Cisco Meeting Server Webinar Session 2

January, 2018

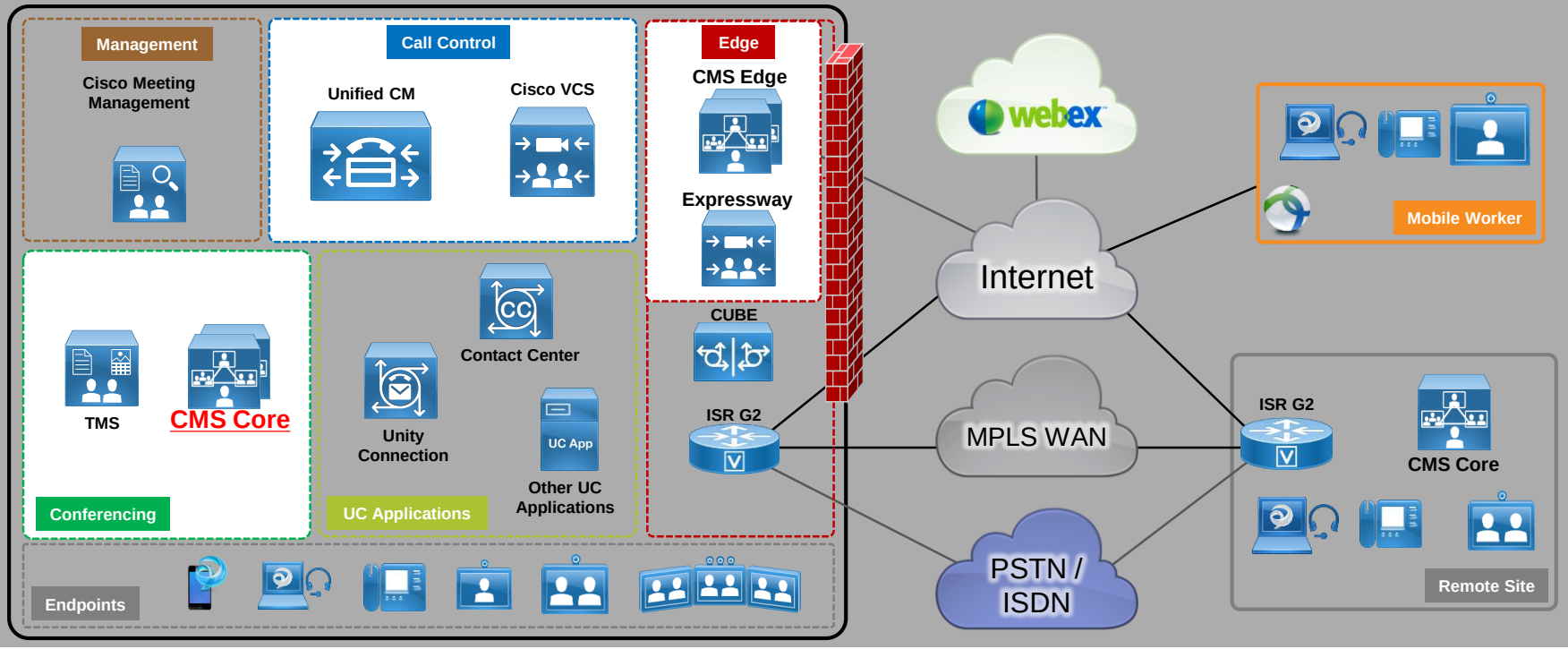
Vikram Dutta

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)

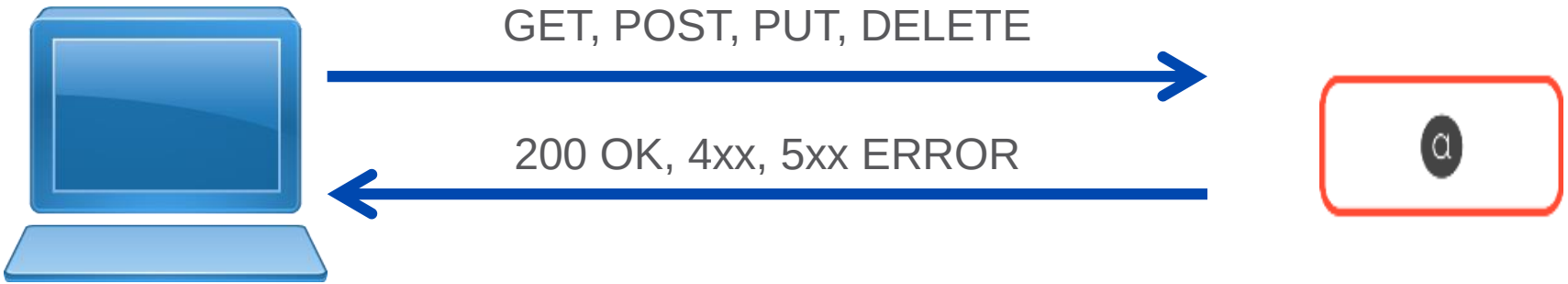
Cisco Meeting Server can be configured in 3 ways:

- 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

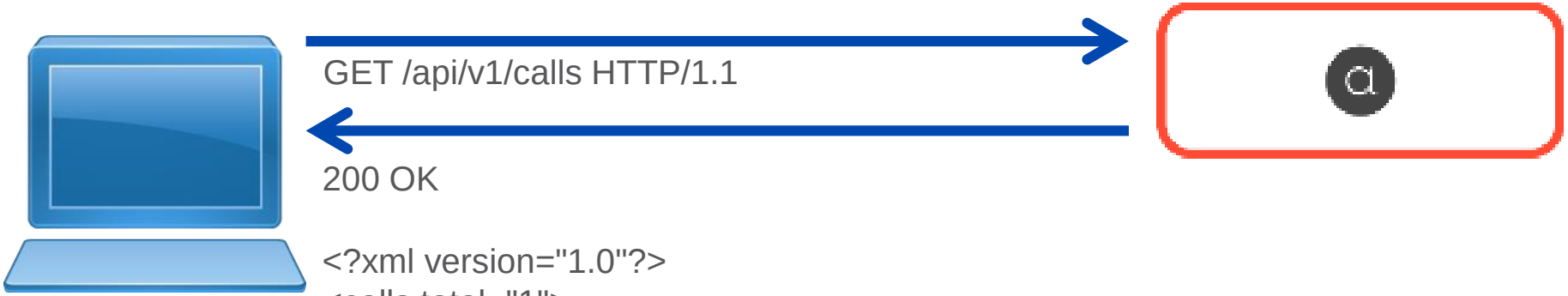
200 OK
Location: /api/v1/coSpaces/f11f1c23-ff75-49d1-af8c-384a404f1f26

Filter Submit

	Name	URI user part	Secondary URI user part	Additional access methods	Call ID
☐	APICoSpace	9000			9000

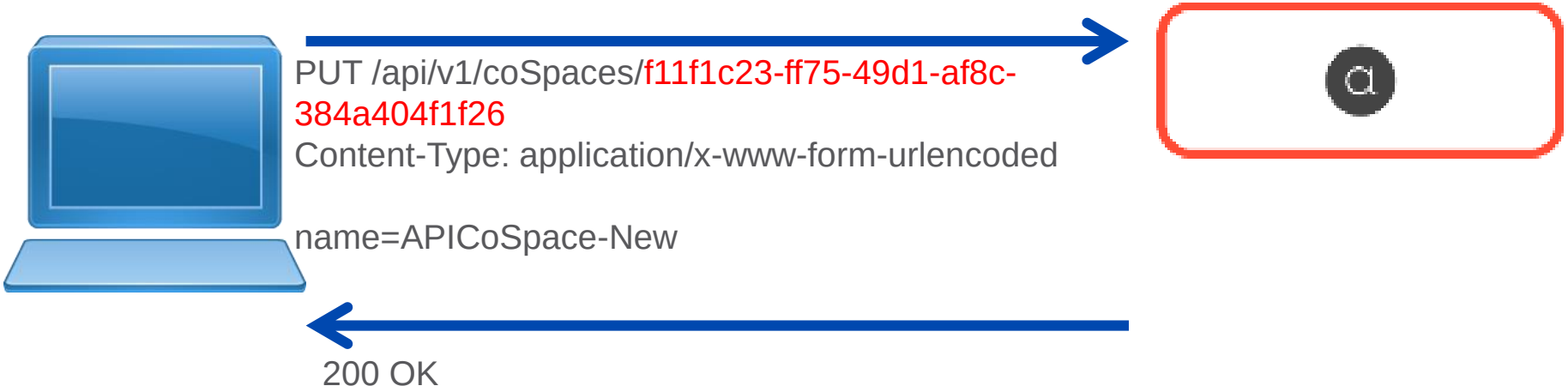
HTTP GET

- Retrieves existing information
- No Content in Body



HTTP PUT

- Modifies existing object

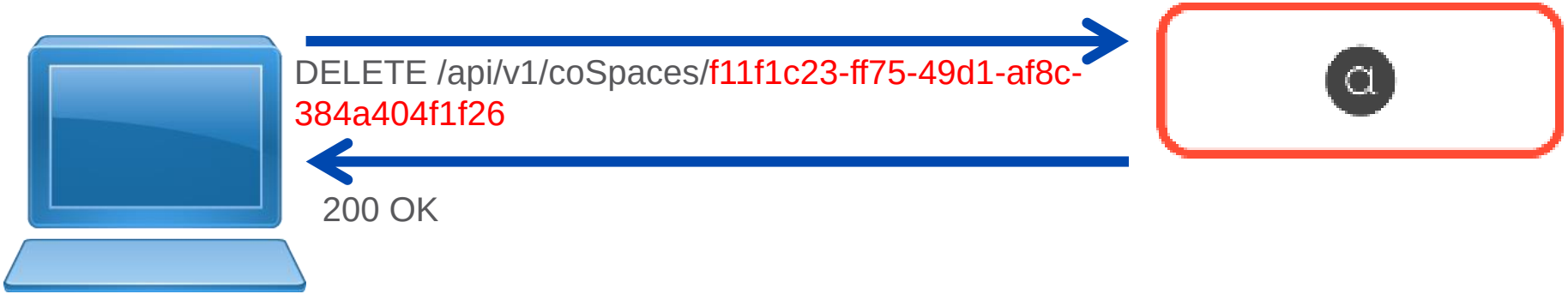


Filter Submit

	Name	URI user part	Secondary URI user part	Additional access methods	Call ID
☐	APICoSpace-New	9000			9000

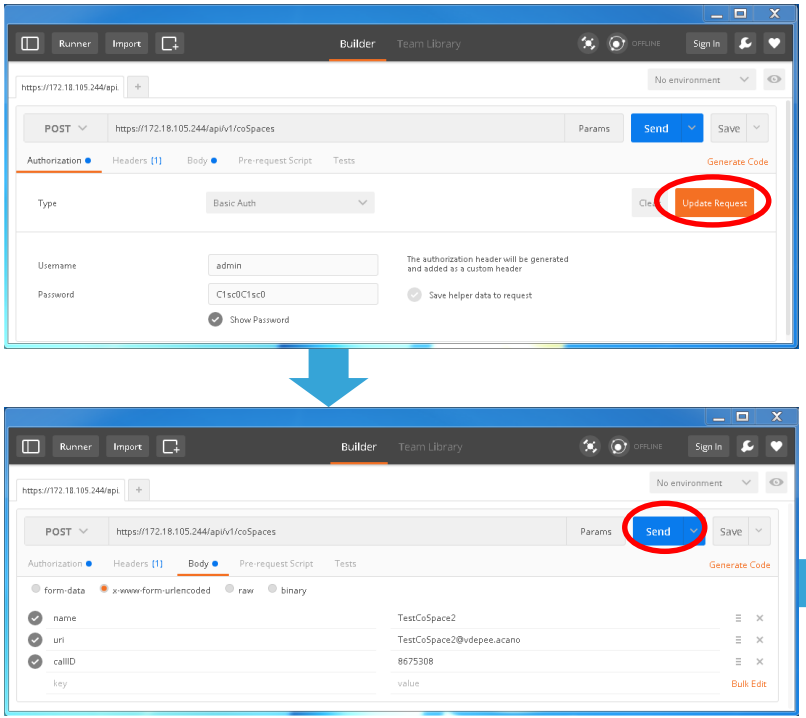
HTTP DELETE

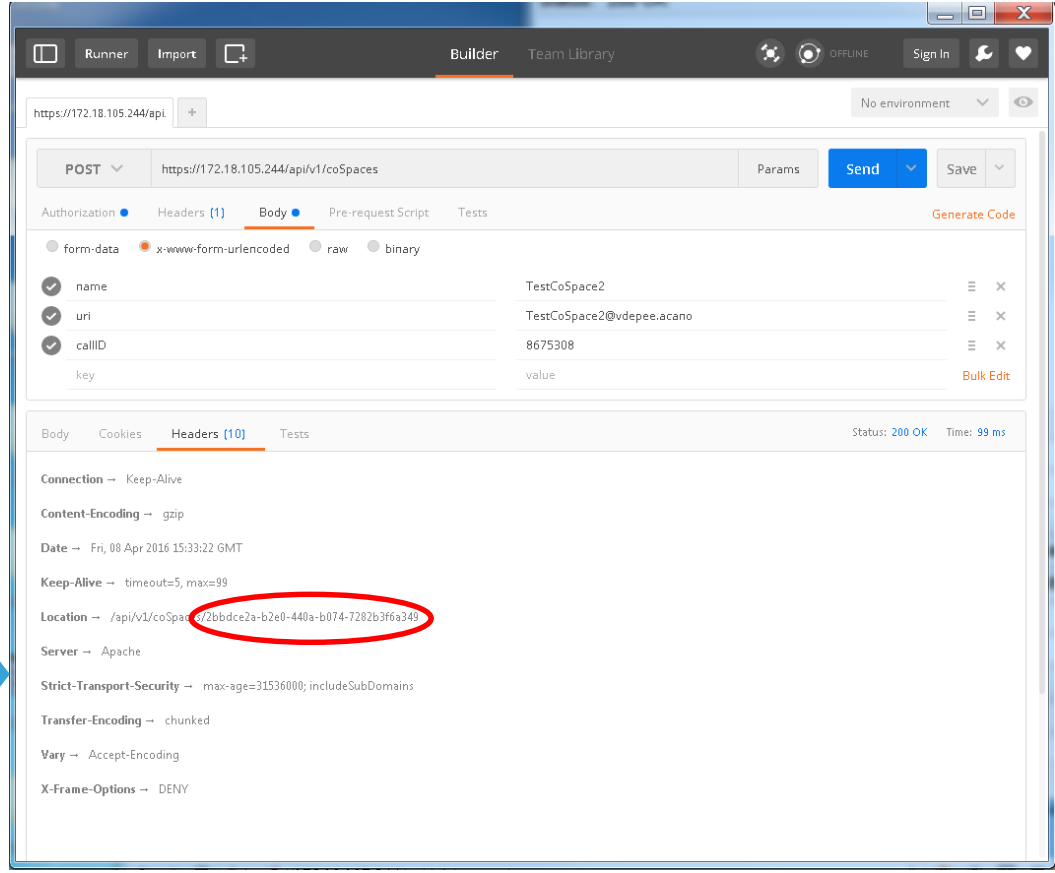
- Destroys an object



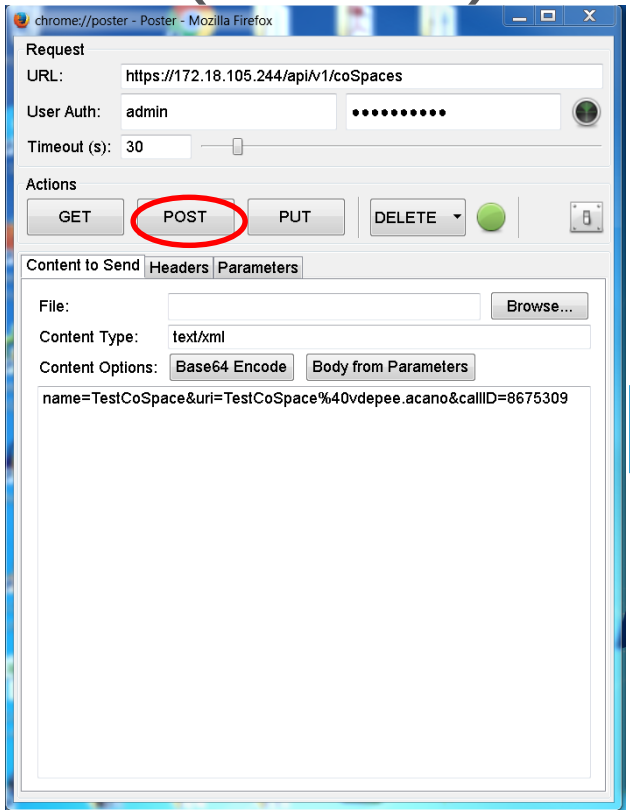
	Name	URI user part	Call ID

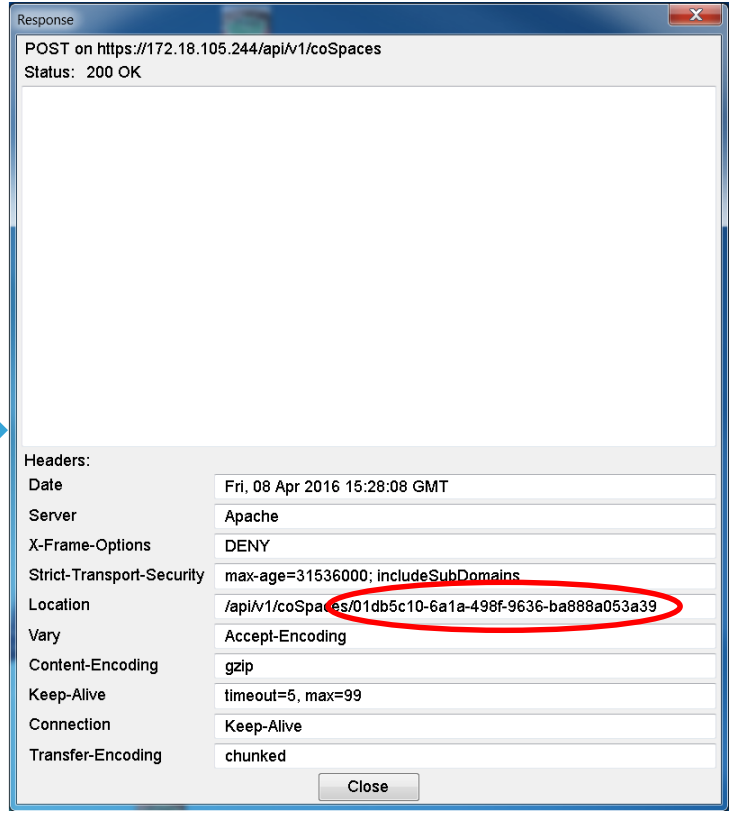
Postman (Chrome)





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?

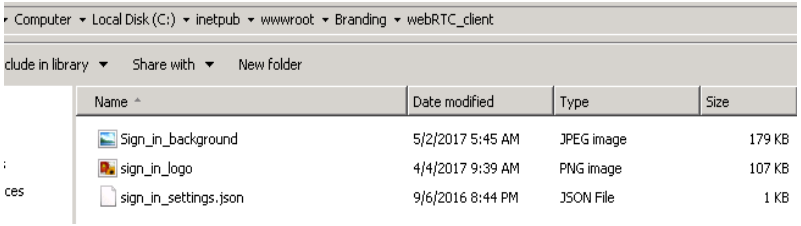
- Web Server is required (Windows server with IIS will be enough)
- Create directories on webserver in which all branding files will be placed.
  (.wav, jpg, png or archive (e.g. zip) files can be stored
- Web server should be reachable from call bridge and there should be no http authentication enabled.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

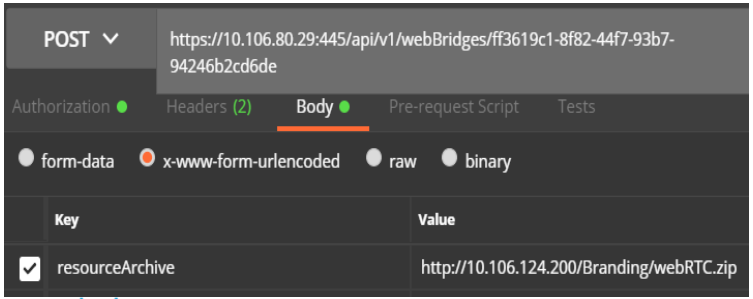
C:\inetpub\wwwroot\Branding

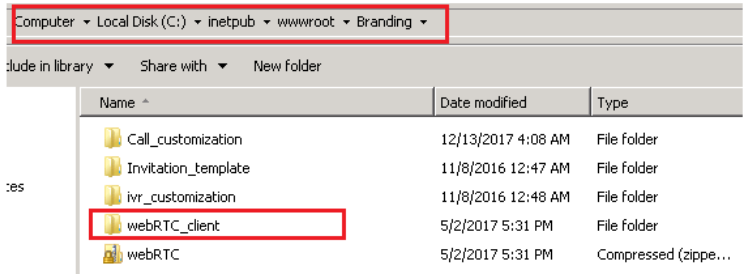
Then we need to run a POST method on **/webBridges**

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





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

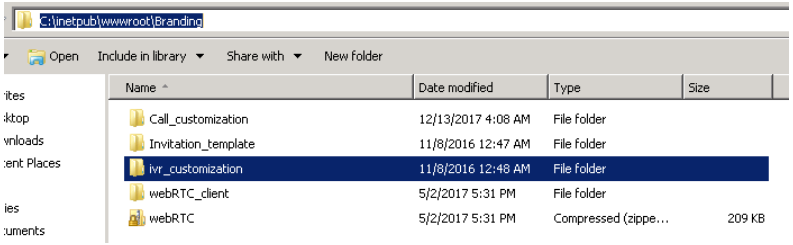
Branding and Customization

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.



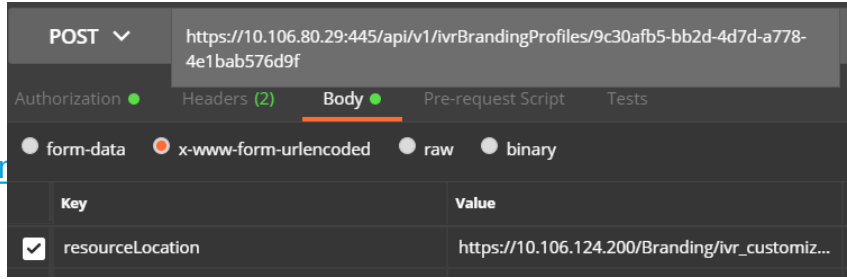
https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-programming-reference-guides-list.html

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_customizatior

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?

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

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

Branding and Customization

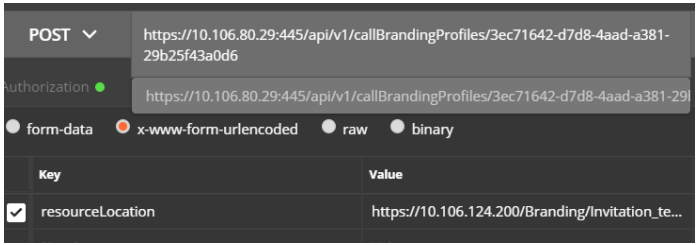
How to do sip/lync call customization

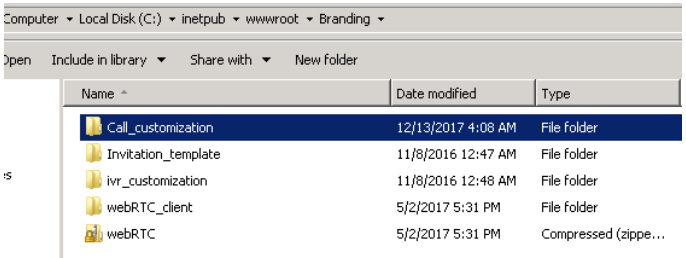
Create a folder “Call_customization” at below location and place your wav files in the folder.

C:\inetpub\wwwroot\Branding

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

resourceLocation= https://10.106.124.200/Branding/Invitation_template.txt

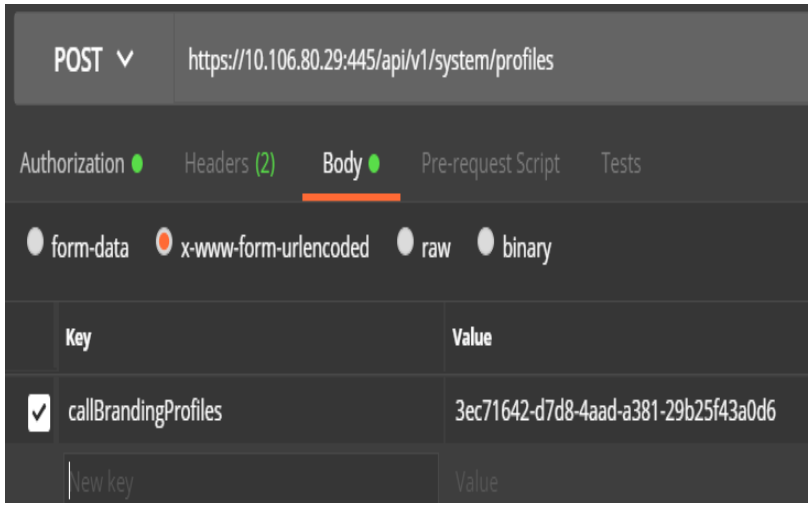




Branding and Customization

SIP/Lync Call Message Customization

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



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

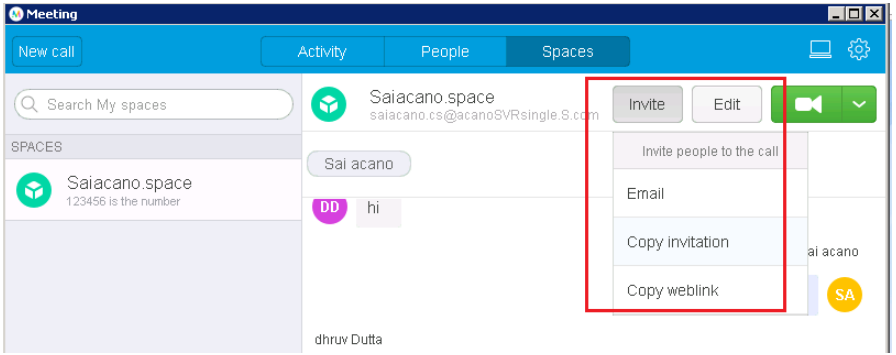
To join from an Android Device, click here: https://bharat.tptac9.com/invited.sf?secret=2D5Ha5d48t9ptkJbSznFsw&id=776655

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

Jabber or Lync Client, Dial: 776655@tptac9.com

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



Branding and Customization

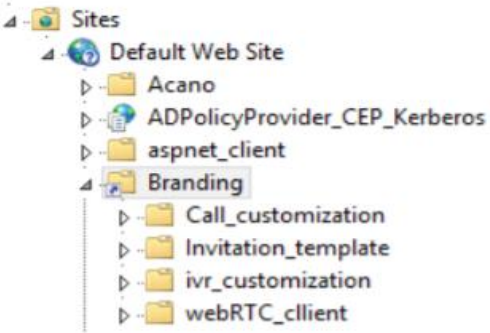
Branding Summary:

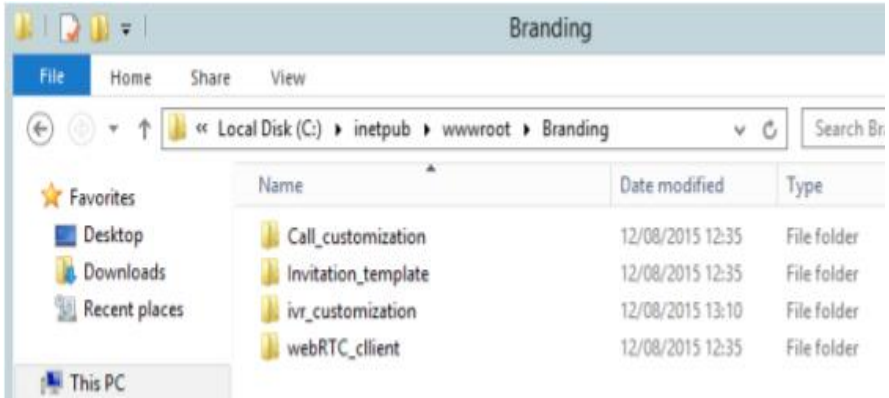
Make sure IIS is running on windows webserver with no authentication enabled.

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.

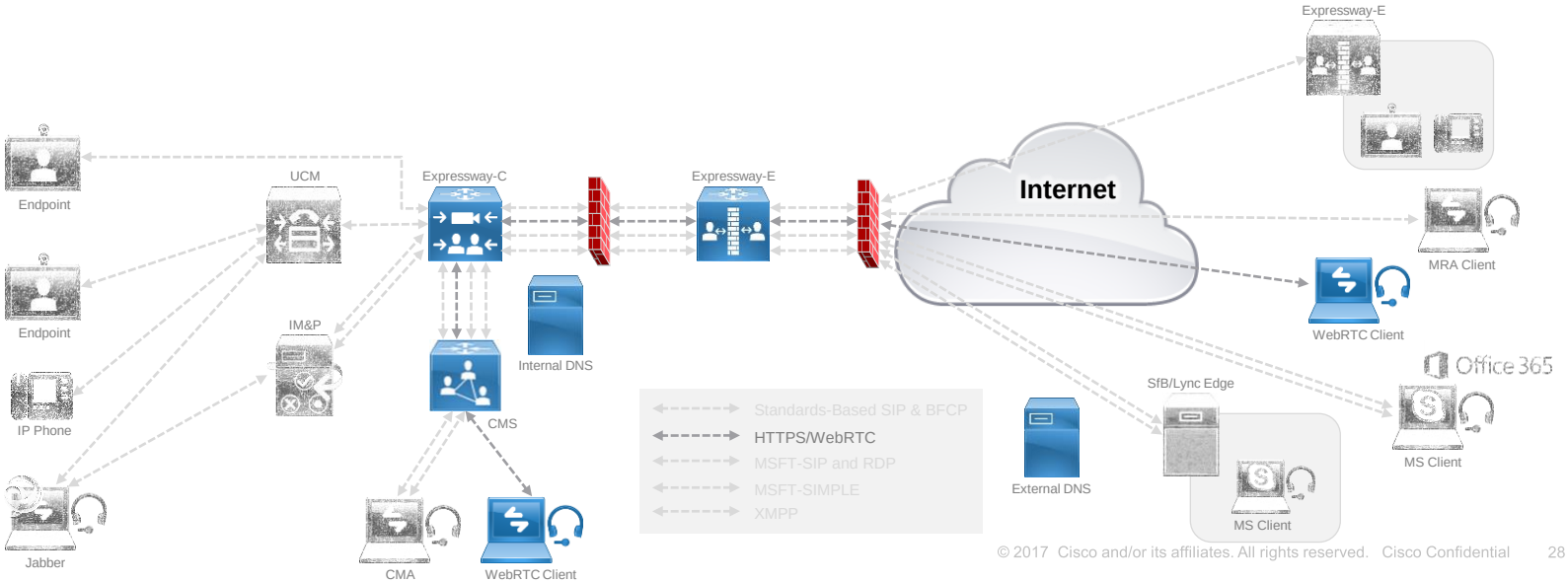
Check output.

Expressway proxy for WebRTC

Single Edge Solution

- **Single Expressway Edge for Cisco Meeting Server deployments**
  - ➢ WebRTC Clients (CMS Web Proxy)

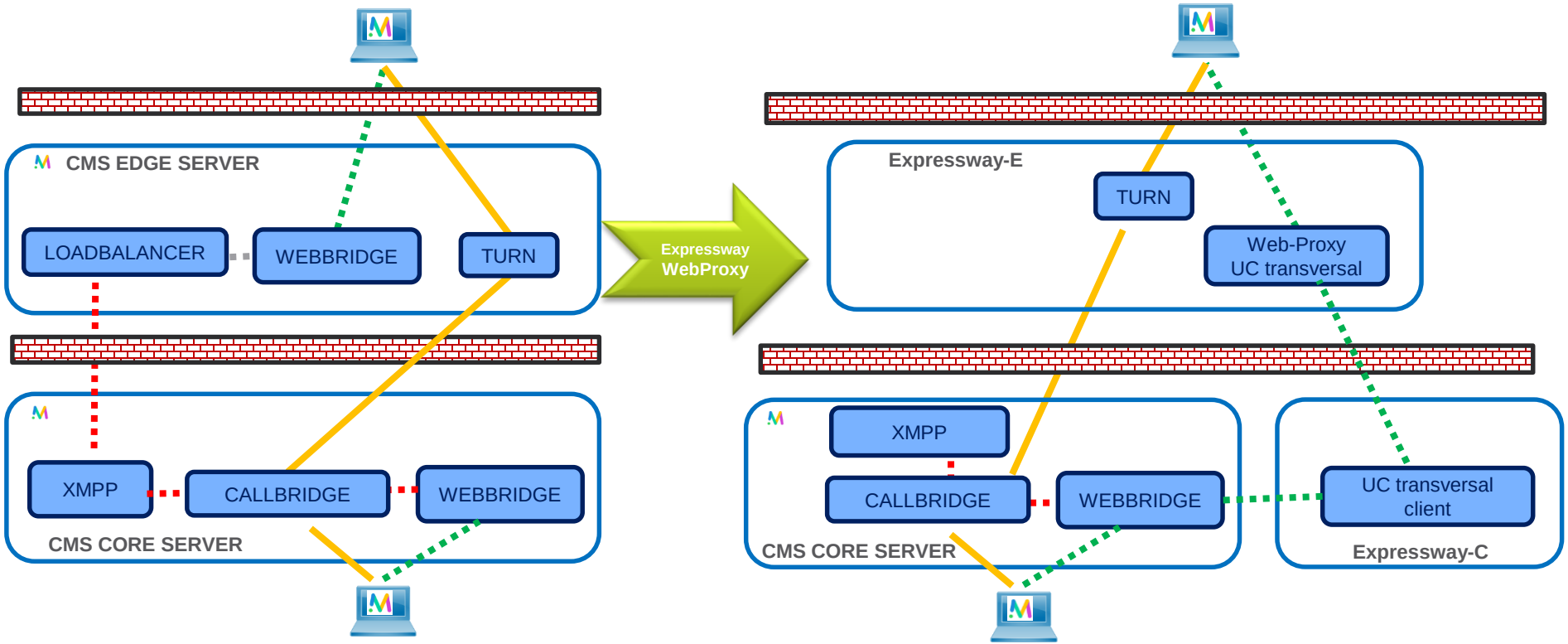
    - Enables external users to join CMS spaces using browser. (chrome only)
    - External users would only need Join URL and passcode (if configured) to connect to CMS space.



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



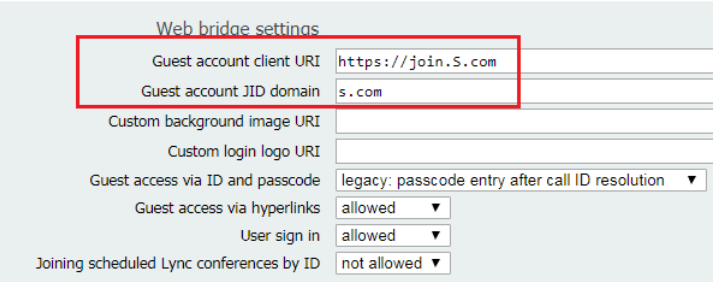
30

Single Edge Solution

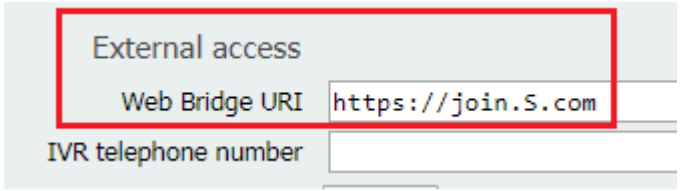
High level configuration overview on CMS

- 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.

```
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
```



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



Single Edge Solution

High level configuration overview on CMS

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

```
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
```

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

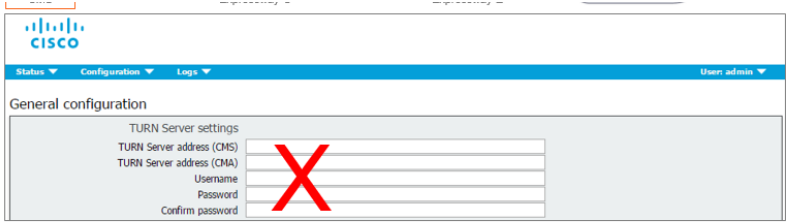
- Make sure Call id is configured on CMS space. (passcode not mandate)

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

IMPORTANT: Configure TCP/TURN port to "3478"

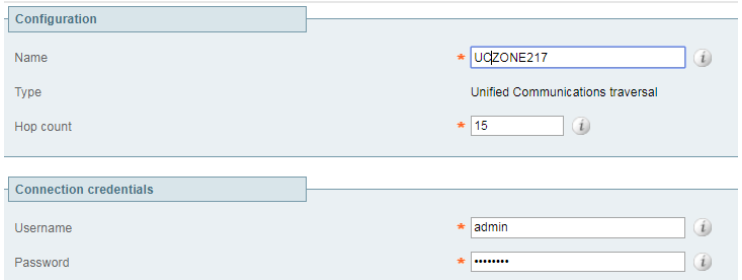
- Example configuration results should look like below. (Note My ExpresswayE is single nic, thus client/server ip are same)

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

Single Edge Solution

High level configuration overview on Expressway C

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



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

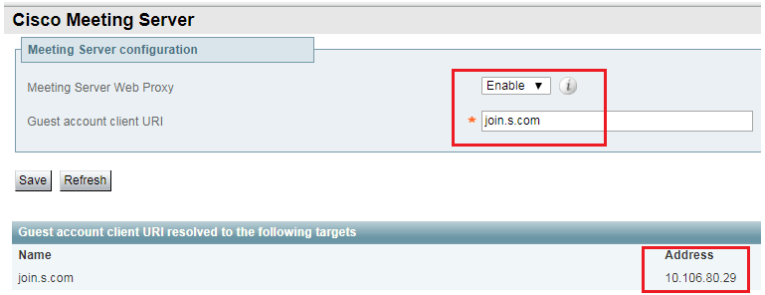
```
X509v3 extensions:
    X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
    X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
    X509v3 Subject Alternative Name:
        DNS:VCS8C.s.com, DNS:VCS8Master.S.com, DNS:federation.com, 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**

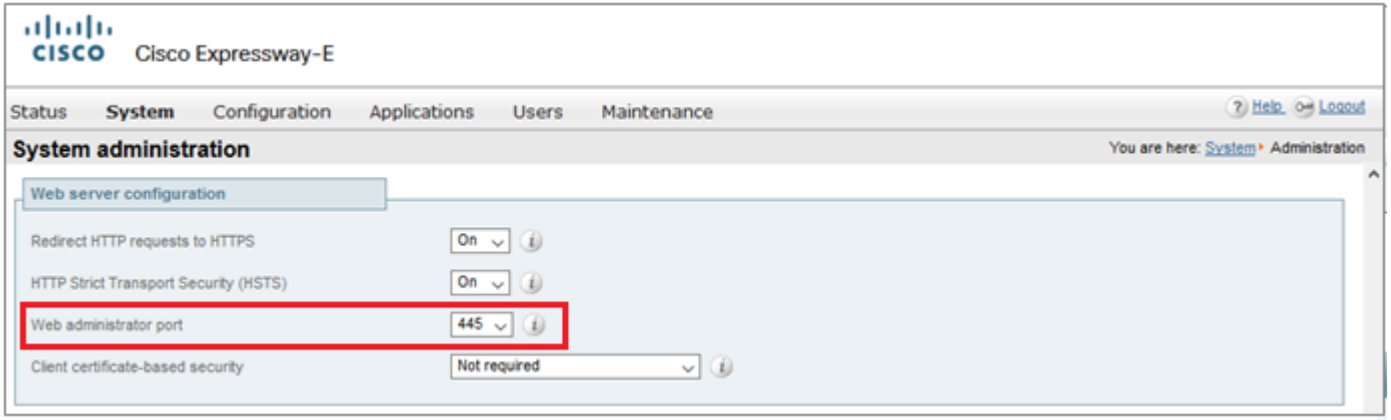
- **Add CMS on Expressway C.**



Single Edge Solution

High level configuration overview on Expressway C

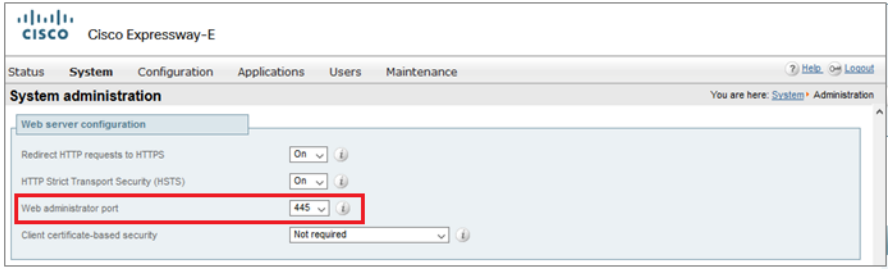
- **Change administration port on Expressway C. You can change the port from CLI to any other port.(gui only support 445 or 443)**



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:acanoSVRsingle.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:C9:0B:70:AD:69:09:C9:BF:E2:28
```

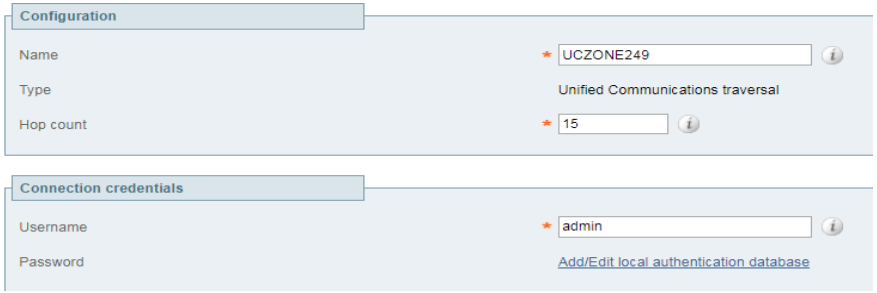
If Join URL is not present in san, a certificate warning will always appear on browser while accessing webrtc link

Single Edge Solution

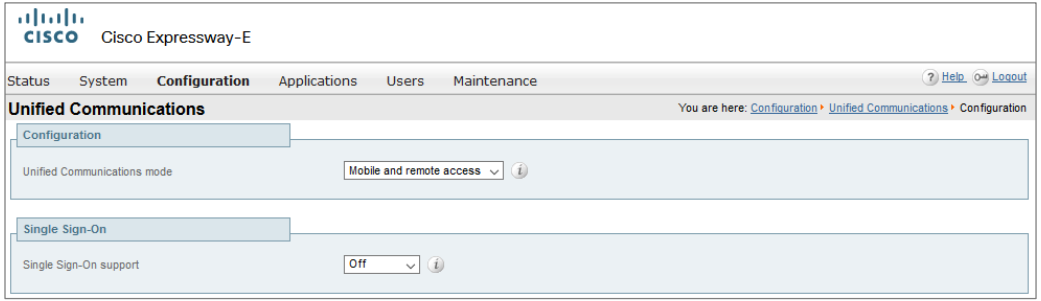
High level configuration overview on Expressway E

- Create Unified traversal zone on Expressway E

-



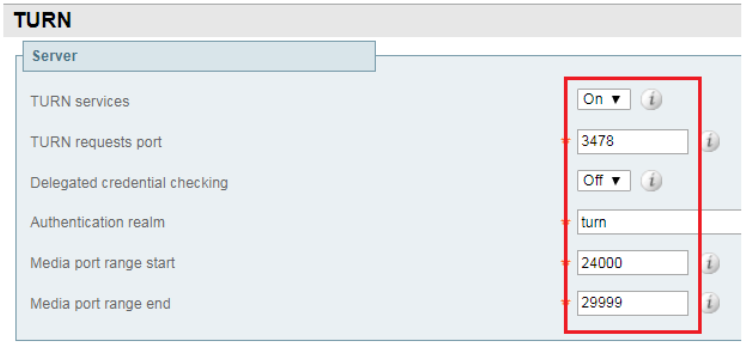
Enabled Mobile and Remote Access mode



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.



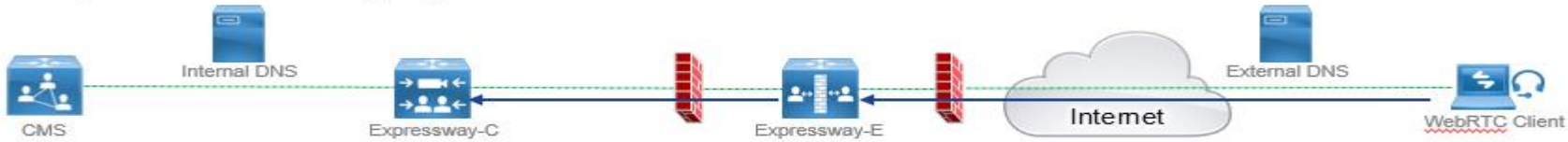
-

- 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

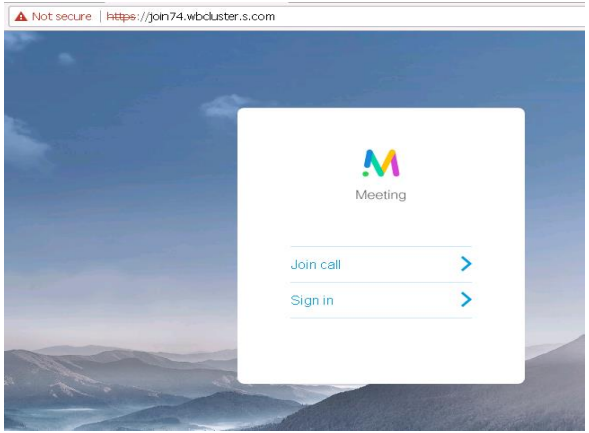
High level Call flow:



- 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 f etches all web browser headers.

-

```
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/ HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/bundle.min.js HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/graphics/logo_cma_a.svg HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/app.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/common.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/animations.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/extension.js HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/typography.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/palettes.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/defaults.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/utilities.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/headings.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/layers.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/effects.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/contexts.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/modules.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/coApps.css HTTP/1.1
|GET http://vcs_control.uc.ciscotp.com:8443/LUNNUy0/css/guest.css HTTP/1.1
```

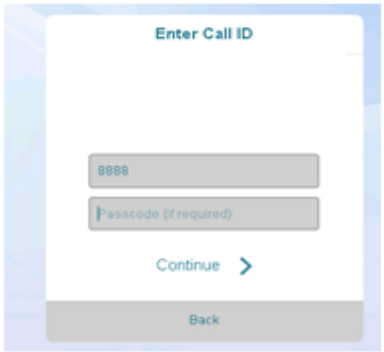


Single Edge Solution

High level Call flow:

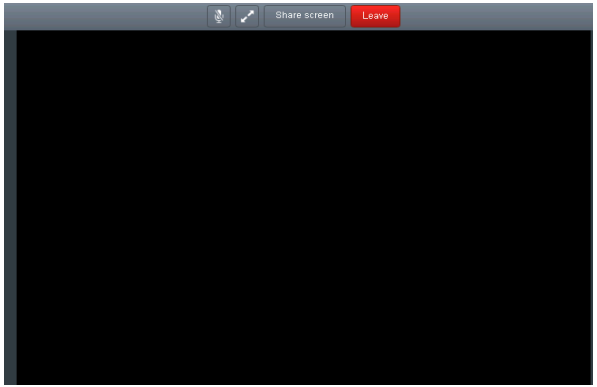
- Once “join” tab appears . Please enter “call Id” (passcode if configured on cms) next.
- Enter a friendly name
- Join the call.

-



>

>



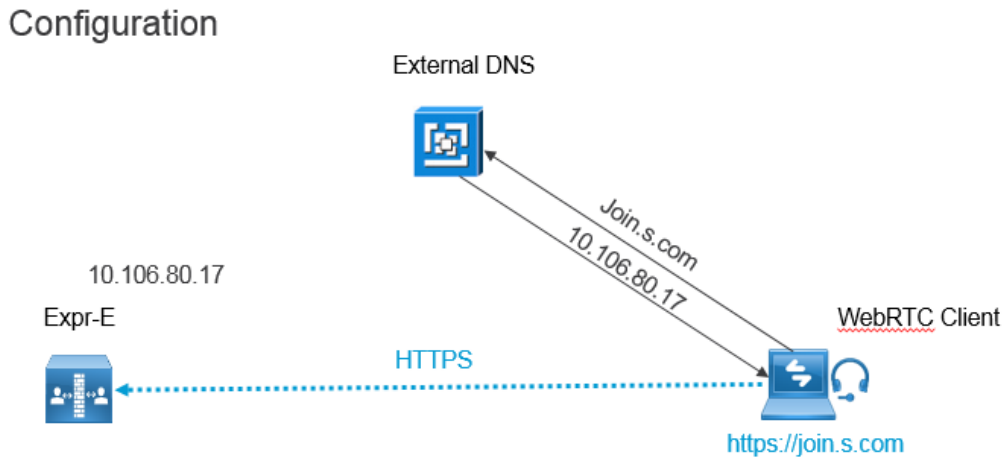
Single Edge Solution

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.



-

Single Edge Solution

High level Call flow:

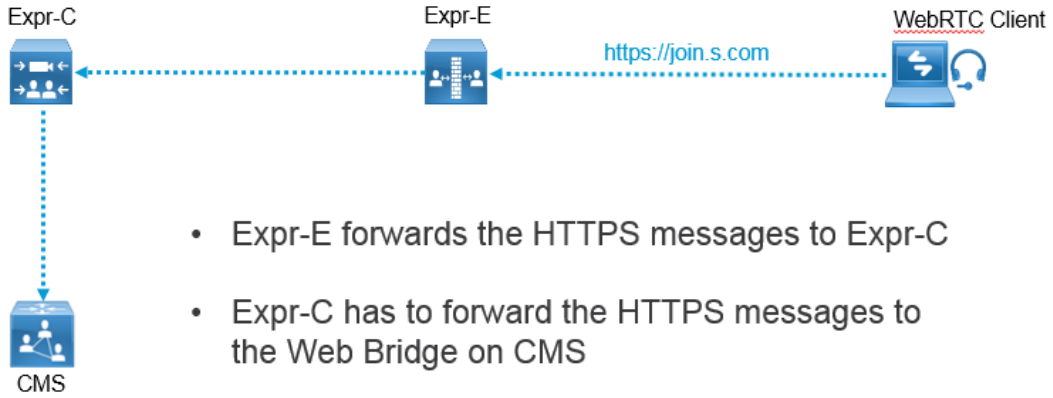
IMP***

Expressway C should be able to resolve

Join URL into CMS webbridge ip address

Internally.

-

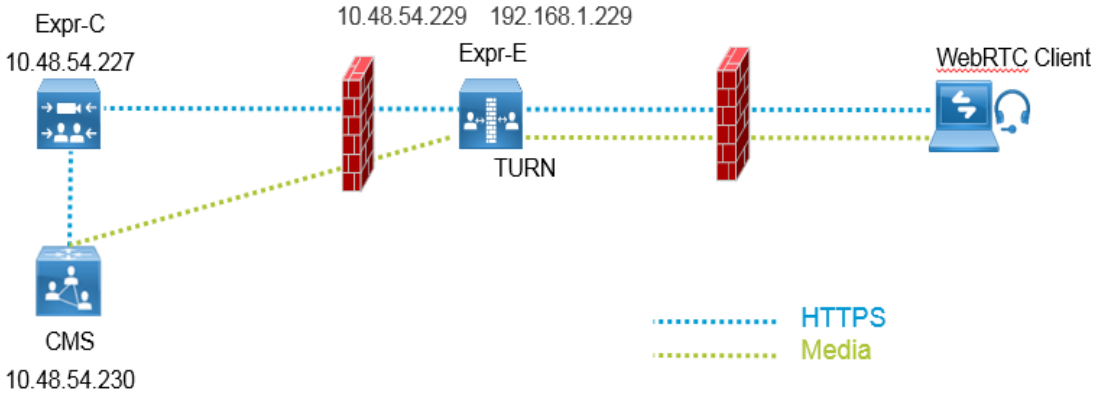


Single Edge Solution

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.



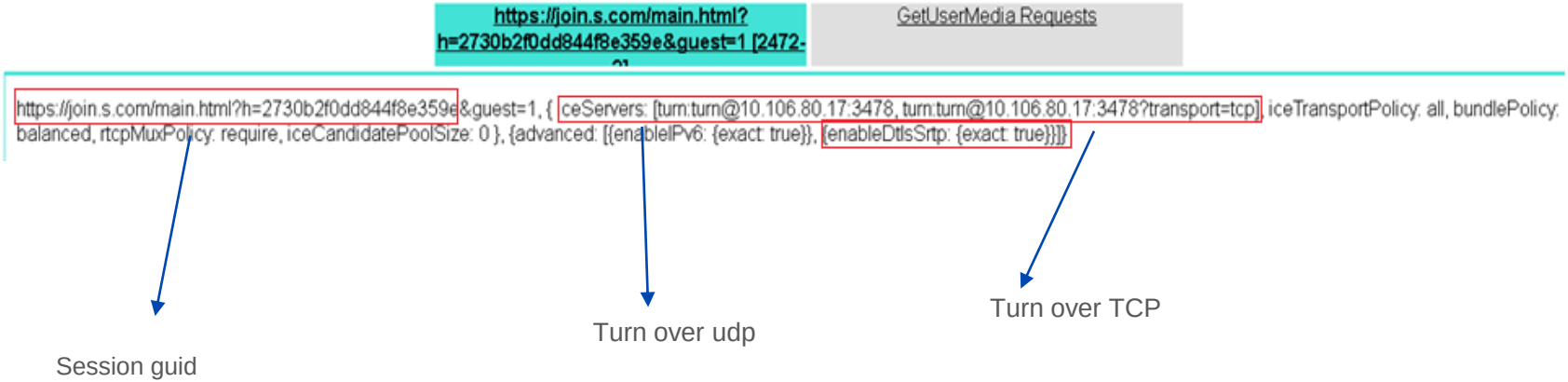
-

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/

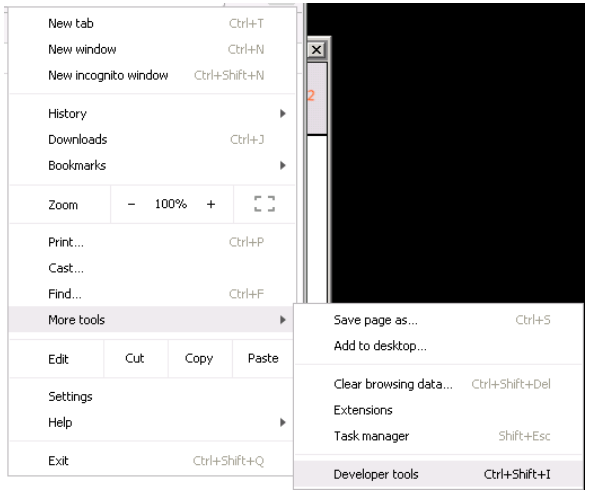
Digging further we see relay candidates offered.

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

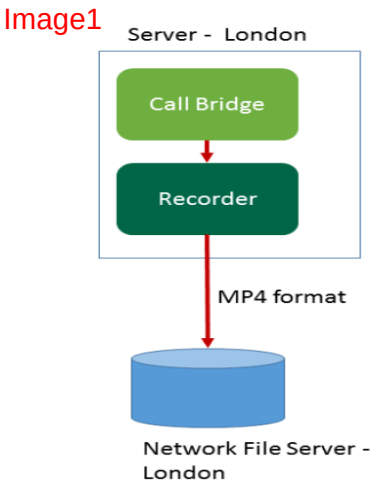
Recorder can be deployed in 2 ways.

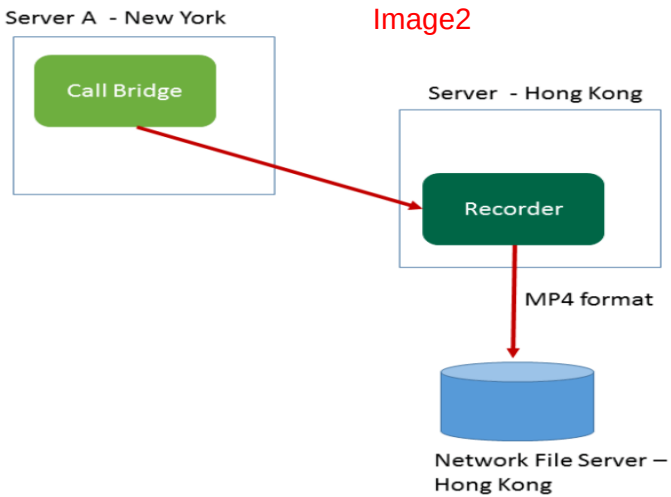
- Recorder can **co-locate** along with call bridge on same box. (Such deployment is not recommended for productions)
- Recorder component can exist on a **separate server** which should be reachable by call bridge.
- You can have a **redundant** setup for recorders and call bridges.
- Recorder and NFS 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 coverts 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

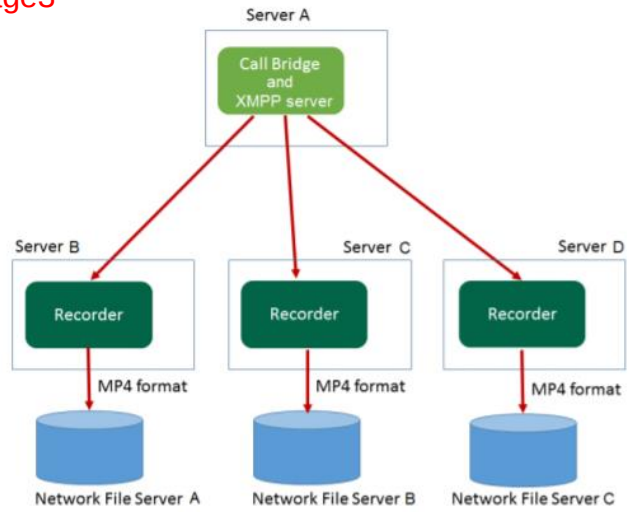
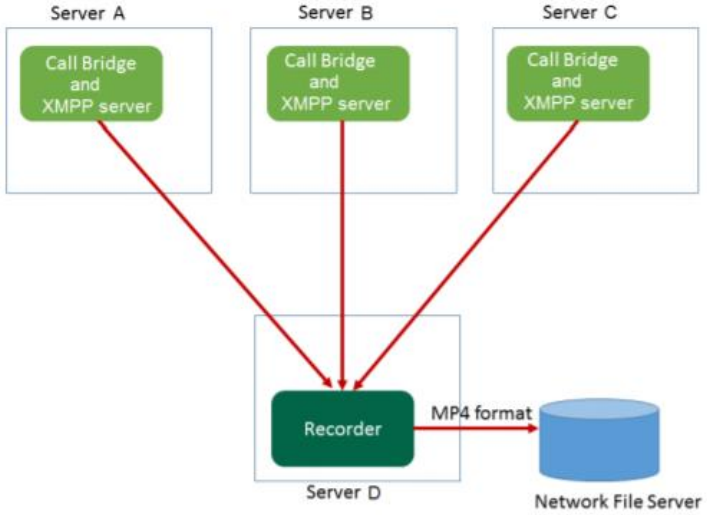


Image4



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> <crt-file> [<crt-bundle>]
  recorder certs none
  recorder trust <crt-bundle>
  recorder trust none
  recorder nfs <hostname/IP>:<directory>

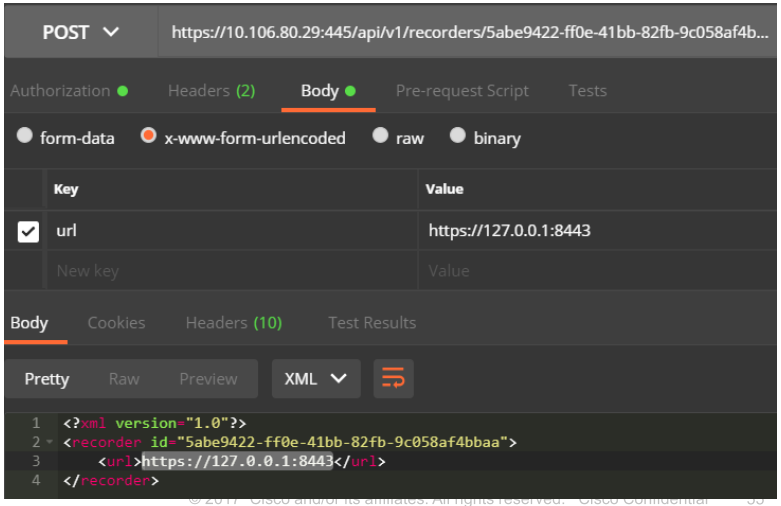
Configuration

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>
```



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.

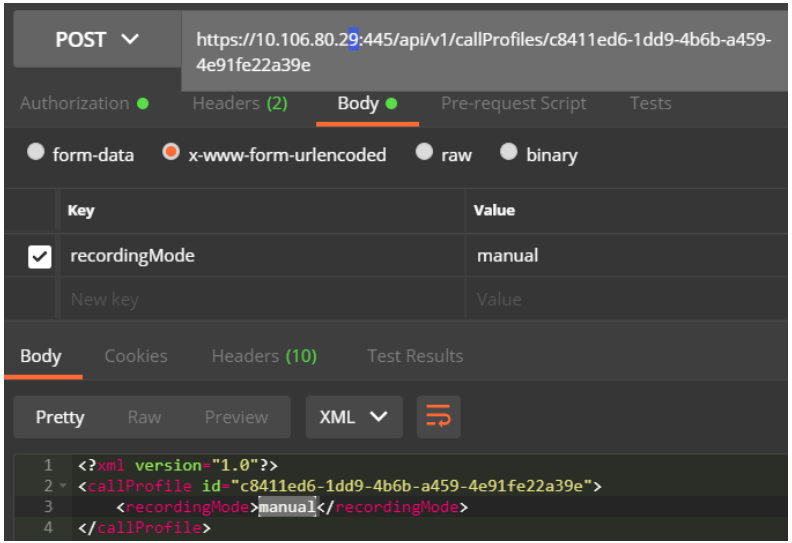
How to configure above?

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.

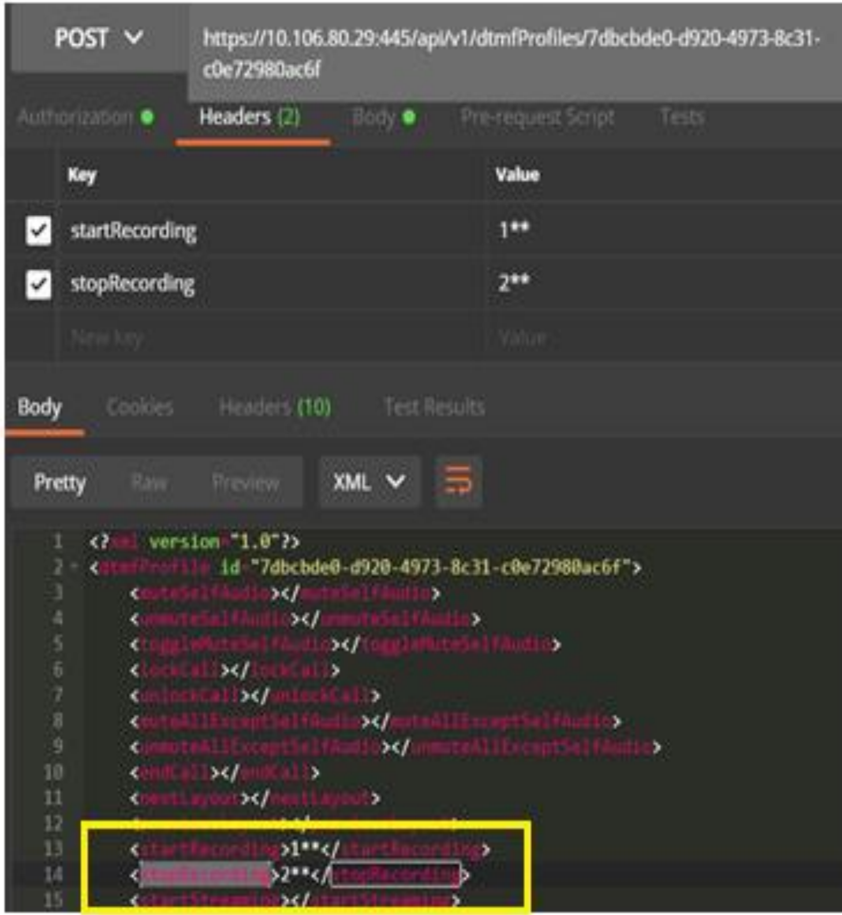
Do a Post for /callProfiles with value recordingMode = Manual



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**



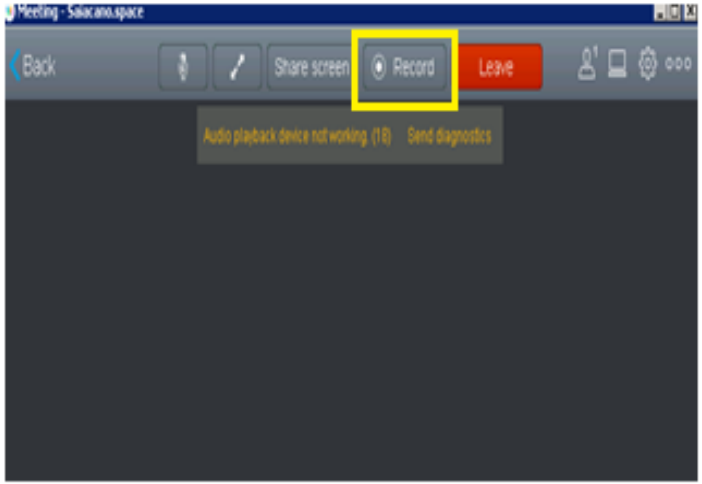
Configuration

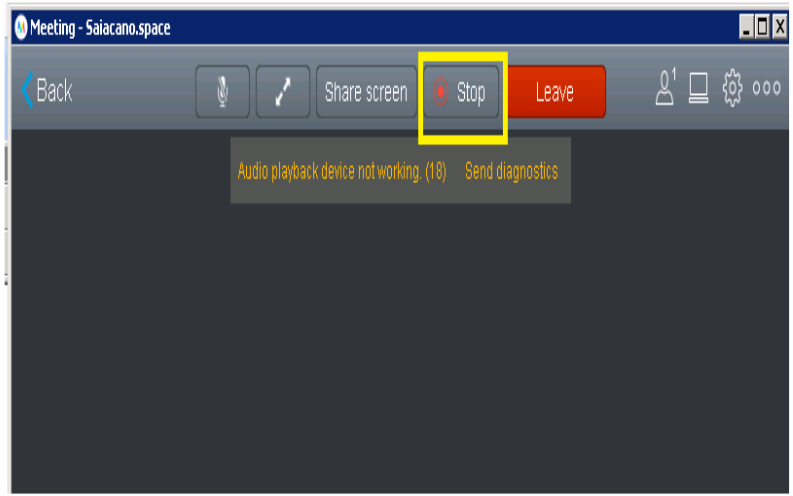
***** IMP Note.**

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.

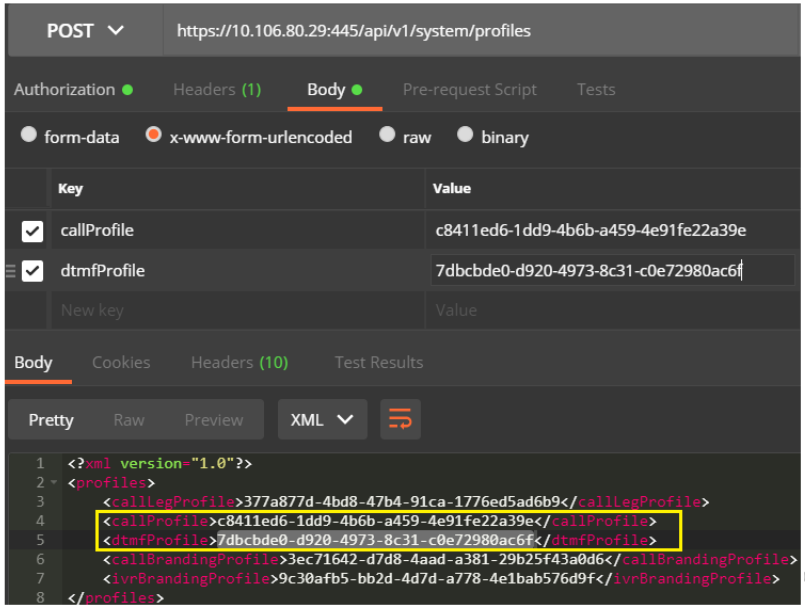




Configuration

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

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

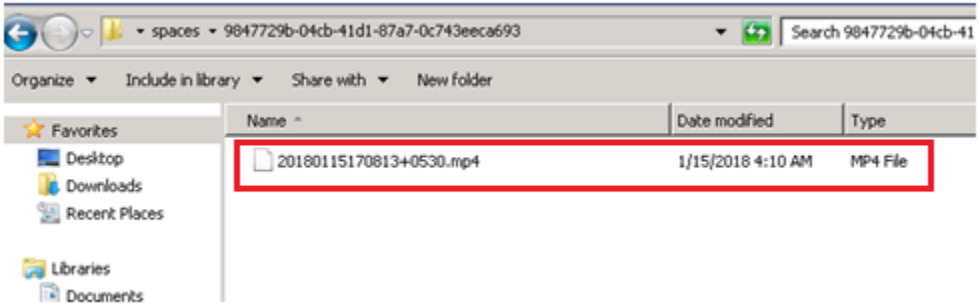


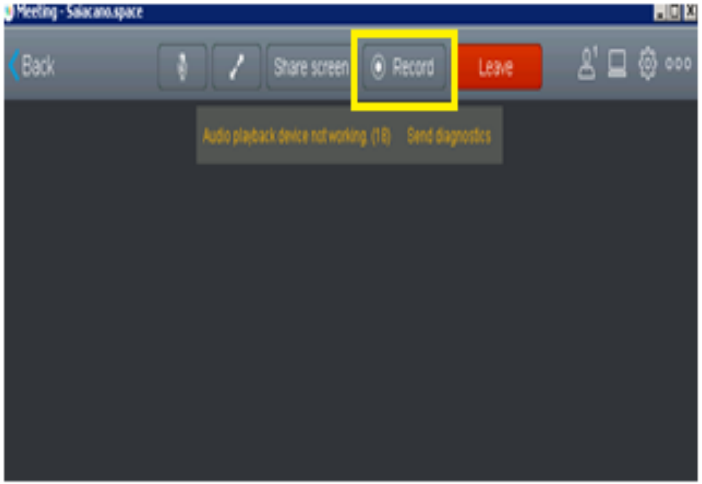
Configuration

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.

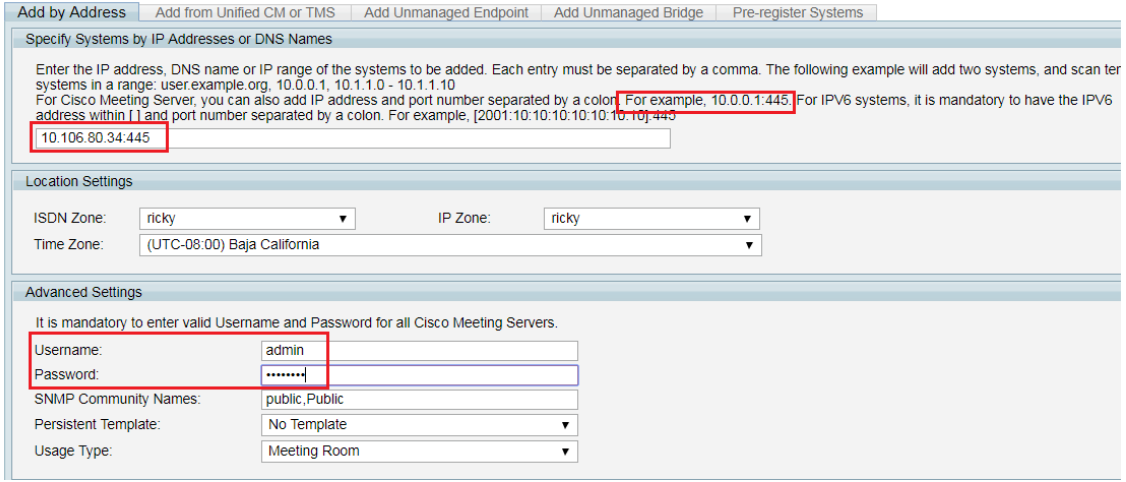




CMS –TMS Integration

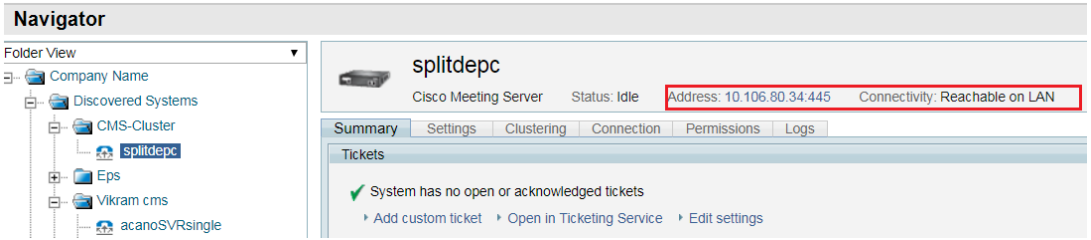
CMS – TMS Integration

-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

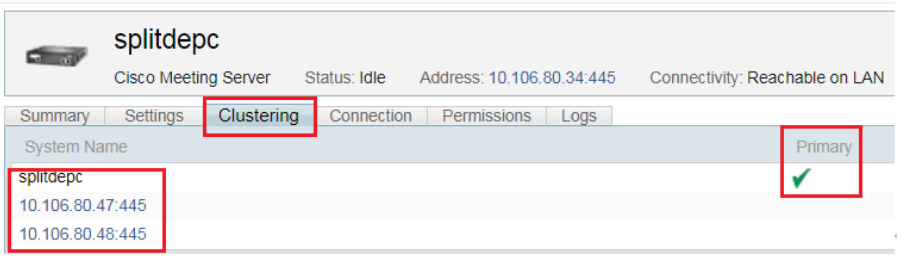


CMS – TMS Integration

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

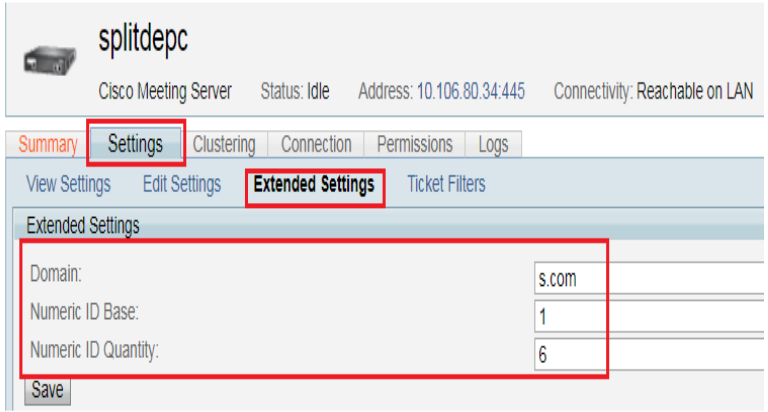


- All subsequent CMS cluster nodes gets added automatically under clustering tab.



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.



Meetings Gets created on CMS

Space configuration

Filter Submit

Name	URI user part	Secondary URI user part	Additional access methods	Call ID
7777	7777			7777
8888	8888			8888
9999	9999			9999
Salacano's space	salacano.cs			036707688
TMS_Scheduled_Meeting_1	1			1
TMS_Scheduled_Meeting_2	2			2
TMS_Scheduled_Meeting_3	3			3
TMS_Scheduled_Meeting_4	4			4
TMS_Scheduled_Meeting_5	5			5
TMS_Scheduled_Meeting_6	6			6

Questions ?????