Cisco Meeting Server

Set up guide for Meeting Server Appliance

Cisco Meeting Server Medium

January 29, 2026

Cisco Systems, Inc.www.cisco.com

Contents

Change History

Date	Change history	Change summary
29 Jan, 2026	Support for Medium platform	Introducing Meeting Server M8 Medium - PID CMS-M-M8-K9.

1 Introduction

The Cisco Meeting Server Medium platform is built on the Cisco UCS technology using a preconfigured Cisco UCS C245 M8 Rack Server with AMD Genoa (4th Gen) processors.

The Medium platform offers the following advantages:

- High CPU density (384 vCPUs)
- Meeting Server application optimised to run bare metal without the need of hypervisor
- Up to 40G fiber port connectivity

2 Installing and Initial setup of Cisco Meeting Server Medium

2.1 Unpacking and initial startup

1. Unpack the Meeting Server, power cords, console adaptor, and rack kit.
2. Position the Meeting Server– see the Cisco UCS C245 M8 Installation Guide.
3. Connect the Ethernet cables to the SFP ports (Ethernet1) on the rear of the Meeting Server and connect to the Ethernet network.
4. Connect the power cords to each power supply and connect to power.
5. Press the power button on the front of the Meeting Server. It will automatically stop and restart itself more than once after initial power on.
6. Connect a console to the Meeting Server to continue. You can use either a monitor and keyboard, or use a virtual console over a network connection. Select from the following options:

2.1.1 Console option 1 - Monitor and keyboard

1. Attach a monitor with a VGA connection to the VGA port on the rear of the Meeting Server, or to the console port on the front.
2. Connect a keyboard to the USB ports located on the rear of the Meeting Server, or to the console port on the front.
   The Meeting Server will automatically boot to the console screen when startup is complete and should be visible on the monitor.

2.1.2 Console option 2 – Virtual console over network

Use this method if no monitor and keyboard are available to connect to the Meeting Server:

1. Connect your computer's serial port to the RJ-45 port on the rear of the Meeting Server labeled 10101 using the standard blue Cisco RJ-45 to DB-9 Null Serial cable provided with routers and switches.
2. Open your terminal program, select the COM port for your serial port/adaptor and set the terminal settings to 115200 baud, No Parity, 8 data bits, 1 stop bit.
3. Connect a second Ethernet LAN port to the RJ-45 port on the rear of the Meeting Server labeled M1. If you only have the resources for one network connection, remove the LAN connected to Ethernet1 and use it for the M1 port temporarily to enable the virtual

console, and move it back to Ethernet1 after configuration. The M1 port must be connected and configured with a valid IP address to use the virtual console.

4. Ensure Meeting Server has its power supplies connected. If not, ensure it has been plugged in for several minutes to allow the CIMC management interface to startup. Meeting Server does not have to be powered on for CIMC to function, but must be connected to power. (There is no external indicator for CIMC status.)

5. In your terminal program, press **Escape** and the **9** keys **simultaneously** to switch the port to CIMC. A username prompt displays.

6. Enter the default username and password (username: `admin`, password: as provided).

7. The first time you login, you will be prompted to change the password to one of your choice. Complete the prompts to set a new password.

8. Once logged in, at the command prompt enter the command `scope cimc` – the command prompt changes to reflect that you are now in the CIMC menu.

9. Enter the command `show network detail` to show the current configuration of the management Ethernet interface, including the current IP address the server has aquired via DHCP (if available on the network). Make a note of the IPv4 address shown (if DHCP is available).

10. If DHCP is not available and you need to set a static IP, use the following commands, changing the sample values to ones appropriate for your network. (These commands assume you are already in the CIMC scope.)

    ```
    scope network
    set dns-use-dhcp no
    set dhcp-enabled no
    set v4-addr 10.1.2.3
    set v4-netmask 255.255.255.0
    set v4-gateway 10.1.2.1
    commit
    ```

11. Enter `show network detail` to confirm your changes. Once complete, enter the command `exit` twice to log out of the CIMC.

12. Switch to your PC's browser, and browse to the IP address you configured or obtained from the CIMC serial interface. Dismiss the certificate security warnings and a Cisco landing page with username and password fields will display.

13. Login with the username of `admin` and the password you set when first connecting to the CIMC.

14. When the **Server Summary** page loads, click the **Launch KVM** link under **Actions**. Depending on your Operating System and browser you may get security warnings and dialogs to acknowledge and accept. Continue until the application loads–it will show the

monitor image as if you were directly connected to the server. If the server is powered off, it will show a larger green window saying **No Signal**.

15. If the server is powered off, under the Actions tab, select the **Power** menu and click **Power On** to start the server. After a few minutes it should boot to the Meeting Server console screen.

You can now use the virtual console the same as if you were connected using a local monitor and keyboard.

Useful information if you are using the virtual console

- CIMC is a powerful out-of-band management interface for the Meeting Server and is recommended for use when the Meeting Server is installed in a rack or computer room. This management interface is not used by the Meeting Server application, so if you want to keep it connected, you must secure a dedicated LAN connection for the M1 Ethernet port. (NIC sharing options are also available in the Cisco UCS Server documentation.)
- If you are using the virtual console with only one network connection and had been temporarily using it for the M1 interface:
    a. You will not need the virtual console anymore to complete the install. Disconnect the Ethernet cable from the M1 interface of the server and reconnect it to the Ethernet1 port.
    b. If you are using DHCP for the interface, you will need to restart the server to obtain a new IP address after connecting the Ethernet cable. To restart, press the power button on the front of the server briefly and the server will initiate an automatic shutdown (this takes several minutes). After it powers off, power it back on using the power button. Because you disconnected the network that the virtual console was using, you will not be able to see the IP address the server obtained. To find the IP address, contact your DHCP administrator to find which IP address the server was assigned. The MAC address of the Ethernet1 interface can be found on the pull-out tab located on the front of the Cisco Meeting Server Medium.

You should now have Ethernet connected to the Ethernet1 port on the rear of the server and know the IP address in use by the Meeting Server.

2.2 Accessing the Cisco Meeting Server Medium Console

If you experience issues with a corrupted or unbootable ISO image, please reach out to the Cisco Support Team for help with reflashing the ISO image.

The Meeting Server instance itself can be accessed by connecting to its own IP address, or via the CIMC console function.

1. If your network has DHCP, to find the current Meeting Server IP address, login to the Meeting Server or KVM console and execute the command **`IPV4 a`**.
2. The first time you login, you will be prompted to enter the user name and password. Log in with the username “admin” and press the “Enter” key to skip the password field.
3. You can ssh to that IP to continue the configuration of the Meeting Server software.
4. You will be prompted to reset the password.
5. If your network does not have DHCP, you will have to assign an IP address to the VM using the virtual machine console in the KVM console and the Meeting Server MMP commands **`ipv4`** or **`ipv6`** as described in Chapter 1 (or see the MMP Command Line Reference Guide).

   CAUTION: Passwords expire after 6 months.

After installation, a fully functioning Cisco Meeting Server is available, which can be run as:

- a complete solution with all components enabled on a single server (single combined server deployment model),
- a split deployment with some components enabled on a Core server deployed on the internal network, and other components enabled on an Edge server deployed in the DMZ (single split server deployment model),
- a scalable and resilient deployment with multiple Call Bridges and databases, clustered together to support growth in usage and minimize downtime.

2.3 Checking the installed software

The Cisco Meeting Server Medium ships with the Cisco Meeting Server software pre-installed. However, it is advised to upgrade to the latest version of Cisco Meeting Server 3.11 available on Cisco Connection Online (CCO) before configuring the Cisco Meeting Server software. To upgrade, follow the procedure outlined in the release notes published for the software version.

Tip: Now that Port A is configured, use SFTP to back up and upgrade Cisco Meeting Server software via Port A.

The rest of the configuration process follows as described in Chapter 3.

3 Configuration

3.1 Points to note about deployments on Meeting Server Medium

- The configurations described below are applicable only for a standalone node. For cluster deployments, please refer to the Scalable and Resilient Deployment Guide.
- Mixed database deployments are not supported.

3.2 Creating your own Cisco Meeting Server Administrator Account

For security purposes, you are advised to create your own administrator accounts as username “admin” is not very secure. In addition, it is good practice to have two admin accounts in case you lose the password for one account, if you do, then you can still log in with the other account and reset the lost password.

Use the MMP command **`user add <name> admin`**, see the MMP Command Reference Guide for details. You will be prompted for a password which you must enter twice. Login with the new account, you will be asked to change the password.

CAUTION: Passwords expire after 6 months.

After creating your new admin accounts delete the default “admin” account.

Note: Any MMP user account at the admin level can also be used to log into the Web Admin Interface of the Call Bridge. You cannot create users through the Web Admin Interface.

3.3 Setting up the Network Interface for IPv4

Note: Although these steps are for IPv4, there are equivalent commands for IPv6. See the MMP Command Reference for a full description.

In the Cisco Meeting Server virtualized deployment, there is only one network interface initially, interface “a”, but up to 4 are supported (see the next section). The MMP runs on interface a in the virtual deployment.

1. To set network interface speed, duplex and auto-negotiation parameters use the **`iface`** MMP command e.g. to display the current configuration on the " a" interface, in the MMP type:

   ```
   iface a
   ```

Set the network interface speed (Mbps), duplex and auto negotiation parameters using the command **`iface (a|b|c|d) <speed> (full|on|off)`**. For example, set the interface to 1GE, full duplex:

```
iface a 1000 full
```

2. The “a” interface is initially configured to use DHCP. To view the existing configuration, type:

   ```
   ipv4 a
   ```

   a. If you are using DHCP IP assignment, no further IP configuration is needed, go to step 3.

   b. If you are using Static IP assignment:

      Use the **`ipv4 add`** command to add a static IP address to the interface with a specified subnet mask and default gateway.

      For example, to add address 10.1.2.4 with prefix length 16 (netmask 255.255.0.0) with gateway 10.1.1.1 to the interface, type:

      ```
      ipv4 a add 10.1.2.4/16 10.1.1.1
      ```

      To remove the IPv4 address, type:

      ```
      ipv4 a del <address>
      ```

3. Set DNS Configuration

   Meeting Server requires DNS lookups for many of its activities including looking up SRV records and is required for a simplified deployment. We recommend you point Meeting Server to the default DNS resolver for your network using a period " ." for the forwardzone value.

   a. To output the dns configuration, type:

      ```
      dns
      ```

   b. To set the application DNS server use the command:

      ```
      dns add forwardzone <domain name> <server IP>
      ```

      Note: A forward zone is a pair consisting of a domain name and a server address: if a name is below the given domain name in the DNS hierarchy, then the DNS resolver can query the given server. Multiple servers can be given for any particular domain name to provide load balancing and fail over. A common usage will be to specify " ." as the domain name i.e. the root of the DNS hierarchy which matches every domain name.

      for example:

      ```
      dns add forwardzone . 10.1.1.33
      ```

   c. If you need to delete a DNS entry use the command:

      ```
      dns del forwardzone <domain name> <server IP>
      ```

for example:

```
dns del forwardzone . 10.1.1.33
```

3.4 Configuring the Call Bridge

The Call Bridge needs a key and certificate pair that is used to establish TLS connections with SIP Call Control devices and with the Lync Front End (FE) server. If you are using Lync, this certificate will need to be trusted by the Lync FE server.

The command **`callbridge listen <interface>`** allows you to configure a listening interface (chosen from A, B, C or D). By default the Call Bridge listens on no interfaces.

1. Create and upload the certificate as described in the Certificate Guidelines.
2. Sign into the MMP and configure the Call Bridge to listen on interface A.

   ```
   callbridge listen a
   ```

   Note: the Call Bridge must be listening on a network interface that is not NAT'd to another IP address. This is because the Call Bridge is required to convey the same IP that is configured on the interface in SIP messages when talking to a remote site.

3. Configure the Call Bridge to use the certificates by using the following command so that a TLS connection can be established between the Lync FE server and the Call Bridge, for example:

   ```
   callbridge certs callbridge.key callbridge.crt
   ```

   The full command and using a certificate bundle as provided by your CA, is described in the Certificate Guidelines.

4. Restart the Call Bridge interface to apply the changes.

   ```
   callbridge restart
   ```

3.5 Configuring the Web Admin Interface

The Web Admin Interface acts as the interface to the Call Bridge; the API of the Cisco Meeting Server is routed through this web interface.

The Web Admin Interface is only accessible through HTTPS, you need to create a security certificate and install it on the Cisco Meeting Server.

Note: You need a certificate uploaded for the Web Admin Interface even if you configure the Call Bridge through the API rather than the Web Admin Interface.

The information below assumes that you trust Cisco to meet requirements for the generation of private key material. If you prefer, you can generate the private key and the certificate externally using a public Certificate Authority (CA), and then load the externally generated key/certificate pair onto the MMP of the Cisco Meeting Server using SFTP.

Note: If testing your Cisco Meeting Server in a lab environment, you can generate a key and a self-signed certificate on the server. To create a self-signed certificate and private key, log in to the MMP and use the command:

```
pki selfsigned <key/cert basename>
```

where **`<key/cert basename>`** identifies the key and certificate which will be generated e.g. " pki selfsigned webadmin" creates webadmin.key and webadmin.crt (which is self-signed). Self-signed certificates are not recommended for use in production deployments.

Note: Before transferring the signed certificate and the private key to the Cisco Meeting Server, check the certificate file. If the CA has issued you a chain of certificates, you will need to extract the certificate from the chain. Open the certificate file and copy the specific certificate text including the BEGIN CERTIFICATE and END CERTIFICATE lines and paste into a text file. Save the file as your certificate with a .crt, .cer or .pem extension. Copy and paste the remaining certificate chain into a separate file, naming it clearly so you recognize it as an intermediate certificate chain and using the same extension (.crt, .cer or .pem). The intermediate certificate chain needs to be in sequence, with the certificate of the CA that issued the chain first, and the certificate of the root CA as the last in the chain.

3.5.1 Configuring the Web Admin Interface for HTTPS Access

Note: The deployment automatically sets up the Web Admin Interface to use port 443 on interface A. However, the Web Bridge also uses TCP port 443. If both the Web Admin Interface and the Web Bridge use the same interface, then you need to change the port for the Web Admin Interface to a non-standard port such as 445, use the MMP command **`webadmin listen <interface> <port>`**.

1. Log in to the MMP and generate the private key and certificate signing request (CSR) using the following command:
   ```
   pki csr <key/cert basename> [<attribute>:<value>]
   ```
   where:

   `<key/cert basename>` is a string identifying the new key and CSR (e.g. " webadmin" results in " webadmin.key" and " webadmin.csr" files).
2. Generate the certificate as described in the Certificate Guidelines.
3. Establish an SSH connection to the MMP and sign in.
4. Use SFTP to upload the private key/certificate pair and certificate bundle (optional) for the Web Admin Interface.
5. Disable the Web Admin Interface before assigning the certificate.

```
webadmin disable
```

6. Assign the private key/certificate pair you uploaded in step 4, using the command:

   ```
   webadmin certs <keyfile> <certificatefile> [<cert-bundle>]
   ```

   where **keyfile** and **certificatefile** are the filenames of the matching private key and certificate. If your CA provides a certificate bundle then also include the bundle as a separate file to the certificate. For example:

   ```
   webadmin certs webadmin.key webadmin.crt webadminbundle.crt
   ```

7. Restart the Web Admin Interface.

   ```
   webadmin restart
   ```

8. Enable the Web Admin Interface.

   ```
   webadmin enable
   ```

For example:

```
webadmin certs webadmin.key webadmin.crt
webadmin listen b 443
webadmin restart
webadmin enable
```

Test that you can access the Web Admin Interface, i.e. enter your equivalent of https://cms-server.mycompany.com (or the IP address) in your browser and login using the MMP user account you created earlier.

Note: You can use Trial Mode for a 90 day full featured period without licenses. In this instance, the Web Admin interface will display " This CMS is currently unlicensed" during this period. For information on Smart licensing and how licensing works see .

3.6 Configuring Web Bridge 3

Web Bridge 3 is a Meeting Server component that enables participants to join meetings using the browser-based Cisco web app client. Web Bridge 3 provides the web server for Cisco Meeting Server web app participants and works in conjunction with the Call Bridge and TURN Server components to support clients. .

Note: If you are not using the web app, you do not need to deploy Web Bridge 3 and can skip this section.

- If you need to support web app clients from your internal network, you should configure Web Bridge on your main Meeting Server instance in the Core and complete the steps in this section.

- If you are using Cisco Expressway as your proxy and TURN Server for web app, Web Bridge needs to be configured on your main Meeting Server instance in the Core and you should complete the steps in this section.
- If you are using the Edge Meeting Server model, you have the option of running Web Bridge just in the Edge or running it both in the Edge and the main Internal Meeting Server instance. Enabling Web Bridge on the internal server allows clients to use web app without making connections to the Web Bridge in the DMZ. The recommendation for deployments using the Edge Meeting Server model is to run Web Bridge in both the DMZ and internal server instances. Complete the steps in this section and configure Web Bridge on the Edge instances and the main Meeting Server instance in the Core.

Note: Running Web Bridge in both the Core and Edge requires clients resolve the same Web Bridge hostname to either the internal or Edge instance as appropriate for them - this is normally referred to as 'Split-DNS' where the DNS Server resolves names to addresses based on where the client is located.

CAUTION: Important notes for Expressway users
If you are deploying Web Bridge 3 and web app you must use Expressway version X14.3 or later, earlier Expressway versions are not supported by Web Bridge 3.

Note: For more information on the web app, see Cisco Meeting Server web app Important Information.

3.6.1 Useful information to help configure Web Bridge 3

The following is useful information to help you configure Web Bridge 3 so that you can use web app:

- " Call Bridge to Web Bridge" protocol (C2W) is the link between the callbridge and webbridge3. It is an outgoing connection from the Call Bridge to the Web Bridge to establish a control channel between them. Certificates are used to authenticate and secure the C2W connection. C2W is exclusive to Call Bridge - Web Bridge traffic and is not used by users or other services.
- A C2W listening port is defined on the Web Bridge server (using `webbridge3 c2w listen`) to allow the Call Bridge to connect to the Web Bridge using an HTTPS connection. There is no set default value for the port number to use, but this guide uses 9999 as the example. This connection must be secured with certificates.
- We recommend you protect the C2W port from external access — it only needs to be reachable from Call Bridges.

- A Call Bridge must be able to uniquely reach the C2W interface of each Web Bridge it is configured to work with (C2W connections must use unique hostname or IP per Web Bridge 3 instance).
- Web app clients will have a single address to reach the Web Bridge so when multiple Web Bridges are used, DNS or Load Balancer solutions should be used to direct a shared name to an available Web Bridge instance. The client to Web Bridge connection is stateless for non-call activity and a session does not need to stay with a single Web Bridge.
- When establishing the TLS connection, both sides must present a certificate to verify. The Call Bridge uses the certificate set using the **`callbridge certs`** command and the Web Bridge uses the certificate set using the **`webbridge3 c2w certs`** command.
- The Web Bridge will trust certificates of Call Bridges and Schedulers that are in the Web Bridge’s C2W trust store or have been signed by a certificate in the trust store, set by **`webbridge3 c2w trust`**. It is recommended to use a bundle containing the Call Bridge certificates that will connect to this Web Bridge so that only specific certificate matches will be allowed (certificate-pinning).
- The Call Bridgewill trust certificates of Web Bridges that are in the Call Bridge’s C2W trust store or have been signed by a certificate in the trust store, set by **`callbridge trust c2w`**. It’s recommended to use a bundle containing the Web Bridge certificates that this Call Bridge will connect so that only specific certificate matches will be allowed (certificate-pinning).
- The Scheduler trusts certificates of Web Bridges that are in the Scheduler’s C2W trust store or have been signed by a certificate in the trust store, set by the command **`scheduler c2w certs <key-file> <crt-fullchain-file>`**.
- If the certificates used for C2W or Call Bridge have extended key usages defined, they must have the usages enabled to allow a Mutual TLS authentication exchange between Call Bridge and Web Bridge. If extended key usages are defined in a certificate, the Web Bridge 3 C2W certificate must include the " server authentication" extended key usage, and the Call Bridge certificate must include " client authentication" extended key usage. If no extended key usages are defined in a certificate, all usages are assumed valid.
- As the C2W connection is only between internal services, you do not explicitly need to use a certificate signed by a public authority. You can use self-signed certificates created within the MMP.
- The SAN/CN in the Web Bridge C2W certificate must match the FQDN or IP address that is used in the c2w:// url used to register the Web Bridge 3 in the Call Bridge API. If this does not match, the Call Bridge will fail the TLS negotiation, rejecting the certificate presented by the Web Bridge, and will fail to connect with the Web Bridge.

Note: If you want a certificate signed by a Public CA you will need to use the FQDN. (Certificates containing an IP address cannot be signed by a Public CA.) If you want to use an IP address in the C2W address you can create your own certificates as the C2W connection is not a public connection, therefore using Public CAs is not necessary.

- The certificate used for the Web Bridge listening interface should be signed by a certificate authority the clients will trust to avoid certificate warnings when clients connect. The FQDN the clients use to reach Web Bridge should be in the certificate CN or SAN list to avoid certificate warnings when clients connect.
- For general certificate information, see the Certificate Guidelines appropriate for your deployment.

3.6.2 Enabling the Web Bridge 3 Service

The Web Bridge service should be enabled on the Core Meeting Server instance if using the Cisco Expressway proxy or supporting web app clients who can reach the Call Bridge directly. When using the Meeting Server Edge deployment, Web Bridge 3 should run on all Edge instances and can optionally be ran on the Core Meeting Server instance where Call Bridge is running.

Complete these steps on each Meeting Server instance where Web Bridge 3 will run.

1. SSH into the MMP and log in.
2. Configure the interface and port web bridge will use for the web server with the command **`webbridge3 https listen <interface>:<port>`**.

   Using the first interface and port 443 is recommended. Example:

   ```
   webbridge3 https listen a:443
   ```
3. Set the HTTPS certificate and key pair Web Bridge will use for its web server with the command **`webbridge3 https certs <key file> <full certificate chain file>`**.

   This command requires the certificate be defined as the full certificate chain - meaning a certificate bundle that starts with the end entity certificate, includes all the intermediate signing certificate authorities, and ends with the root certificate. Example:

   ```
   webbridge3 https certs wb3-https.key wb3-https-fullchain.crt
   ```
4. Configure the interface and port for the C2W connection with the command

   `webbridge3 c2w listen <interface>:<port>` .

   Using the first interface and the default example port 9999 is recommended. Example:

   ```
   webbridge3 c2w listen a:9999
   ```
5. Configure the C2W connection certificates with the command **`webbridge3 c2w certs <key file> <full certificate chain file>.`**

   Example:

```
webbridge3 c2w certs wb3-c2w.key wb3-c2w-fullchain.crt
```

Note: This certificate must include the FQDN or IP address of the C2W interface in the CN or SAN list of the certificate. Additional information is also available in this FAQ - How do I configure connection certificates for use with Web Bridge 3?

6. The Web Bridge 3 C2W trust store must be configured to control which Call Bridge will be allowed to connect to this Web Bridge. The trust bundle should include the Call Bridge certificate of all Call Bridges that will connect to this Web Bridge, or the certificate of the CA that signed the Call Bridge certificates. For the most control, it is recommended to use the individual Call Bridge certificates in the bundle (certificate-pinning) rather than the certificate of the signing authority. Configure the web bridge's c2w trust bundle with the command **`webbridge3 c2w trust <certificate bundle>`**Example:

   ```
   webbridge3 c2w trust wb3-c2w-trust-bundle.crt
   ```

7. Enable the http redirect. This is optional, but recommended for end-user ease of use

   ```
   webbridge3 http-redirect enable
   ```

8. Enable the web bridge service

   ```
   webbridge3 enable
   ```

Repeat the above steps for each Meeting Server instance where Web Bridge will be running and ensure the certificate or key pairs used are correct for each instance.

C2W is the control interface between the Call Bridge and Web Bridge instances and must be configured in the Call Bridge if Web Bridge is deployed. The Call Bridge’s C2W trust bundle should include the Web Bridge C2W certificates of all Web Bridge that this Call Bridge will connect to, or the certificate that signed the Web Bridge C2W certificates. For the most control, it is recommended to use the individual Web Bridge C2W certificates in the bundle (certificate-pinning) rather than the certificate of the signing authority.

1. Connect to the MMP interface of the Internal Meeting Server running Call Bridge.

2. The Call Bridge should already be configured with a certificate from the steps performed in Configuring the Call Bridge listening interface. Confirm by running the command **`callbridge`** and checking that the Key File and Certificate file settings are configured. If not, repeat the steps in Configuring the Call Bridge listening interface before proceeding. The Call Bridge must be configured with certificates for C2W functionality.

3. Use the command **`callbridge trust c2w <certificate bundle file>`** to configure the Call Bridge's C2W trust store with a certificate bundle that includes the C2W certificates of the Web Bridge instances. Example:

   ```
   callbridge trust c2w c2w-callbrige-trust-store.crt
   ```

Note: Unless limited by scopes, the Call Bridge will attempt to connect to all Web Bridge that are defined in the Meeting Server API.

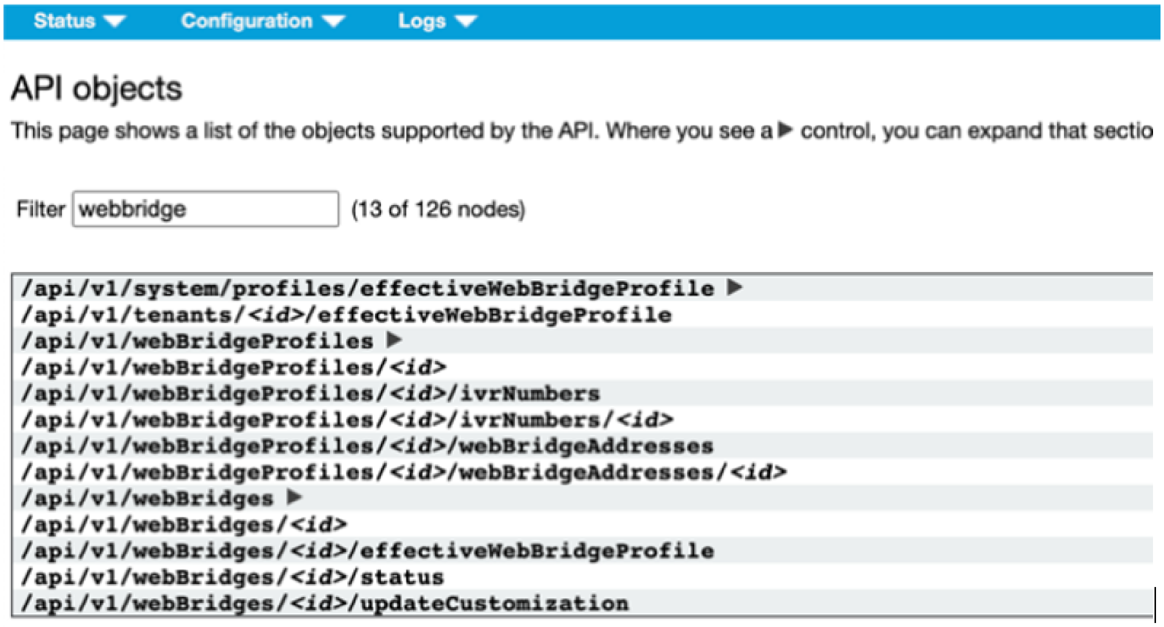
4. Restart the Call Bridge

   ```
   callbridge restart
   ```

3.6.3 Configure Call Bridge with Web Bridge Addresses

The Call Bridge must be told the C2W address of each Web Bridge it will connect to (including a co-resident Web Bridge) by creating a Web Bridge entry in the Meeting Server API. This guide will use API explorer in the Web Admin interface of Meeting Server to illustrate how to complete this task.

1. Log in to the Meeting Server Web Admin interface and select **Configuration** > **API.**
2. Using the Filter input box, type **`webBridges`** to filter the list view, as shown here:



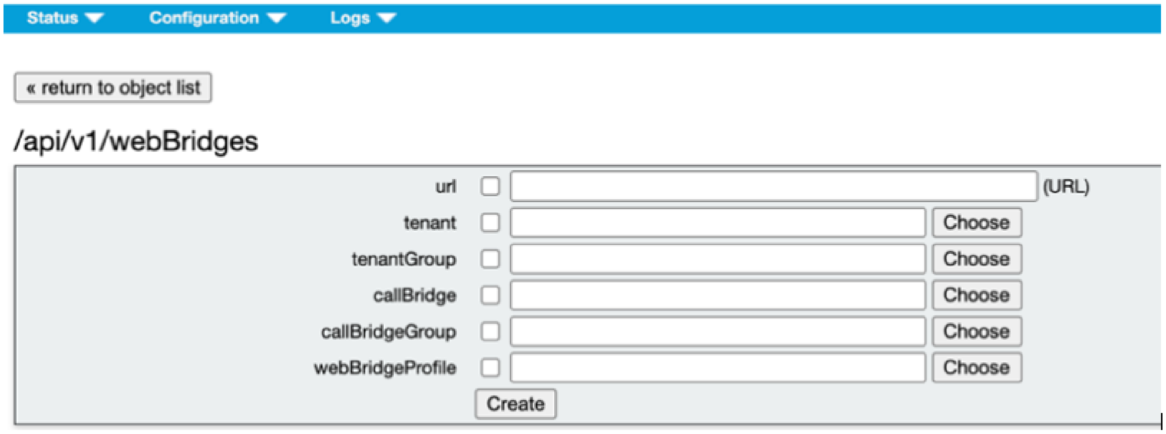
API objects

This page shows a list of the objects supported by the API. Where you see a ▶ control, you can expand that sectio

Filter webbridge (13 of 126 nodes)

```
/api/v1/system/profiles/effectiveWebBridgeProfile ▶
/api/v1/tenants/<id>/effectiveWebBridgeProfile
/api/v1/webBridgeProfiles ▶
/api/v1/webBridgeProfiles/<id>
/api/v1/webBridgeProfiles/<id>/ivrNumbers
/api/v1/webBridgeProfiles/<id>/ivrNumbers/<id>
/api/v1/webBridgeProfiles/<id>/webBridgeAddresses
/api/v1/webBridgeProfiles/<id>/webBridgeAddresses/<id>
/api/v1/webBridges ▶
/api/v1/webBridges/<id>
/api/v1/webBridges/<id>/effectiveWebBridgeProfile
/api/v1/webBridges/<id>/status
/api/v1/webBridges/<id>/updateCustomization
```

3. Locate the **`/api/v1/webBridges`** row from the resulting list and click the ▶ icon to expand it.
4. Click **Create new** to create a new Web Bridge object and the following parameter fields display as shown here:



5. Fill in the **url** field using the format *c2w://<Web Bridge FQDN>:<c2w port>* with the FQDN address of the C2W interface for Web Bridge being added. Example:

   ```
   c2w://cmsedge1.company.com:9999
   ```

   Note: The FQDN entered here must be the CN or in the list of SAN names of the certificate assigned to the C2W interface of Web Bridge 3 and must resolve to the IP of the C2W interface for the Web Bridge. IP Addresses can only be used if the C2W certificate has the IP address in the certificate’s SAN or CN.

6. Click **Create** to save the new Web Bridge entry.

If you have multiple Web Bridges, repeat the above steps creating one Web Bridge object for each Web Bridge instance.

Appendix A Technical specifications for Cisco Meeting Server Medium

A.1 Physical specifications:

Chassis: Cisco UCS C245 M8 Server Installation and Service Guide

Weight: 19+ kg (40 lbs)

Size: 2RU high

A.2 Environmental specifications

Operating temperature: 5° C to 35° C (41-95° F)

Operating humidity: 8% to 90% non-condensing

A.3 Electrical specifications

See Power Supply Specifications in the appropriate Cisco UCS C245 M8 Server Installation and Service Guide.

A.4 Video and audio specifications:

This table provides a comparison of the call capacities across the platforms hosting Cisco Meeting Server software.

Table 1: Call capacities across Meeting Server platforms

Type of calls	Cisco Meeting Server Small M7 (VM)	Cisco Meeting Server M8 Medium
Full HD calls 1080p60 video 720p30 content	60	150
Full HD calls 1080p30 video 720p30 content	120	225
HD calls 720p30 video 720p5 content	240	450

Type of calls	Cisco Meeting Server Small M7 (VM)	Cisco Meeting Server M8 Medium
SD calls 480p30 video 720p5 content	480	850
Audio calls (G.711)	3000	3000

Meeting Server M8 platform supports a maximum load limit of 450,000.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco Trademark