

Configure Example of CMS Edge

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Pre-Configure](#)

[Network Diagram](#)

[CMS Core and Edge Configurations](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure the Cisco Meeting Server (CMS) Edge.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these CMS 3.X components:

- Webbridge 3
- Callbrige
- C2W
- Firewall
- Turn Server

Components Used

The information in this document is based on these software and hardware versions:

- CMS3.X Open Virtual Appliance (OVA)
- Chrome browser 122.0.6261.112
- Firefox browser 123.0.1 (20240304104836)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Pre-Configure

1. Configure Network Time Protocol (NTP) Server:

It is better to configure the same NTP server on the CMS Edge and core server.

2. Configure Domain Name Server (DNS):

1. Configure internal DNS for CMS Core server (the internal DNS CMS Edge A record points to CMS Edge internal IP address; if impossible, two CMS Edge A records must be configured, one pointing to CMS internal IP address, another to external IP address).
2. Configure external DNS for CMS Edge server. The external DNS A CMS record points to the external IP address of CMS Edge.

3. CMS Core Uses the Internal CMS Edge A Record for Connection.

4. Public Users Access CMS Edge via a Public IP Address.

5. User Domain: cms.demo:

a. A record of CMS Edge:

- edge.cms.demo (internal user login with this A record)
- edge.cms.demo (public user also use same A record from internet, you could specify the different external A record)

b. A record of CMS Core:

core.cms.demo

6. Produce CMS Core and Edge Servers Certification:

a. Produce certification

- cmscore-fullchain.cer (all the services involve the fullchain certificates in the lab, you also can involve the server certificates)
- cmsedge-fullchain.cer (all the services involve the fullchain certificates in the lab, you also can involve the server certificates)

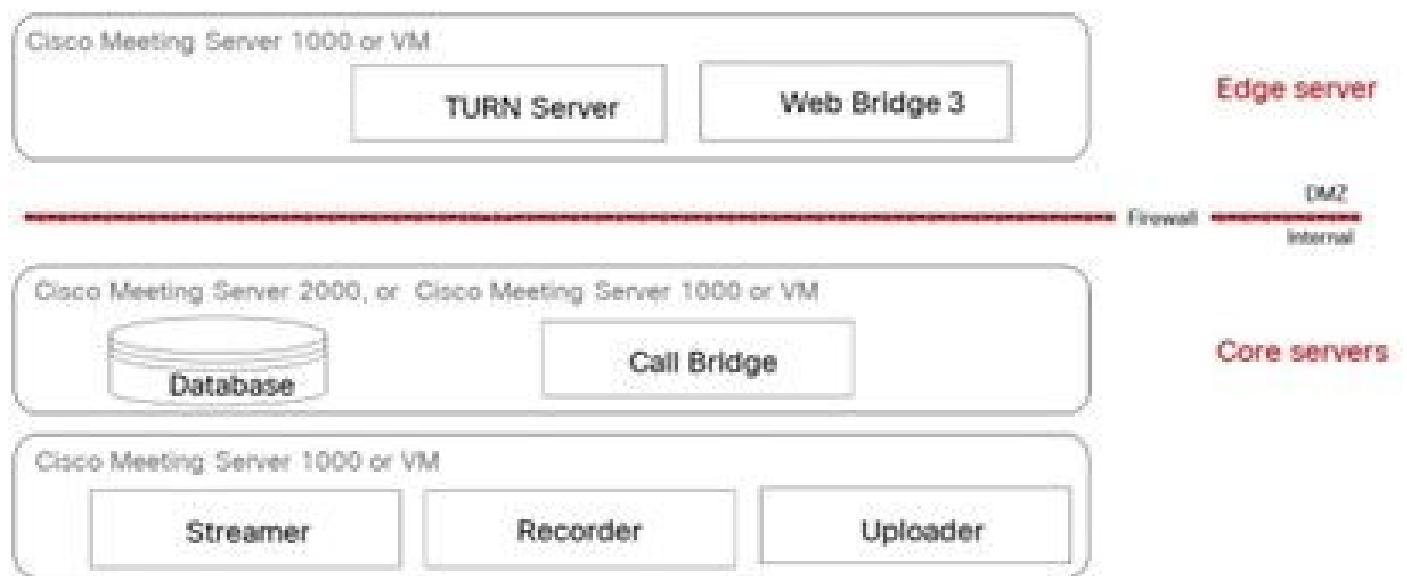
b. Produce two servers' fullchain certification.

- cmscore-fullchain.cer (this certificate includes a root certificate)
- cmsedge-fullchain.cer (this certificate includes a root certificate)

Network Diagram

Table 7: Call capacities for server specifications with recommended hardware

Type of calls	1 x 4 vCPU VM call capacity	1 x 16 vCPU VM call capacity
Full HD calls 1080p30 video	100	350
HD calls 720p30 video	175	700
SD calls 448p30 video	250	1000
Audio calls (G.711)	850	3000



CMS Core and Edge Configurations

1. Activate CMS Core Server-related Services.

a. Configure signal network.

Activate network interface:

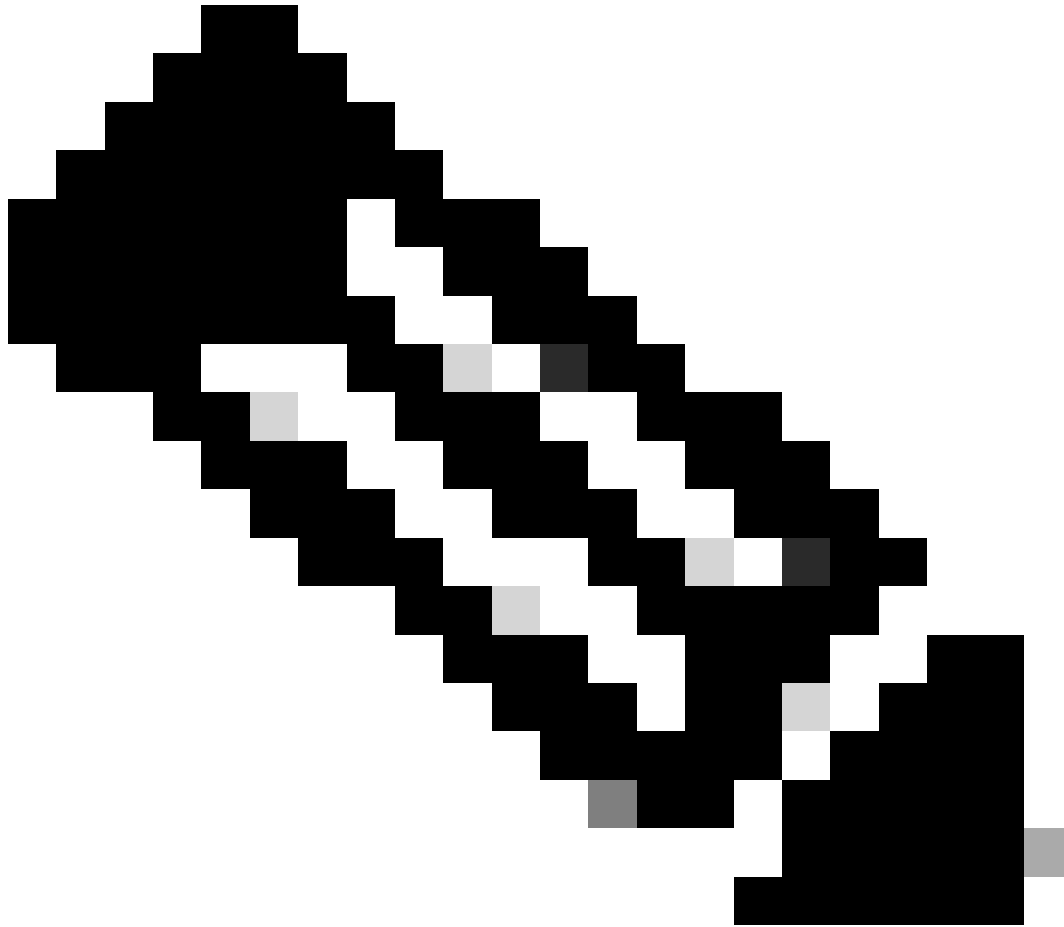
```
ipv4 a add 10.124.56.224/24 10.124.56.1
```

b. Activate the Callbridge component.

```
callbridge listen a
callbridge certs core.key cmscore-fullchain.cer
callbridge trust c2w cmsedge-fullchain.cer (if not, which result in WebRTC failed)
callbridge enable
```

2. Activate CMS Edge server-related services:

a. Configure two network interfaces.



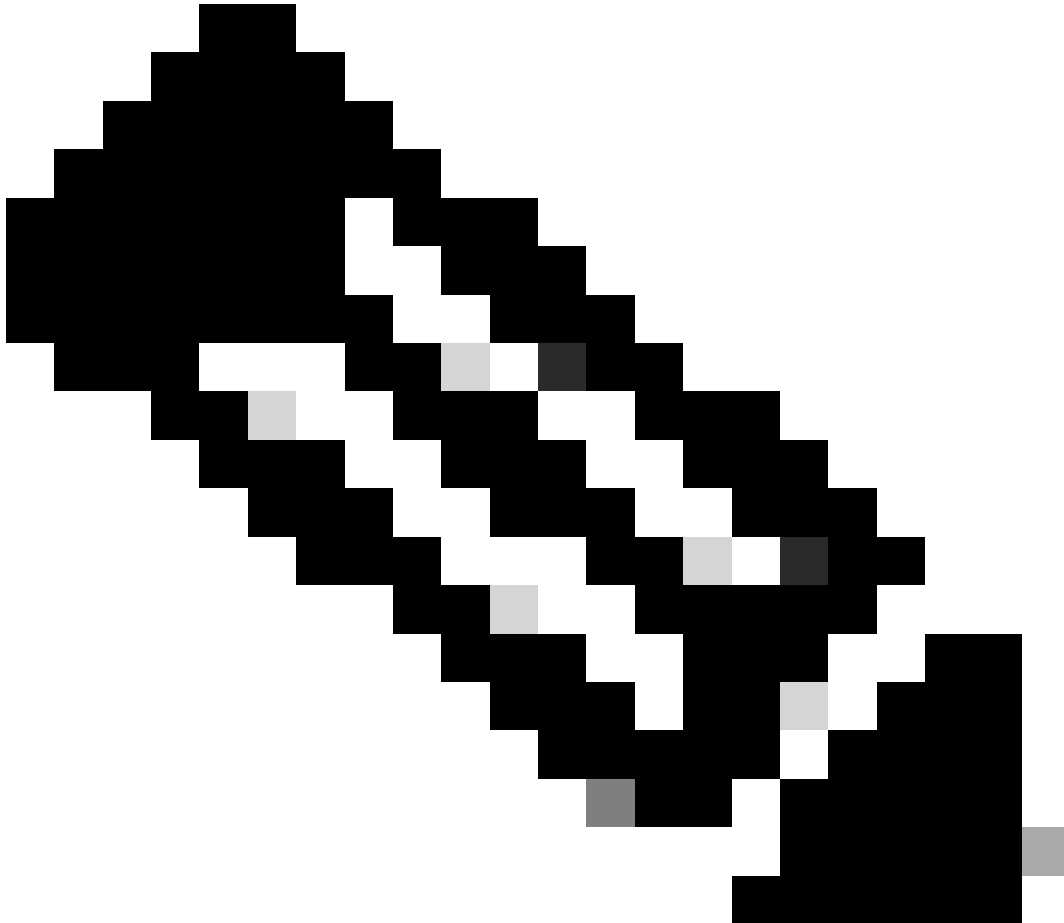
Note: 'b' is the public network interface, and a is the internal network interface.

- Activate network a, b
- Configure default gateway is b (it is a public network interface)
- Configure internal gateway a

```
ipv4 a add 10.124.144.80/24 10.124.144.1
ipv4 b add 10.124.42.112/24 10.124.42.1
ipv4 b default
```

b. Activate turn components.

```
turn certs edge.key cmsedge-fullchain.cer
turn listen a b
turn credentials <username> <password> <cms.demo> (cms.demo is actual domain deployment)
turn public-ip x.x.x.x
turn tls 447
turn enable
```



Note:

1. x.x.x.x is NAT map Public IP address; if there is no NAT map, then no need to configure this step.
2. The port can be defined by self, refer to the related CMS guide.

c. Activate webbridge3 components.

```
webbridge3 https certs cmsedge.key cmsedge-fullchain.crt (cmsedge-fullchain.crt ,please refer to CMS fu
webbridge3 https listen b:445 (b is public network interface , this step just provide public users WebR
webbridge3 https listen a:445 b:445 (this step could provide both internal and external WebRTC service,
```

```

webbridge3 c2w certs edge.key cmsedge-fullchain.crt
webbridge3 c2w listen a:6000 (a is internal network interface, 6000 is self-defined port which need to
webbridge3 c2w trust cmscore-fullchain.cer (if no this step, result in WebRTC failed)
webbridge3 enable

```

3. Build the communication between related components.

- a. Callbridge <---> Turn (public media service)
- b. Callbridge <---> WebBridge3 (WebRTC service)

Configure turn and webbridge3 on CMS Core:

- a. Configure the connection between Callbridge and Turn, and activate public media service.
- Log in to webadmin GUI, navigate to Configuration > General.

General configuration

TURN Server settings

TURN Server address (CMS)

TURN Server address (web app)

Username

Password

Confirm password

Lync Edge settings

Server address

Username

Number of registrations

IVR

IVR numeric ID

Joining scheduled Lync conferences by ID

- b. Configure the connection between Callbridge and Webbridge3, and activate WebRTC service.
- Create webbridge via API on CMS, then add a C2W connection, for example, c2w://edge.cms.demo:6000 (the port must be kept the same with the webbridge3 service configuration).

/api/v1/webBridges/aa292aed-57bb-4305-b89d-eacd72172e4f

<input type="checkbox"/>	url	<input type="text" value="c2w://edge.cms.demo:6000"/>	(URL) - present
<input type="checkbox"/>	tenant	<input type="text"/>	<input type="button" value="Choose"/>
<input type="checkbox"/>	tenantGroup	<input type="text"/>	<input type="button" value="Choose"/>
<input type="checkbox"/>	callBridge	<input type="text"/>	<input type="button" value="Choose"/>
<input type="checkbox"/>	callBridgeGroup	<input type="text"/>	<input type="button" value="Choose"/>
<input type="checkbox"/>	webBridgeProfile	<input type="text"/>	<input type="button" value="Choose"/>
<input type="button" value="Modify"/>			

restart Callbridge component and apply all configuration
callbridge restart (go to CLI)

4. Enable the firewall function and disable the public 22 port (ssh).

```
firewall a default allow ( a is the external/public network interface)
firewall a deny 22
firewall a enable
```

Verify

1. Verify all the services are running on CMS Core and Edge:

CMS Core services status:

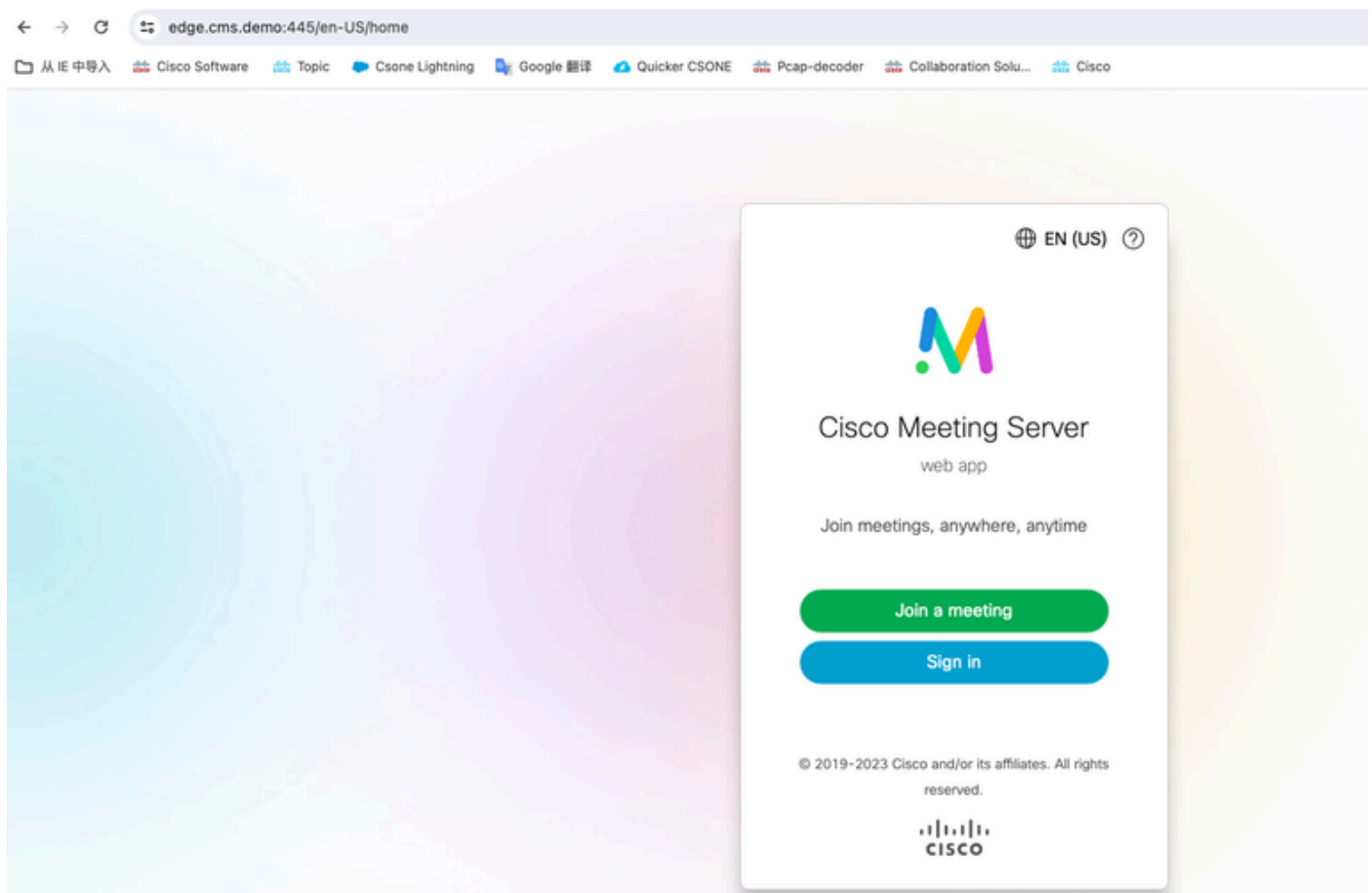
```
CMS> webadmin
Enabled                : true
TLS listening interface : a
TLS listening port     : 443
Key file               : core.key
Certificate file       : cmscore-fullchain.cer
HTTP redirect         : Disabled
STATUS                : webadmin running
CMS> callbridge
Listening interfaces  : a
Preferred interface   : none
Key file             : core.key
Certificate file      : cmscore-fullchain.cer
Address              : none
C2W trusted certs    : cmsedge-fullchain.cer
Callbridge cluster trusted certs : none
Callbridge trust branding certs : none
UCM trusted certs    : none
UCM verification mode : disabled
IMPS trusted certs   : none
IMPS verification mode : disabled
WC3 JWT Expiry in hours : 24
```

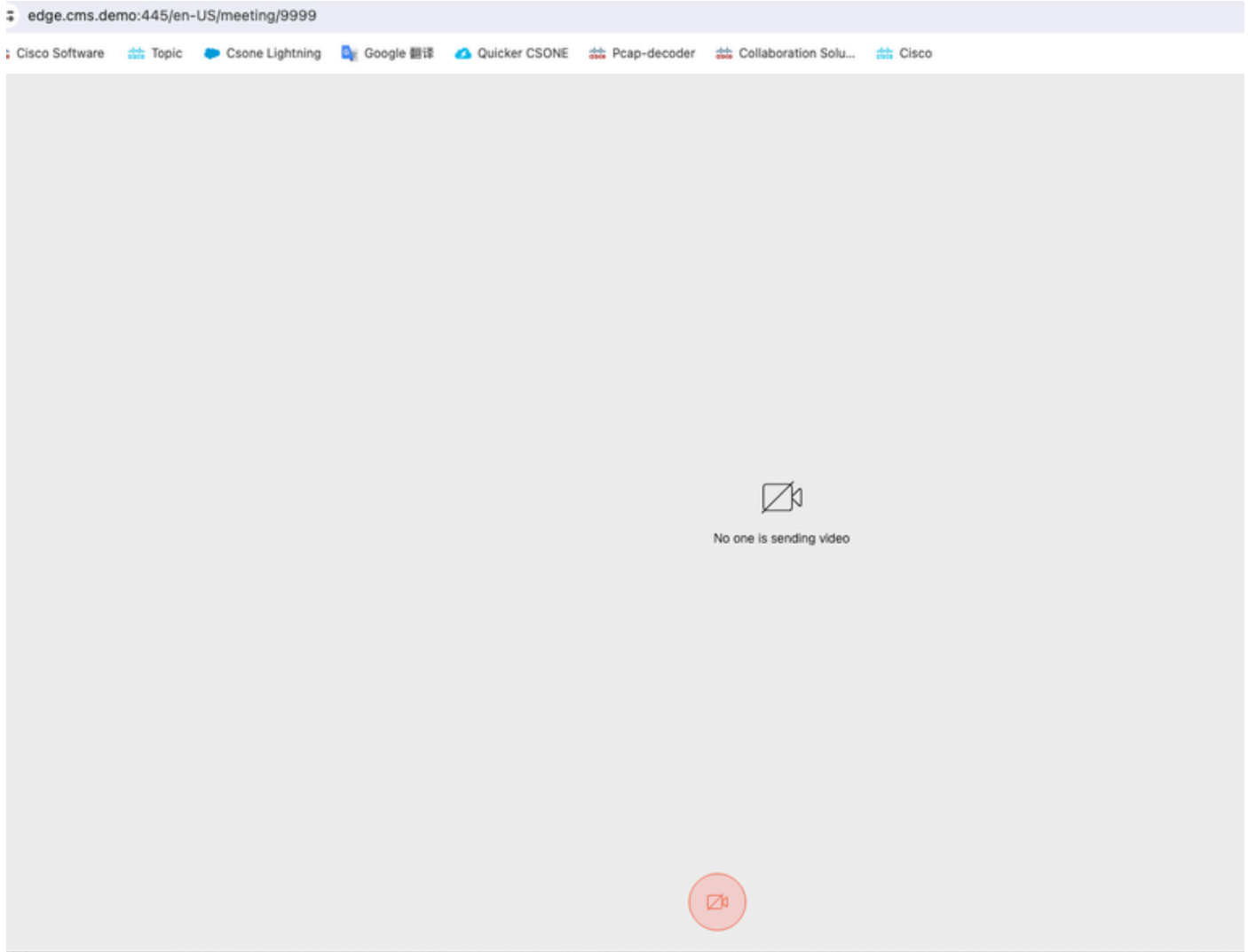
CMS Edge services status:

```
CMS> webbridge3
Enabled                : true
HTTPS listening ports and interfaces : a:445 b:445
HTTPS Key file         : edge.key
HTTPS Full chain certificate file    : cmsedge-fullchain.cer
HTTPS Frame-Ancestors : none
HTTP redirect         : Disabled
C2W listening ports and interfaces  : a:6000
```

```
C2W Key file : edge.key
C2W Full chain certificate file : cmsedge-fullchain.cer
C2W Trust bundle : cmscore-fullchain.cer
Meetingapps address : none
Meetingapps port : none
Audio priority flag : Enabled
Beta options : none
CMS> turn
Enabled : true
Username : admin
Password : Cisco.123
Short term credentials : disabled
Shared secret : none
Realm : cms.demo
Public IP : none
High Capacity Mode : enabled
Relay address : 10.124.144.80
TLS port : 447
TLS cert : cmsedge-fullchain.cer
TLS key : edge.key
TLS bundle : none
Listen interface a
Listen interface b
```

2. Verify the webrtc login status and join the meeting:





Troubleshoot

1. CMS Edge: You can see webrtc Participant "Thomas" joins the call. Participant ID: fcf42f4-ac94-4ab2-a14a-f4165ec960a7.

This participant ID can be found in the CMS Core log file.

```
Feb 23 09:02:21.588 local0.info CMS client_backend: INFO : WebApp Audit : Session: a77d94b1-ba12-4e4e-8
Feb 23 09:02:21.599 local7.info CMS 3b8086e0e5a0 wb3_frontend: [Join call:fcfe42f4-ac94-4ab2-a14a-f4165
Feb 23 09:02:21.633 user.info CMS client_backend: INFO : WebSocket : Got authenticated JWT for guest157
```

Webrtc participant leaves the call:

```
Feb 23 09:02:37.982 local0.info CMS client_backend: INFO : WebApp Audit : Session: a77d94b1-ba12-4e4e-8
```

2. CMS Core: The purple line is Conference ID, there is the same Conference ID when other participants join this conference. The blue line is the specific user ID: guest1573064743.

```
Feb 23 09:02:21.594 user.info CMS host:server: INFO : guest login request 1450660605: resolution in pro
Feb 23 09:02:21.594 user.info CMS host:server: INFO : guest login request 1450660605: call ID lookup sc
Feb 23 09:02:21.594 user.info CMS host:server: INFO : guest login request 1450660605: resolution in pro
Feb 23 09:02:21.597 user.info CMS host:server: INFO : guest login request 1450660605: credential storag
Feb 23 09:02:21.597 user.info CMS host:server: INFO : created guest account with user ID "guest15730647
Feb 23 09:02:21.597 user.info CMS host:server: INFO : guest login request 1450660605: credential storag
Feb 23 09:02:21.597 user.info CMS host:server: INFO : guest login request 1450660605: credential storag
Feb 23 09:02:21.598 user.info CMS host:server: INFO : guest login request 1450660605: successfully stor
Feb 23 09:02:21.598 user.info CMS host:server: INFO : instantiating user "guest1573064743"
Feb 23 09:02:21.598 user.info CMS host:server: INFO : conference db0fafc3-ad47-43bd-bcbd-47886416451b:
Feb 23 09:02:21.598 user.info CMS host:server: INFO : conference db0fafc3-ad47-43bd-bcbd-47886416451b:
Feb 23 09:02:21.598 user.info CMS host:server: INFO : API "9999" Space GUID: 58ef98d1-5181-4e63-a386-4b
Feb 23 09:02:21.598 user.info CMS host:server: INFO : unable to apply logo (space '9999') -- no license
Feb 23 09:02:21.599 user.info CMS host:server: INFO : conference db0fafc3-ad47-43bd-bcbd-47886416451b:
Feb 23 09:02:21.599 user.info CMS host:server: INFO : API call leg fcfe42f4-ac94-4ab2-a14a-f4165ec960a7
Feb 23 09:02:21.599 user.info CMS host:server: INFO : conference db0fafc3-ad47-43bd-bcbd-47886416451b h
Feb 23 09:02:21.599 user.info CMS host:server: INFO : conference db0fafc3-ad47-43bd-bcbd-47886416451b n
Feb 23 09:02:21.601 user.info CMS host:server: INFO : new session created for user "guest1573064743"
Feb 23 09:02:21.603 local0.info CMS postgres[54639]: [6-1] 2024-02-23 09:02:21.603 UTC [54639] LOG: cou
Feb 23 09:02:21.603 local0.err CMS postgres[54639]: [7-1] 2024-02-23 09:02:21.603 UTC [54639] FATAL: co
Feb 23 09:02:21.768 user.info CMS host:server: INFO : call 11: allocated for guest1573064743 / "Thomas"
Feb 23 09:02:21.768 user.info CMS host:server: INFO : call 11: configured - API call leg fcfe42f4-ac94-
Feb 23 09:02:21.768 user.info CMS host:server: INFO : call 11: ActiveControlState change, unknown -> un
Feb 23 09:02:21.769 user.info CMS host:server: INFO : call 11: setting up combined RTP session for DTL
Feb 23 09:02:21.770 user.info CMS host:server: INFO : call 11: ActiveControlState change, unknown -> in
Feb 23 09:02:21.770 user.info CMS host:server: INFO : call 11: ActiveControlState finality change (inac
Feb 23 09:02:21.770 local0.info CMS host:server: INFO : participant "guest1573064743" joined space 58ef
Feb 23 09:02:21.770 user.info CMS host:server: INFO : participant "guest1573064743" (fcfe42f4-ac94-4ab2
Feb 23 09:02:21.772 user.info CMS host:server: INFO : call 11: starting DTLs combined media negotiation
```

Webrtc user leaves the call: guest1573064743 leave Space ID: 58ef98d1-5181-4e63-a386-4b60597be7e4 (9999).

```
Feb 23 09:02:37.943 user.info CMS host:server: INFO : user "guest1573064743": deactivating due to sessi
Feb 23 09:02:37.943 user.info CMS host:server: INFO : call 11: tearing down ("guest1573064743" conferen
Feb 23 09:02:37.943 user.info CMS host:server: INFO : call 11: destroying API call leg fcfe42f4-ac94-4a
Feb 23 09:02:37.943 local0.info CMS host:server: INFO : participant "guest1573064743" left space 58ef98
Feb 23 09:02:37.943 user.info CMS host:server: INFO : removing guest account 'guest1573064743' (name 'T
Feb 23 09:02:37.943 user.info CMS host:server: INFO : destroying guest account with user ID "guest15730
Feb 23 09:02:37.944 user.info CMS host:server: INFO : conference bf286660-6e5d-403f-8926-514d385dad3cd
```

Related Information

- [Cisco-Meeting-Server-3-8-Single-Combined-Server-Deployment](#)
- [Cisco-Meeting-Server-3-8-Single-Split-Server-Deployment](#)
- [Cisco Technical Support & Downloads](#)