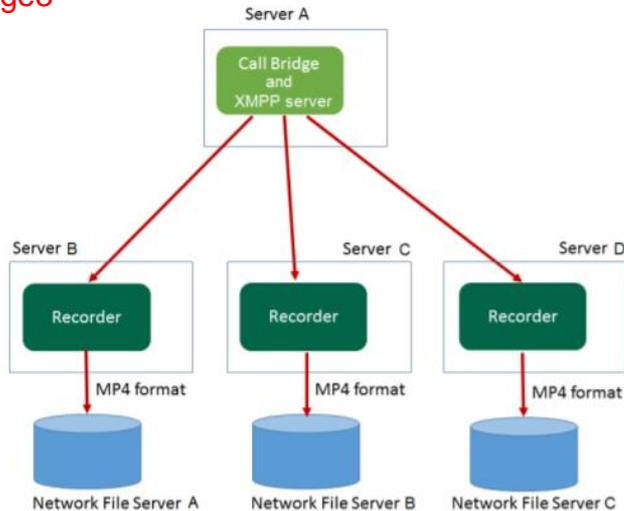
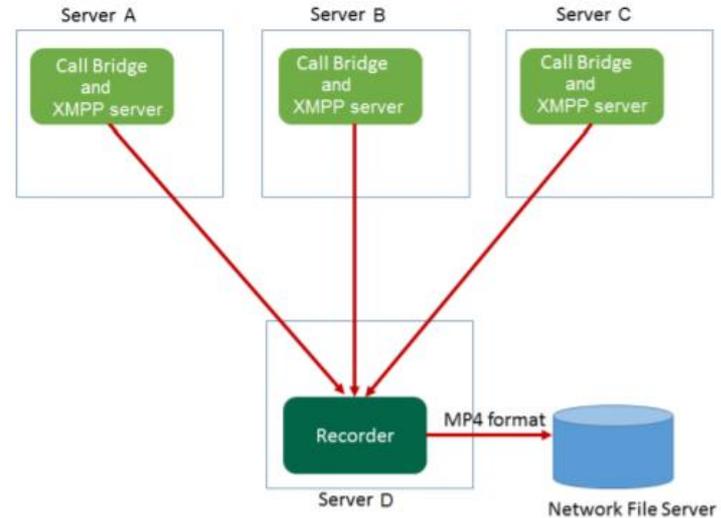


Image4



# Configuration

- Use MMP command to configure Recorder on CMS server.

Example:

```
acanoSVRsingle> recorder ?  
Configure recorder
```

Usage:

```
recorder  
recorder restart  
recorder enable  
recorder disable  
recorder listen <interface[:port] whitelist>  
recorder certs <key-file> <cert-file> [<cert-bundle>]  
recorder certs none  
recorder trust <cert-bundle>  
recorder trust none  
recorder nfs <hostname/IP>:<directory>
```

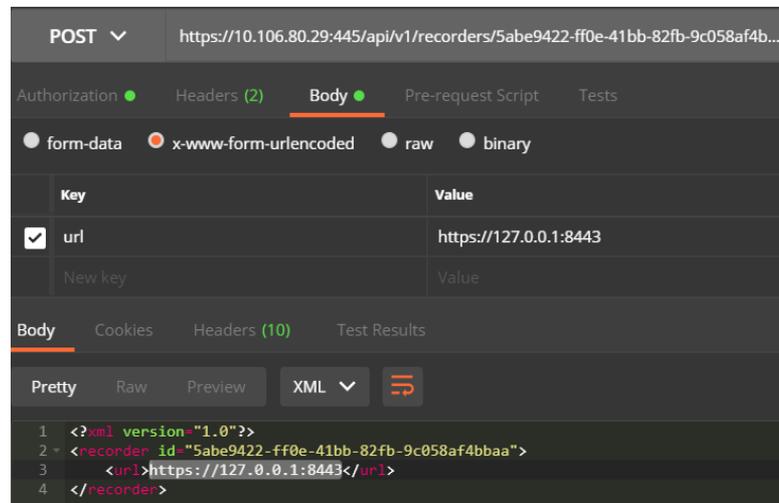
# Configuration

## Basic MMP command configuration flow

- Configure recorder to listen on a network interface **recorder listen <interface[:port] whitelist>**
- Configure certificate for recorder **recorder certs <key-file> <crt-file> [<crt-bundle>]**
- Configure the path for NFS directory **recorder nfs <hostname/IP>:<directory>**
- Configure the Https URL via API, which call bridge will use to contact Recording server.
- API tag /recorders/GUID , do a Post with value url = <https://127.0.0.1:8443> ; where 127.0.0.1 should be replaced with recorder's ip address.

## Working configuration below

```
acanoSVRsingle> recorder
Enabled           : true
Interface whitelist : lo:8443
Key file          : callbridge1.key
Certificate file   : CB1.cer
CA Bundle file    : UCTPROOTCA.cer
Trust bundle      : CB1.cer
NFS domain name   : 10.106.124.200
NFS directory     : /Acanomeetingrecordings
acanoSVRsingle>
```



The screenshot shows a REST client interface for a POST request to `https://10.106.80.29:445/api/v1/recorders/5abe9422-ff0e-41bb-82fb-9c058af4b...`. The request body is set to `x-www-form-urlencoded` and contains a single parameter:

Key	Value
url	https://127.0.0.1:8443

The response is shown in XML format:

```
1 <?xml version="1.0"?>
2 <recorder id="5abe9422-ff0e-41bb-82fb-9c058af4bbaa">
3   <url>https://127.0.0.1:8443</url>
4 </recorder>
```

# Configuration

## How to start recording from clients?

There are 2 ways you can record **Automatic** and **Manual**

**Automatic** - recording occurs without any user intervention, if recording cannot start, the meeting still occurs.

**Manual** - Users can manually start and stop the recording using DTMF.

## How to configure above?

Create a `/callProfiles` and define the recording mode.

Create a `/dtmfProfiles` and define start /stop number to be dialed out from sip client.

Place the `/callProfiles` and `/dtmfProfiles` into `/system/profiles`

# Configuration

Create a /callProfiles and define the recording mode.

Do a Post for /callProfiles with value recordingMode = Manual

The screenshot shows a REST client interface with the following details:

- Method:** POST
- URL:** https://10.106.80.29:445/api/v1/callProfiles/c8411ed6-1dd9-4b6b-a459-4e91fe22a39e
- Body Type:** x-www-form-urlencoded (selected)
- Form Data:**

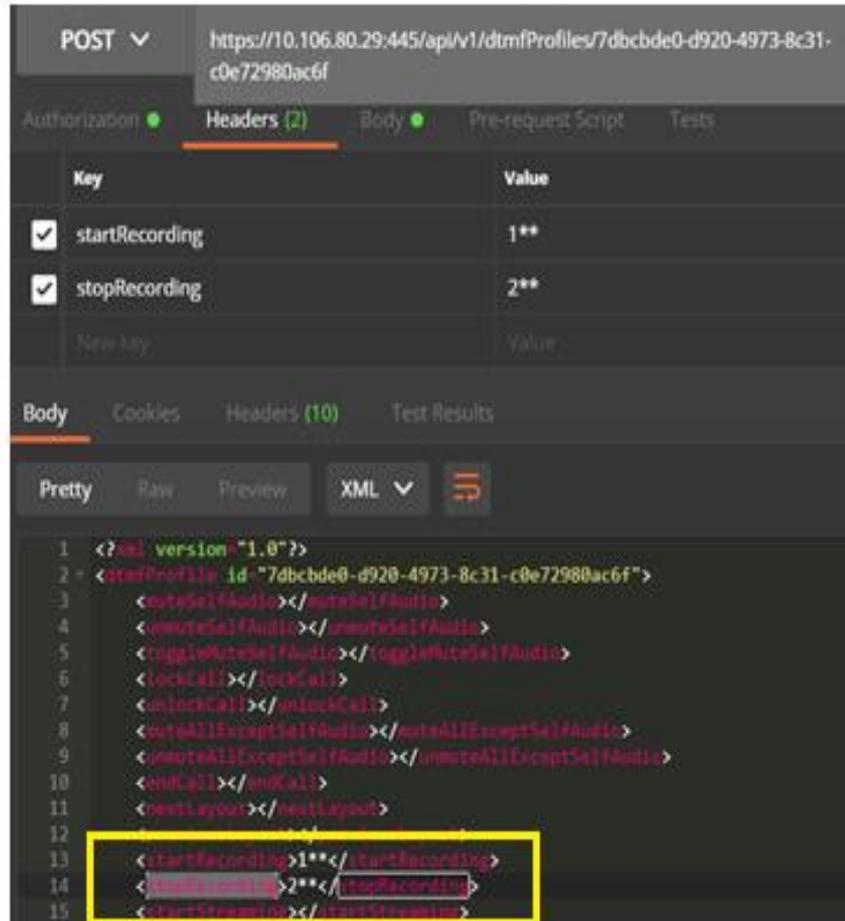
Key	Value
<input checked="" type="checkbox"/> recordingMode	manual
New key	Value
- Response:** XML view showing:

```
1 <?xml version="1.0"?>
2 <callProfile id="c8411ed6-1dd9-4b6b-a459-4e91fe22a39e">
3   <recordingMode>manual</recordingMode>
4 </callProfile>
```

# Configuration

Create a **/dtmfProfiles** and define start/stop number to be dialed out from sip client.

Do a Post for **/dtmfProfiles** with value startRecording = 1\*\*  
stopRecording = 2\*\*



POST `https://10.106.80.29:445/api/v1/dtmfProfiles/7dbcbe0-d920-4973-8c31-c0e72980ac6f`

Authorization Headers (2) Body Pre-request Script Tests

Key	Value
<input checked="" type="checkbox"/> startRecording	1**
<input checked="" type="checkbox"/> stopRecording	2**
New key	Value

Body Cookies Headers (10) Test Results

Pretty Raw Preview XML

```
1 <?xml version="1.0"?>
2 <dtmfProfile id="7dbcbe0-d920-4973-8c31-c0e72980ac6f">
3   <muteSelfAudio></muteSelfAudio>
4   <unmuteSelfAudio></unmuteSelfAudio>
5   <toggleMuteSelfAudio></toggleMuteSelfAudio>
6   <lockCall></lockCall>
7   <unlockCall></unlockCall>
8   <muteAllExceptSelfAudio></muteAllExceptSelfAudio>
9   <unmuteAllExceptSelfAudio></unmuteAllExceptSelfAudio>
10  <endCall></endCall>
11  <nextLayout></nextLayout>
12  <startRecording>1**</startRecording>
13  <stopRecording>2**</stopRecording>
14  <startStreamId></startStreamId>
```

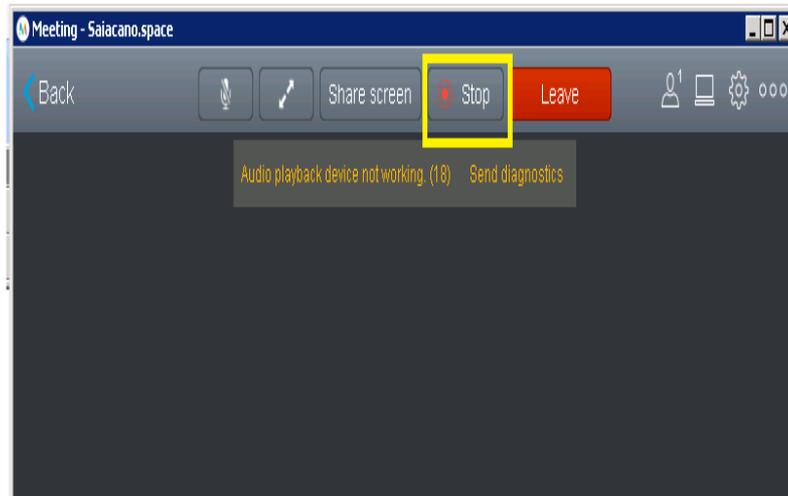
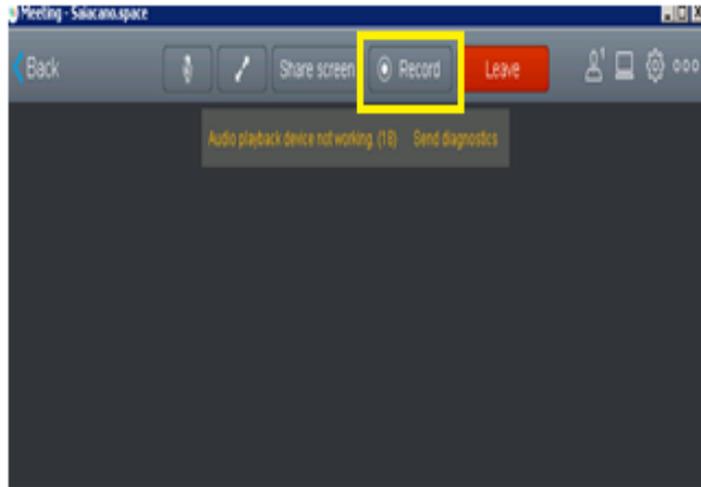
# Configuration

## \*\*\* IMP Note.

DTMF tones are used by SIP devices and webRTC to start and stop recording.

Only CMA clients gets a record button on them to start/stop recording.

Red dot symbolizes that recording has started. Announcement is made.



# Configuration

Add **/callProfiles** and **/dtmfProfiles** to **/system/profiles**

Do a POST API with parameter = **callProfile** and **DtmfProfile** IDs generated.

The screenshot shows a REST client interface for a POST request to `https://10.106.80.29:445/api/v1/system/profiles`. The request body is set to `x-www-form-urlencoded`. The parameters are:

Key	Value
<input checked="" type="checkbox"/> callProfile	c8411ed6-1dd9-4b6b-a459-4e91fe22a39e
<input checked="" type="checkbox"/> dtmfProfile	7dbcdbde0-d920-4973-8c31-c0e72980ac6f
New key	Value

The response body is shown in XML format:

```
1 <?xml version="1.0"?>
2 <profiles>
3   <callLegProfile>377a877d-4bd8-47b4-91ca-1776ed5ad6b9</callLegProfile>
4   <callProfile>c8411ed6-1dd9-4b6b-a459-4e91fe22a39e</callProfile>
5   <dtmfProfile>7dbcdbde0-d920-4973-8c31-c0e72980ac6f</dtmfProfile>
6   <callBrandingProfile>3ec71642-d7d8-4aad-a381-29b25f43a0d6</callBrandingProfile>
7   <ivrBrandingProfile>9c30afb5-bb2d-4d7d-a778-4e1bab576d9f</ivrBrandingProfile>
8 </profiles>
```

# Configuration

How to use the recorder.

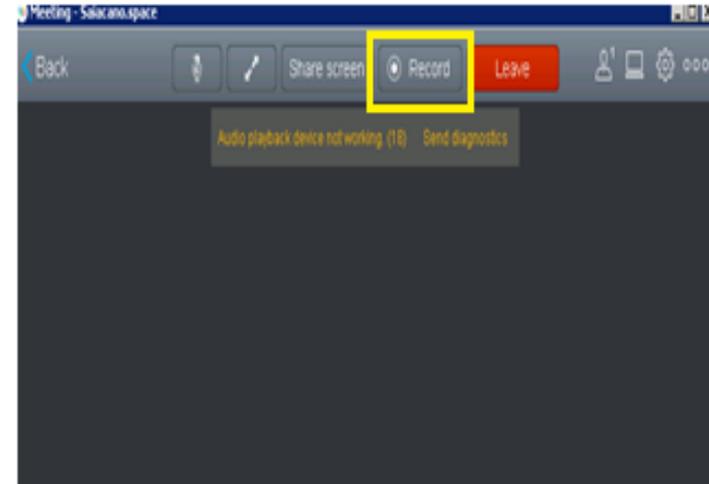
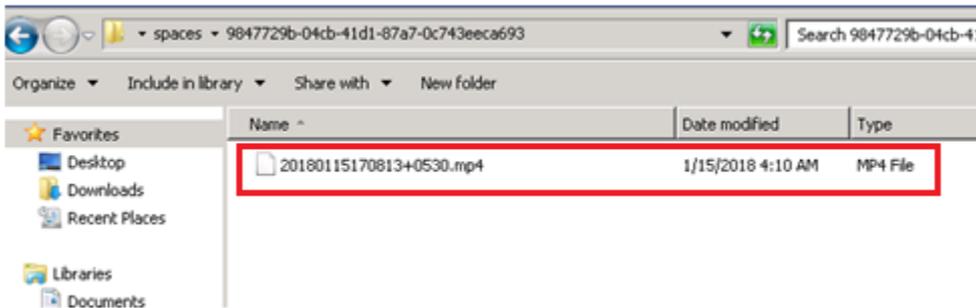
Once configuration is finished, Launch CMA client and make a call into space. Press Recorder button and Recording starts with an Announcement.

From Sip endpoints, you will have to use a touch panel Or remote control to dial

1\*\* to start recording

2\*\* to Stop recording

Once recording is stopped. Call bridge converts the file into MP4 format and saves on NFS server.



# CMS –TMS Integration

# CMS – TMS Integration

- Cisco Meeting Server like any other MCU can be integrated with TMS.
- This integration helps us in scheduling meetings using TMS on CMS, using CMS resources.
- TMS 15.3 above and CMS 2.0 above is needed.
- You need to add CMS on TMS as shown below IPAddressOfCms:445  
445 is webadmin port

The screenshot shows the 'Add by Address' tab in the Cisco Meeting Server configuration interface. The 'Specify Systems by IP Addresses or DNS Names' section contains a text input field with the IP address '10.106.80.34:445' entered. A red box highlights this input. Below this, the 'Location Settings' section shows 'ISDN Zone' set to 'ricky', 'IP Zone' set to 'ricky', and 'Time Zone' set to '(UTC-08:00) Baja California'. The 'Advanced Settings' section includes a note: 'It is mandatory to enter valid Username and Password for all Cisco Meeting Servers.' Below this note, the 'Username' field is set to 'admin' and the 'Password' field is filled with dots. A red box highlights the 'Username' and 'Password' fields. Other settings include 'SNMP Community Names' set to 'public,Public', 'Persistent Template' set to 'No Template', and 'Usage Type' set to 'Meeting Room'.

# CMS – TMS Integration

-Once CMS is added, we can see status of CMS.

The screenshot shows the Cisco Meeting Server interface. On the left is a 'Navigator' pane with a 'Folder View' showing a tree structure: 'Company Name' > 'Discovered Systems' > 'CMS-Cluster' > 'splitdepc'. The main pane displays details for the 'splitdepc' node, identified as a 'Cisco Meeting Server'. The status is 'Idle', the address is '10.106.80.34:445', and the connectivity is 'Reachable on LAN'. Below this, there are tabs for 'Summary', 'Settings', 'Clustering', 'Connection', 'Permissions', and 'Logs'. The 'Summary' tab is active, showing a 'Tickets' section with a green checkmark and the text 'System has no open or acknowledged tickets'. There are links for 'Add custom ticket', 'Open in Ticketing Service', and 'Edit settings'.

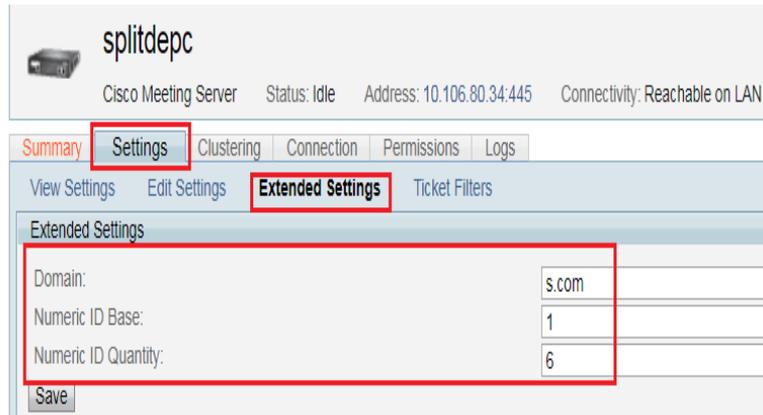
- All subsequent CMS cluster nodes gets added automatically under clustering tab.

The screenshot shows the 'Clustering' tab for the 'splitdepc' node. The node is identified as a 'Cisco Meeting Server' with status 'Idle', address '10.106.80.34:445', and connectivity 'Reachable on LAN'. The 'Clustering' tab is active, showing a table of cluster nodes. The table has two columns: 'System Name' and 'Primary'. The first row shows 'splitdepc' with a green checkmark in the 'Primary' column. The second row shows '10.106.80.47:445' and the third row shows '10.106.80.48:445'. The 'splitdepc' and 'Primary' labels are highlighted with red boxes.

System Name	Primary
splitdepc	✓
10.106.80.47:445	
10.106.80.48:445	

# CMS – TMS Integration

- Once CMS is added on TMS, you can define Domain, Numeric ID Base and Numeric ID Quantity.
- TMS Scheduled meetings gets created on CMS.



splitdepc  
Cisco Meeting Server Status: Idle Address: 10.106.80.34:445 Connectivity: Reachable on LAN

Summary **Settings** Clustering Connection Permissions Logs

View Settings Edit Settings **Extended Settings** Ticket Filters

Extended Settings

Domain: s.com

Numeric ID Base: 1

Numeric ID Quantity: 6

Save

## Meetings Gets created on CMS

### Space configuration

Filter  Submit

	Name	URI user part	Secondary URI user part	Additional access methods	Call ID
<input type="checkbox"/>	7777	7777			7777
<input type="checkbox"/>	8888	8888			8888
<input type="checkbox"/>	9999	9999			9999
<input type="checkbox"/>	Saiacano's space	saiacano.cs			036707688
<input type="checkbox"/>	TMS_Scheduled_Meeting_1	1			1
<input type="checkbox"/>	TMS_Scheduled_Meeting_2	2			2
<input type="checkbox"/>	TMS_Scheduled_Meeting_3	3			3
<input type="checkbox"/>	TMS_Scheduled_Meeting_4	4			4
<input type="checkbox"/>	TMS_Scheduled_Meeting_5	5			5
<input type="checkbox"/>	TMS_Scheduled_Meeting_6	6			6

# Questions ?????