



Cisco Meeting Server

Single Server Simplified Setup Guide

Version 2.9

December 20, 2021

What's new

Version	Change
December 20, 2021	Updated link to deployment guide in Appendix A.1.
June 01, 2020	New version of guide for 2.9
September 26, 2019	Minor correction.
October 25, 2018	First version published.

Contents

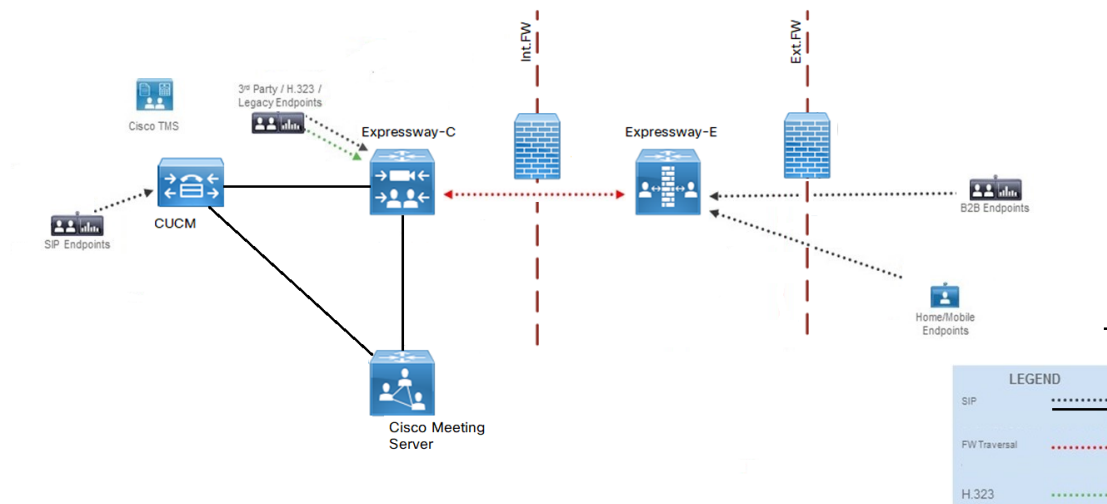
What's new	2
1 Introduction	5
1.1 Cisco Meeting Server Installation Assistant	5
1.2 Scope of the Simplified Deployment Guide	6
2 Configuration outline	7
2.1 Prerequisites	7
2.1.1 Software Versions	7
Task 1: Configuring IP interface for admin and/or A interface	8
Task 2: Setting host name	10
Task 3: Setting MMP accounts	10
Task 4: Upgrading software, if necessary	11
Task 5: Selecting and Setting License Details	11
Task 6: Configuring Network Time Protocol (NTP) server	12
Task 7: Generating certificates for Meeting Server	13
Task 8: Enabling Call Bridge service	15
Task 9: Enabling Web Admin service	15
Task 10: Configuring basic call settings	16
Task 11: Configuring incoming call rules for answering calls	17
Task 12: Configuring outgoing call rules	18
Task 13: Creating a test space	19
Task 14: Configuring Call Control to route to the Meeting Server	19
14a) Cisco Expressway/VCS: adding calling rules to Call Control for Meeting Server	20
14b) Unified CM: adding calling rules to Call Control for Meeting Server	22
Task 15: Optional. Configuring Unified CM adhoc conference escalation	25
Task 16: Enabling Web Bridge 3	26
Configure Web Bridge 3 on Interface A	26
Configure the c2w connection	26
Define Web Bridge 3 in Call Bridge	27
Task 17: Configuring user import (Optional)	29
Meeting Server LDAP settings explained	30
Configuring LDAP import	31
Running the LDAP import	34
Confirm Web Bridge 3 logins	35

Task 18: Configuring space templates	35
Create Space Template	36
Link Space Template to a LDAP Source	37
Finish Installation	38
Appendix A Additional information	39
A.1 Firewall ports information	39
A.2 Adding firewall traversal and external networks	39
A.3 Microsoft deployment information	39
Appendix B LDAP Tips and Examples	40
B.1 Tips on Meeting Server LDAP Mappings	40
B.2 Tips on LDAP	40
Example 1: Import all Active Directory Users, set JID based on sAMAccountName, and create a space	41
Example 2: Import all users that are members of a specific Active Directory group, cn=CMSAdmins,cn=Users,=dc=company,dc=com and create spaces for each	41
B.3 Common user LDAP filters	41
Appendix C ActiveControls CallLeg Profiles	43
C.1 Purpose	43
C.1.1 Settings Included	43
C.2 Configuration	43
Cisco Legal Information	46
Cisco Trademark	47

1 Introduction

This guide covers a simplified deployment of Meeting Server intended to reduce the time and complexity needed to complete a basic stand-alone installation. This deployment implements a stand-alone conference bridge integrated with Unified CM or Expressway/VCS call control as shown in Figure 1. It is also enhanced with the Meeting Server Web Bridge functionality that enables browser-based clients to connect to your conferences.

Figure 1: Cisco Meeting Server simple deployment



1.1 Cisco Meeting Server Installation Assistant

The Cisco Meeting Server Installation Assistant is a utility that you can download to complete a simplified deployment. Using the Installation Assistant has many advantages over a manual setup – the Installation Assistant:

- provides a graphical, guided experience
- does not require the user to enter commands manually in the CLI
- simplifies certificate creation and setup
- narrows configuration only to the elements necessary
- configures additional profiles for ActiveControl and meeting controls not previously included in the Simplified Deployment Guide

Note: You **must** use the Installation Assistant version that matches your Meeting Server version.

We recommend using the Installation Assistant to complete a single simplified Meeting Server deployment for the reasons described above. However, this guide outlines the best practices should you wish to manually complete such a deployment.

The Cisco Meeting Server Installation Assistant is a free download for Meeting Server customers and can be obtained from the Cisco [Software Download](#) site alongside the Meeting Server 1000 software.

1.2 Scope of the Simplified Deployment Guide

Cisco Meeting Server has additional functionality not part of this simplified deployment including resilient design, recording, streaming, Microsoft Integration, and more. For details on these additional components, see the configuration guides appropriate to your deployment requirements: <https://www.cisco.com/c/en/us/support/conferencing/meeting-server/products-installation-and-configuration-guides-list.html>. For this simplified deployment we are only using the Call Bridge, Database, Web Admin, and Web Bridge 3 components.

New for Meeting Server 2.9 is the Web Bridge 3 and web app component, which is intended to eventually replace the original Web Bridge and Meeting App component. In version 2.9, both Web Bridge 3 and the original Web Bridge can co-exist on Meeting Server. However, the original Web Bridge (also referred to as Web Bridge 2) will be removed from a future version of Meeting Server. The Cisco Meeting Server Installation Assistant 2.9 can deploy either the original Web Bridge 2 or the new Web Bridge 3.

This 2.9 version of the simplified guide only covers installing the new Web Bridge 3 and web app configuration.

2 Configuration outline

This guide assumes you are deploying Meeting Server as a virtual machine, either on a spec-based Hypervisor or on the Cisco Meeting Server 1000 platform.

- For the Cisco Meeting Server 1000 platform, the Hypervisor should have its network configured and be accessible via the network to complete these tasks. Refer to the: [Cisco Meeting Server 2.x, Installation Guide for Cisco Meeting Server 1000 and Virtualized Deployments](#) for specific instructions on how to complete the initial setup of the Meeting Server 1000 platform to get to where you can connect with the VMware client.
- For Virtual Machine installations, this guide assumes you have deployed the Meeting Server OVA file and allocated memory and CPU resources as necessary for the size of your deployment. Please refer to the [Cisco Meeting Server 2.x, Installation Guide for Cisco Meeting Server 1000 and Virtualized Deployments](#) for specific instructions on deploying the OVA and sizing your virtual machine.

To set up your Meeting Server to operate in this simple deployment scenario, check the [Prerequisites](#) and follow the configuration tasks.

2.1 Prerequisites

Before you proceed with the configuration tasks, the following requirements must be in place:

- A DNS "A" record must be created for the Meeting Server IP address using a Fully Qualified Domain Name (FQDN) you want end-users to be comfortable with; for example: **meetingserver.company.com**
- Choose a SIP Domain for Meeting Server; we suggest using a subdomain, such as **meet.company.com**
- Your Meeting Server virtual machine must be deployed to your hypervisor including having the hardware configured
- Configuration will require individuals with access to a virtual console for your Meeting Server Virtual Machine and individuals who can configure your call control platform

2.1.1 Software Versions

This guide is intended for a deployment using the following versions:

- Meeting Server 2.9
- Cisco Unified CM 11.5, 12.0, 12.5, 12.6
- Expressway X8.11 or X12.5
-

Caveats or steps for other versions are not detailed in this guide.

Task 1: Configuring IP interface for admin and/or A interface

Before using the console to complete this task, you need to do the initial login as follows:

1. Using your VMware client, power on your Meeting Server virtual machine and open a virtual console for the machine.
2. When the initial power on is complete, the Meeting Server login prompt displays.
3. Log in with the username “admin” and the initial password “admin”. If this is the first time the machine has been logged into, you will be prompted to enter a new password and confirm it. If so, set the new password for the admin account.

CAUTION: Passwords automatically expire after 6 months. Password policies, including strength and expiration rules can be customized using the **user rule** MMP commands. Please see the Password Rules section of the [Cisco Meeting Server MMP Command Reference](#) for more information.

4. After successful login, a command prompt displays. This is the Meeting Server MMP interface and is accessible via local machine console, or SSH after the networking interface has been configured.

Note: Meeting Server enforces an inactivity timer on all management interfaces. After approximately 30 seconds of inactivity on any management interface, the software will automatically log you out. You must log back in with your credentials to continue with your tasks.

A virtual instance of Meeting Server can have up to 4 network interfaces, a, b, c, d. For this deployment example, we will only use one interface, "a". The "a" interface must be configured with ethernet and IP address information to match the connected network.

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 enter the command:

iface a

- 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, to set the interface to 1GE, full duplex, enter:

iface a 1000 full

- b. Switch auto negotiation on or off using the command **iface a autoneg <on|off>**. For example, enter:

```
iface a autoneg on
```

Note: We recommend that the network interface is set to auto negotiation "on" unless you have a specific reason not to.

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

```
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, enter:

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

To remove the IPv4 address, enter:

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

3. Set DNS Configuration

Meeting Server requires DNS lookups for many of its activities 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. View the current DNS configuration, enter the MMP command:

```
dns
```

- b. Set the application DNS server, enter 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
```

The MMP interface should now be accessible via SSH to the IP address that was configured. Check that you can connect with your preferred SSH client.

Task 2: Setting host name

Meeting Server requires the hostname be configured to identify the server in logs and messages. We recommend you set the hostname to the FQDN of the server.

1. If necessary, SSH into the MMP and log in.
2. Set the hostname using the MMP command: `hostname <name>`, for example:

```
hostname meetingserver.company.com
```

3. Enter the `reboot` command to restart the server:

```
reboot
```

Note: A reboot is required after issuing the hostname command.

Task 3: Setting MMP accounts

For security purposes, you are advised to create your own administrator accounts as the 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.

1. While logged into the MMP console, create a new user with admin permissions with the MMP command `user add <name> admin`.

for example:

```
user add jbloggs admin
```

You will be prompted to supply a password, and to confirm the password. Note that the first time the new user logs in, they will be prompted to set their own password.

CAUTION: Passwords automatically expire after 6 months. Password policies, including strength and expiration rules can be customized using the `user rule` MMP commands. Please see the Password Rules section of the [Cisco Meeting Server MMP Command Reference](#) for more information.

2. We recommend you create a second admin account – repeat the commands in Step 1 to create a second admin level account.

3. After creating your new admin accounts delete the default “admin” username account. To remove this account, use the command `user del admin`

See the [MMP Command Reference Guide](#) for more information on user accounts, passwords, and permissions.

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.

Task 4: Upgrading software, if necessary

For this guide, your Meeting Server should be running software version 2.9 (or a 2.9 maintenance release). If running another version, obtain the appropriate file from the [software download](#) pages of the Cisco website and upgrade your Meeting Server using the following steps.

1. To find out which version the Meeting Server is running, SSH into the MMP, log in and enter:

```
version
```

2. To get the latest 2.9 software, go to the [software download](#) pages of the Cisco website. Click on **Meeting Server 1000**, then click on **TelePresence Software**. From the **Latest Release** expandable list, select **2.9.x**, ensuring you select the latest 2.9.x release available. From the list of files, select the file described: ‘**Use this image to upgrade a virtual machine deployment**’; download and extract this zip file which will result in a file named **upgrade.img**.

3. Use an SFTP client to upload the new software image to the MMP. For example:

```
sftp admin@10.1.124.10
```

```
put upgrade.img
```

where 10.1.124.10 is the IP address or FQDN of your Meeting Server.

4. After copying the file, to begin the upgrade, connect via SSH to the MMP and enter:

```
upgrade
```

Allow several minutes for the server to restart.

5. To verify that the upgrade was successful, SSH into the MMP, log in and enter:

```
version
```

Task 5: Selecting and Setting License Details

You need license files specific to your Meeting Server instance to complete the deployment. Meeting Server licenses are delivered using Cisco’s Product Activation Keys (PAK) and fulfilled using Cisco’s [License Registration Portal](#).

This section assumes that you have already purchased the licenses that will be required for your Meeting Server from your Cisco Partner and you have received your PAK code(s).

Follow these steps to register the PAK code with the MAC address of your Meeting Server using the [Cisco License Registration Portal](#).

1. Obtain the MAC address of your Meeting Server by logging in to the MMP of your server, and enter the MMP command: `iface a`

Note: This is the MAC address of your VM, not the MAC address of the server platform that the VM is installed on.

2. Open the [Cisco License Registration Portal](#) and register the PAK code(s) and the MAC address of your Meeting Server.
3. If your PAK does not have an R-CMS-K9 activation license, you will need this PAK in addition to your feature licenses.
4. The license portal will email a zipped copy of the license file. Extract the zip file and rename the resulting xxxxx.lic file to `cms.lic`.
5. Using your SFTP client, log into Meeting Server and copy the `cms.lic` file to the Meeting Server file system.
6. Restart the Call Bridge using the MMP command `callbridge restart`
7. After restarting the Call Bridge, check the license status by entering the MMP command `license`

The activated features and expirations will be displayed.

Task 6: Configuring Network Time Protocol (NTP) server

Configure Network Time Protocol (NTP) server to synchronize time between the Meeting Server components.

Note: Sharing a common view of time is important for multiple reasons. Time synchronization is necessary when checking for certificate validity and to prevent replay attacks..

1. Log in to the MMP using SSH or console.
2. Set up an NTP server, use the command:

```
ntp server add <domain name or IP address of NTP server>
```

for example:

```
ntp server add ntp.example.com
```

To find the status of configured NTP servers, enter the MMP command `ntp status`

See the [MMP Command Reference](#) for a full list of `ntp` commands.

Task 7: Generating certificates for Meeting Server

Meeting Server uses x.509 certificates to configure secure (TLS) connections for its services and for some authentication tasks. In this deployment, certificate configuration is required for the Call Bridge, Web Bridge, and Web Admin services. Certificates can be self-signed or signed by internal or external certificate authorities. For a full explanation of certificate uses and requirements, please see the [Certificate Guidelines](#).

For this simplified deployment we will use one x.509 certificate with the correct attributes signed by an internal or external Certification Authority (CA). Using a self-signed certificate here is possible but is not recommended as it will cause errors to be seen in web pages and will prevent you from incorporating Meeting Server into Unified CM as a conference bridge.

For this deployment, our certificate should have the server FQDN as the Common Name (CN) and must be in the Subject Alternate Name (SAN) attribute of the certificate. The "digitalSignature" key usage bit must also be set. To generate a Certificate Signing Request (CSR) and private key using the MMP:

1. Log in to the MMP using SSH or console.
2. Enter the `pki csr` command using this syntax:

```
pki csr <key/cert basename> <CN:value> [OU:<value>] [O:<value>] [ST:<-value>] [C:<value>] [subjectAltName:<value>]
```

For example:

```
pki csr singleCert CN:meetingserver.company.com
```

Note: The `CN`, `OU`, `O`, `ST`, `C` values and other attributes are optional in the certificate and are omitted here for simplicity. They can be defined and included if desired, see the [Certificate Guidelines](#) for a complete breakdown of the commands.

Note: The `CN` value should always be part of the SubjectAltName (SAN) list. The Meeting Server `pki csr` command adds the `CN` to the SAN list automatically so you do not have to list it separately.

The output of this command generates a private key file with the extension `.key` and a Certificate Signing Request (CSR) file with the extension `.csr` on the Meeting Server's file system.

3. Using your SFTP client, log into Meeting Server and copy the CSR file to your machine so it can be supplied to your signing certificate authority.
4. Supply the CSR file to your certificate authority to be signed. They will return a signed certificate in a binary or text encoded (PEM) format (for example, `singleCert.crt`). This guide

will use examples using PEM files. Other formats are supported but not documented here. See the [Certificate Guidelines](#) for more information about supported formats and uses. Obtaining your files in PEM format or converting them to PEM is recommended for simplicity.

5. To complete the installation, you will need three variations of your certificate files. You will need the signed certificate itself (example: **singleCert.crt**), the Root & Intermediate certificate bundle from your CA (example: **ca-bundle.crt**), and a full chain file version of your certificate (example: **single-chain.crt**).

The Root & Intermediate certificate bundle includes the chain of trust that signed your certificate. This means a certificate bundle that includes the public certificate of each Intermediate CA in the hierarchy of CAs that signed your certificate leading back to and including the Root CA. CAs typically provide such a bundle pre-configured, or you can create your own by downloading the public certificates of the CAs in your chain.

The full chain file is simply a certificate bundle that starts with your server certificate, followed by the same contents as the Root & Intermediate certificate bundle. It includes the public certificates of each step in the chain – from the server certificate, all the way to the Root CA. You may have to create this full chain file yourself depending on the options your CA provides.

Certificate bundles using PEM files are created by simply concatenating the text versions of the certificates together in a single file. The text version of a certificate in a PEM file is the encoded text in between and including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- tag lines.

To create a bundle file:

- a. Open the certificate file to include using a plain text editor such as Notepad or Text Edit. Highlight and copy the block of encoded certificate text including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- lines.
 - b. Paste the certificate contents into a new empty text file.
 - c. For each additional certificate to add: open and copy the block of encoded certificate text including the BEGIN and END tag lines and paste at the end of the new text file that was created in Step . Each certificate should start on its own line, with no extra lines in between certificates. Certificates should be pasted in hierarchical order so that the file ends with the Root Certificate.
 - d. Place one extra blank line at the end of the file and save the text file with an extension of .pem .cer or .crt. Example: **single-chain.crt**
6. Using your SFTP client, log into Meeting Server and copy the signed certificate file, certificate authority bundle, and full chain file to your Meeting Server.

Note: File names are restricted on Meeting Server, so your files must use common file extensions such as `.crt`, `.cer`, `.key`, `.pem` or `.der`

Task 8: Enabling Call Bridge service

The Call Bridge service must be configured with the certificate to use and which network interface to listen on.

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. Log in to the MMP using SSH or console and configure the Call Bridge to listen on interface A by entering the MMP command:

```
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.

2. Configure the Call Bridge to use the certificate, key, and bundle generated in "Generating certificates for Meeting Server" on page 13, using the MMP command `callbridge certs <keyfile> <certificatefile> <ca bundle>`, for example:

```
callbridge certs singleCert.key singleCert.crt ca-bundle.crt
```

3. Use the MMP command `callbridge restart` to restart the Call Bridge to apply the changes:

```
callbridge restart
```

If successful, you will get SUCCESS lines returned stating that the Call Bridge is correctly configured for network and certificate values.

Task 9: Enabling Web Admin service

The Web Admin Interface is the browser-based interface to Meeting Server for administrators. The Web Admin service must be configured with the certificate to use and which interface to listen on before it can be enabled. By default, Web Admin will listen on the standard HTTPS port of 443. However, in this deployment we will also enable Web Bridge 3 for conference users and set a preference for that service to be available on the default HTTPS port. To enable both services to co-exist, we will configure Web Admin to listen on port 445 and require administrators to supply the extra port information when browsing to the Web Admin interface.

1. Use the MMP command `webadmin listen <interface> <port>` to instruct Web Admin to listen on interface a port 445:

```
webadmin listen a 445
```

2. Use the MMP command `webadmin certs <keyfile> <certificatefile> <ca bundle>` to configure Web Admin with the certificate files generated in "Generating certificates for Meeting Server" on page 13. For example:

```
webadmin certs singleCert.key singleCert.crt ca-bundle.crt
```

3. Use the MMP command `webadmin enable` to start the Web Admin service.

```
webadmin enable
```

If successful, you will get SUCCESS lines returned stating Web Admin is correctly configured for network and certificate values. Check the service is operational by using a web browser and enter the Web Admin address, for example: <https://meetingserver.company.com:445>

Note the specific use of https in the prefix and the :445 at the end of the address.

If you do not get the success messages or the page did not load properly, enter the MMP command `webadmin` by itself to display the existing configuration. Check for any typing errors with the files specified. Correct any errors and try enabling the service again before proceeding.

Task 10: Configuring basic call settings

The Call Bridge service is now running but is using only the system defaults. In this task we will configure some common settings needed before making test calls.

1. Log in to the Web Admin Interface using your browser and go to **Configuration > Call settings**.
2. Select the appropriate **SIP media encryption** setting (**allowed**, **required** or **disabled**).

The **SIP media encryption** setting must be compatible with your existing call control and endpoints. The setting recommended for most usages is **allowed** – this allows both encrypted and non-encrypted connections. Take care before setting to **required** – a mismatch of encryption capabilities between Meeting Server and devices will prevent calls from connecting. Choose your setting and click **Submit** at the bottom of the page.

3. On the same page, you can optionally:
 - Choose to enable **SIP call participant labels** if you want participant names to display overlaid on video images. Enabling participant labels is encouraged for those migrating from MCUs that use this feature.
 - Customize the maximum bandwidth per call to use for the different call types. Bandwidth numbers are in bits/sec. We recommend leaving bandwidth values at their default settings for this deployment.
1. Click **Submit** after making any changes.

Task 11: Configuring incoming call rules for answering calls

The **Configuration > Incoming calls** page determines how the Meeting Server handles incoming SIP calls. Any call routed to the Meeting Server will have the alias being called checked against the rules in the **Call matching** table to determine where Meeting Server should look for potential matches. Each rule can be set to match for any combination of users, spaces, IVRs, or Microsoft Skype/Lync lookups. Meeting Server checks incoming calls by checking the value after the "@" symbol in the called alias with the values in the Domain Name column of the table.

The example Call matching rule below seeks to match all calls coming in with the dialed domain **meet.company.com** to both Cisco Meeting App users and spaces.

Incoming call handling

Call matching

<input type="checkbox"/>	Domain name	Priority	Targets spaces	Targets users	Targets IVRs	Targets Lync
<input type="checkbox"/>	meet.company.com	0	yes	yes	yes	no
	<input type="text"/>	<input type="text"/>	yes <input type="button" value="v"/>	yes <input type="button" value="v"/>	yes <input type="button" value="v"/>	no <input type="button" value="v"/>

1

We recommend that rules are created for every domain expected for incoming calls. With some call control solutions, the domain in the alias may be the IP address or hostname of the Meeting Server.

Rules with a higher priority value are matched first. In cases where multiple rules have the same priority, matching occurs based on alphabetical order of the domain.

After a rule is matched and executed, rules further down the list are ignored for the call.

If all Call matching rules fail, the next table (**Call forwarding**) is checked. Note that Call forwarding is not covered in this deployment.

Points to note:

- Once a domain is matched, matching for space and/or users is only done on the part of the URI before the "@" symbol.
- The highest priority rule that targets space aliases is used to form the URI in the invitations created by Cisco web app. Rules that are for the deployment as a whole should be the highest priority rules, with rules for individual IP addresses or hostnames set using lower priorities.

To configure incoming call rules:

1. Log in to the Web Admin Interface using your browser and go to **Configuration > Incoming calls**.
2. Configure the highest priority incoming rule to be the SIP domain you will be using for spaces. Use the empty row to add a rule with the following values:
 - **Domain name:** <your SIP domain for Meeting Server> (for example, meet.company.com)

- **Priority:** 100
- **Target spaces, users, IVRs:** set to **yes**

Click **Add New** to save the changes.

3. To ensure compatibility with different trunk configurations, add a rule for the FQDN of your Meeting Server. (If your SIP domain and Meeting Server FQDN are the same, you can skip this step.) Use the empty row to add a rule with the following values:

- **Domain name:** *<your FQDN for Meeting Server>* (for example, meetingserver.company.com)
- **Priority:** 90
- **Target spaces,users, IVRs:** set to **yes**

Click **Add New** to save the changes.

4. To ensure compatibility with different trunk configurations, add a rule for the IP address of your Meeting Server. Use the empty row to add a rule with the following values:

- **Domain name:** *<IP address of interface of where Call Bridge is listening>*
- **Priority:** 90
- **Target spaces,users, IVRs:** set to **yes**

Click **Add New** to save the changes.

Task 12: Configuring outgoing call rules

To make calls out from Meeting Server, calls must be directed via the **Outbound calls** rules to a destination, such as Unified CM or Expressway/VCS. Similar to the incoming call rules, all routing is based on the domain of the dialed alias. Rules are processed highest priority to lowest, and if matched, Meeting Server attempts to send the call to the SIP proxy defined. The **Behavior** setting in a rule controls whether further rules are processed if the rule matches, but the remote proxy rejects the call. For this simplified deployment, we will route all outbound calls to our singular call control (Unified CM or Expressway/VCS). More advanced configuration details are covered in the larger Meeting Server deployment guides.

To configure outgoing call rules:

1. Log in to the Web Admin Interface using your browser and go to **Configuration > Outbound calls**.
2. Create a new outbound rule with the following values:
 - **Domain name:** [Leave blank. Note that this is a special use that allows us to match all domains]
 - **SIP Proxy to use:** Enter the FQDN of your Unified CM or Expressway/VCS call control node (IP Address can be used, but FQDN is recommended)

- **Local contact domain:** [Leave blank]
- **Local from domain:** Enter your SIP domain for Meeting Server (for example: meet.company.com)
- **Trunk type:** Standard SIP
- **Behavior:** Continue
- **Priority:** 1
- **Encryption:** Auto

Click **Add New** to save the changes.

3. Optional. If you wish to define additional proxies for failover or other domains, you can do so, but it is not required. For most scenarios, we recommend that you route to call control, and do your destination routing there.

Task 13: Creating a test space

Creating a test space allows verification of your configuration once call control has been configured in [Task 14](#). Aliases defined in this table will only include the left-hand side of the SIP URI. The incoming call rules table handles matching on the right-hand side of the alias.

1. Log in to the Web Admin Interface using your browser and go to **Configuration > Spaces**.
2. Use an empty row to create a new space. Fill in the fields with the following values:
 - **Name:** Test Meeting
 - **URI user part:** test
 - **Secondary URI user part:** 881000
 - **Call ID:** 881000

For **Secondary URI user part**, use an E.164 value that will be compatible with the dial plan you will be routing to Meeting Server. For **Call ID**, the parameter supports only a numeric value and therefore, should be configured with any number that is not already in use. In this example, for simplicity, it is set to the same value as the **Secondary URI user part**.

3. Click **Add New** to save the new values.

Task 14: Configuring Call Control to route to the Meeting Server

The previous tasks configured Meeting Server to listen to incoming calls and where to send calls. Next, you need to configure your Call Control to identify calls intended for Meeting Server and where to send them.

In this deployment, Meeting Server will listen for SIP calls on the "a" network interface where Call Bridge is listening on TCP ports 5060 or 5061. You must configure your Call Control to

identify which alias patterns are intended for Meeting Server and the trunks/zones of where to send the calls.

This guide has both Cisco Expressway/VCS and Cisco Unified CM examples. Complete [Task 14a](#) for Cisco Expressway/VCS deployments, or [Task 14b](#) if using Cisco Unified CM.

14a) Cisco Expressway/VCS: adding calling rules to Call Control for Meeting Server

This task will add dial plan configuration to an existing Cisco Expressway/VCS to route SIP URIs and E.164 dial patterns to Meeting Server using SIP TLS. Use of TLS is described as best practice, however use of SIP TCP port 5060 is also valid.

1. Sign in to the Expressway as an administrator.
2. Set up a zone to route calls to the Meeting Server:
 - a. In the Expressway web interface, go to **Configuration > Zones > Zones**
 - b. Click **New** to create a new Zone with the settings below:
 - **Name** = <Label for your zone. Example: CMS1>
 - **Type** = Neighbor
 - **Hop Count** = [Leave Default]
 - **H.323 Mode** = Off.
 - **SIP Mode** = On
 - **SIP Port** = 5061
 - **Transport** = TLS
 - **TLS verify** = Off
 - **SIP Accept Proxied Registrations** = Allow
 - **Media encryption mode** = Auto
 - **ICE support** = Off
 - **Multistream Mode** = On
 - **Preloaded SIP routes support** = Off
 - **AES GCM support** = Off
 - **Authentication Policy** = Treat as authenticated
 - **SIP Authentication Trust Mode** = Off
 - **Look up Peers By** = Address
 - **Peer 1 Address** = <the Call Bridge FQDN> (example: meetingserver.company.com)

Note: FQDN is recommended as TLS is being used. IP Address can also be used provided **TLS verify** = Off

- **Zone Profile** = Default
- c. Click **Create Zone** to save the new zone.
3. Add a search rule to route to the Meeting Server:
 - a. In the Expressway web interface, go to **Configuration > Dial Plan > Search rules**
 - b. Click **New** to create a new search rule with the settings below, edit domain and priority values to match your deployment:
 - **Name** = <Label for your rule. Example: SIP URI to CMS1>
 - **Priority** = <Set relative to your other search rules>
 - **Protocol** = Any
 - **Source** = Any
 - **Request Must be Authenticated** = No
 - **Mode** = Alias pattern match
 - **Pattern type** = Regex
 - **Pattern string** = `.*@meet.company.com`
 - **Pattern Behavior** = Leave
 - **On Successful Match** = Stop
 - **Target** = <Select the Zone created for Meeting Server>
 - **State** = Enabled
 - c. Click **Create search rule** to save your new zone.
 4. The rule created in the previous step routed calls using the Meeting Server SIP domain. If you also use an E.164 dial plan, create another search rule to route based on the E.164 number pattern you will use for Meeting Server.
 - a. In the VCS web interface, go to **Configuration > Dial Plan > Search rules**
 - b. Click **New** to create a new search rule with the settings below. Edit the example regex pattern to match your dial plan. The example routes 88XXXX patterns to Meeting Server.
 - **Name** = <Label for your rule. Example: e164 aliases to CMS1>
 - **Priority** = <Set relative to your other search rules>
 - **Protocol** = Any
 - **Source** = Any

- **Request Must be Authenticated** = No
- **Mode** = Alias pattern match
- **Pattern type** = Regex
- **Pattern string** = (88\d{4})*
- **Pattern Behavior** = Replace
- **Replace String**: \1@meet.company.com
- **On Successful Match** = Stop
- **Target** = <Select the Zone created for Meeting Server>
- **State** = Enabled

c. Click **Create search rule** to save your new zone.

After completing these steps, the new zone should show in the **Configuration > Zones > Zones** page as **SIP Status** = Active and **Search Rule Status** should show 2 enabled search rules.

5. Now that call control is configured, you can dial into the Meeting Server test space created in [Task 13](#) to validate the configuration. With an endpoint registered to your call control, dial the SIP URI of the test meeting created earlier (for example: **test@meet.company.com**). Repeat the test using the E.164 alias.

If your calls fail to connect, use the Event Log in the Web Admin interface of Meeting Server and the Search and Call history pages in the Expressway/VCS web interface to see where your call is failing.

14b) Unified CM: adding calling rules to Call Control for Meeting Server

This task adds dial plan configuration to an existing Cisco Unified CM to route SIP URIs and E.164 dial patterns to Meeting Server using SIP TLS. Use of TLS is described as best practice, however use of SIP TCP port 5060 is also valid. SIP TCP configuration is not covered in this guide.

See [Cisco Meeting Server x.x with Cisco Unified Communications Manager Deployment Guide](#) for more details.

Our testing has been done on trunks without Media Termination Point (MTP) configured. Therefore:

- Disable MTP if this will not negatively affect your deployment. Turning off MTP might have a negative impact on your deployment if you are using SCCP phones and need to send DTMF to the Meeting Server.
- If the above is not a valid implementation, you may need to increase the MTP capacity on the Unified CM depending on the number of simultaneous calls.

1. If not done so already, install a CA signed certificate for the CallManager service on each Unified CM which has the CallManager service activated.

Note: This is a recommendation and not a requirement as Meeting Server does not validate received certificates by default, it accepts all valid certificates and will accept Call Manager's self-signed certificate.

- a. Log into the Unified CM **OS Administration** page, choose **Security > Certificate Management**.
 - b. In the **Certificate List** window, click **Generate CSR**.
 - c. From the **Certificate Name** drop-down list, choose **CallManager**.
 - d. Click **Generate CSR** to generate a Certificate Signing Request.
 - e. Once the CSR is successfully generated, click **Download CSR**. From the Download Signing Request dialog box choose **CallManager** and click **Download CSR**.
 - f. Get this CSR signed by a Certificate Authority. An internal CA signed certificate is acceptable.
 - g. Once a certificate is returned from the CA, go to the **Upload Certificate/Certificate chain** window. From the **Certificate Purpose** drop-down list select **CallManager-trust**. Browse and upload first the root certificate, followed by the intermediate certificates. From the **Certificate Purpose** drop-down list select **CallManager**. Browse and upload the certificate for the CallManager Service.
 - h. For the new certificate to take effect you need to restart the CallManager service in **Cisco Unified Serviceability**, do this during a maintenance period.
2. Upload the root and intermediate certificates of the certificate you generated in Task 7 to the CallManager-trust store.
 - a. From the Cisco Unified Communications Manager **OS Administration** page, choose **Security > Certificate Management**.
 - b. Click **Upload Certificate/Certificate Chain**. The Upload Certificate/Certificate Chain popup window appears.
 - c. From the **Certificate Purpose** drop-down list choose **CallManager-trust**.
 - d. Browse and upload first the root certificate, followed by the intermediate certificates to CallManager-trust.
 3. Create a SIP trunk security profile.

Cisco Unified Communications Manager applies a default security profile called **Non Secure SIP Trunk** when you create the SIP Trunk, this is for TCP. To use TLS, or something other than the standard security profile, follow these steps:

- a. Log into Cisco Unified Communications Manager Administration.
 - b. Go to **System > Security > SIP Trunk Security Profile**.
 - c. Click **Add New**.
 - d. Complete the fields as follows:
 - **Name** = type in a name, e.g. "CMS_SecureTrunk"
 - **Device Security Mode** =select **Encrypted**
 - **Incoming Transport Type** = select **TLS**
 - **Outgoing Transport Type** = select **TLS**
 - **X.509 Subject Name** = enter the CN of the Call Bridge certificate. This should be the FQDN of your Meeting Server.
 - **Incoming Port** = enter the port that will receive TLS requests. The default for TLS is 5061
 - **Accept Replaces Header** = check this box if you intend to use Call Bridge Grouping.
 - e. Click **Save**
4. Check that your SIP Profile is configured correctly. If using the default **Standard SIP Profile For TelePresence Conferencing** on Unified CM version 10.5.2 or later, this should be sufficient. The key values to ensure are checked are: **Allow iX Application Media**, **Use Fully Qualified Domain Name in SIP Requests**, and **Allow Presentation Sharing use BFCP**.
 5. Create the SIP trunk.
 - a. In Unified CM, go to **Device >Trunk**.
 - b. Click **Add New**.
 - c. Configure these fields:
 - **Trunk Type** = SIP trunk
 - **DeviceProtocol** =SIP
 - **Trunk Service Type** = None (default)
 - d. Click **Next**
 - e. Configure the destination information for the SIP trunk, see Table 1 below.

Table 1: Destination information for the SIP Trunk

Field	Description
Device name	Type in a name e.g. CiscoMeetingServer (no spaces allowed)

Field	Description
Device pool	The pool you want your device to belong to (as configured in System > Device Pool in Unified CM).
SRTP Allowed	Select SRTP Allowed to allow media encryption
Inbound Calls > Calling Search Space	Select default, not required if only allowing escalated 2-way adhoc calls from Unified CM to a meeting on the Meeting Server.
Outbound Calls > Calling Party Transformation CSS	Select as appropriate.
SIP Information > Destination address	Enter the FQDN of a single Meeting Server, it must match the CN of the Meeting Server certificate. Note: For clusters, enter the FQDN of a single Meeting Server
SIP Information > Destination Port	Enter 5061 for TLS
SIP Trunk Security Profile	Select the security profile that you created in step 3.
Rerouting Calling Search Space	When doing call bridge grouping, set this to a calling search space that contains the partitions of the calling parties.
SIP Profile	Select the Standard SIP Profile For TelePresence Conferencing
Normalization Script	Assign the cisco-meeting-server-interop script to this SIP trunk. Note: ideally download the latest normalization script from the Cisco website. For older UCM versions that do not have the Meeting Server script,download the latest interop scripts or alternatively use the cisco-telepresence-conductor-interop script as it has similiar interop behaviors.
Run On All Active Unified CM Nodes	Check this checkbox if you wish calls to egress other Unified CM nodes as well.

- Click **Save** and apply the configuration.
- Use the **Trunk List** to confirm that the trunk goes into service after a few minutes.
- Now call control is configured, you can dial into the Meeting Server test space created in [Task 13](#) to validate the configuration. With an endpoint registered to your call control, dial the SIP URI of the test meeting created earlier (for example: **test@meet.company.com**). Repeat the test using the E.164 alias.

If your calls fail to connect, use the Event Log in the Web Admin interface of Meeting Server and tracing diagnostics in Unified CM to identify where your call is failing.

Task 15: Optional. Configuring Unified CM adhoc conference escalation

Meeting Server can act as the video and audio bridge for Unified CM devices that request bridging multiple parties using the **Conference** button on the device. This feature is optional but

recommended for Unified CM deployments. You can add this feature to your deployment by following the steps in Chapter 4 "Setting up escalated ad hoc calls" in the [Cisco Meeting Server x.x with Cisco Unified Communications Manager Deployment Guide](#).

Complete that configuration if desired and then return to the next task in this guide.

Task 16: Enabling Web Bridge 3

Enabling Web Bridge support requires configuring the Web Bridge 3 service, configuring the link between Call Bridge/Web Bridge (labeled c2w), and defining the Web Bridge's location in the Call Bridge's configuration.

Note: The XMPP service is not used when you deploy Web Bridge 3.

Note: The Web Bridge 3 and c2w configurations use the fullchain certificate files (example: **single-chain.crt**) and not the server certificate files as was common with previous Meeting Server conventions.

Configure Web Bridge 3 on Interface A

1. Log in to the MMP using SSH or console.
2. Use the MMP command `webbridge3 https listen <interface[:port]>` to configure Web Bridge 3 to listen on Interface "a" and port 443

```
webbridge3 https listen a:443
```

3. Configure Web Bridge 3 service with the certificate key and full chain certificate file generated in [Task 7](#) using the MMP command `webbridge3 https certs <keyfile> <crt-fullchain-file>`, for example:

```
webbridge3 https certs singleCert.key single-chain.crt
```

4. The Web Bridge 3 supports HTTPS. It will forward HTTP to HTTPS if configured to use "http-redirect". If desired, you can enable HTTP redirect using the following command:

```
webbridge3 http-redirect enable
```

Configure the c2w connection

1. Use the MMP command `webbridge3 c2w listen <interface[:port]>` to configure the Call Bridge to Web Bridge 3 (c2w) connection to listen on Interface "a" and port 9999

```
webbridge3 c2w listen a:9999
```

2. Configure the c2w interface to use the server certificate key and full chain certificate file generated in [Task 7](#) using the MMP command `webbridge3 c2w certs <keyfile> <crt-fullchain-file>`

For example:

```
webbridge3 c2w certs singleCert.key single-chain.crt
```

3. Configure the c2w interface to trust the Call Bridge's certificate using the full chain certificate file generated in [Task 7](#) using the MMP command `webbridge3 c2w trust <cert-fullchain-file>`

For example:

```
webbridge3 c2w trust single-chain.crt
```

4. Use the MMP command `webbridge3 enable` to enable the Web Bridge 3 service:

```
webbridge3 enable
```

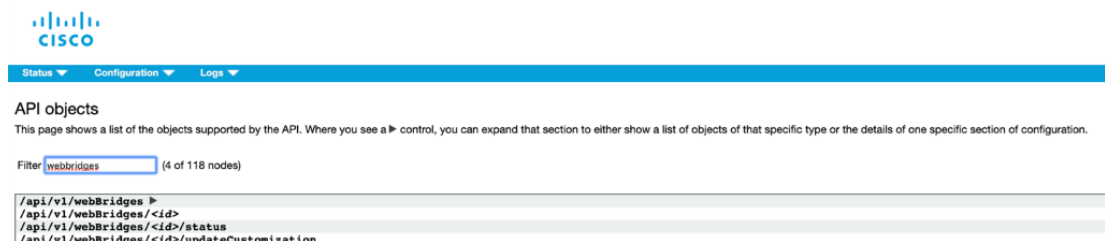
The server should respond with SUCCESS messages if completed properly. If you do not get all SUCCESS messages, enter the MMP command `webbridge3` by itself to display the existing configuration. Check for any typing errors with the files specified. Correct any errors by disabling the webbridge3 service with the MMP command `webbridge3 disable`, repeating the corrected commands and enabling the service again before proceeding.

Define Web Bridge 3 in Call Bridge

The Call Bridge must be told where to reach Web Bridge 3 and how to verify the certificate the c2w interface will present. This requires both MMP and API configuration.

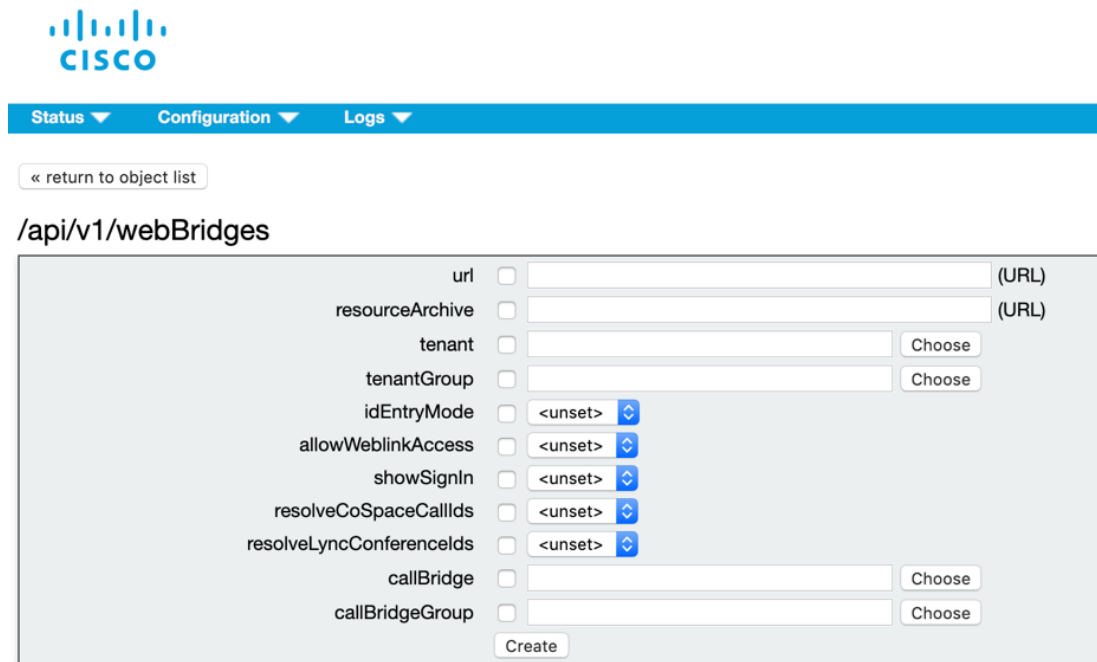
1. Configure the Call Bridge to trust the c2w interface of Web Bridge 3 using the full chain certificate file assigned to the c2w interface of Web Bridge 3. Use the MMP command `callbridge trust c2w <bundle>`. For example:


```
callbridge trust c2w single-chain.crt
```
2. Telling Call Bridge where to reach Web Bridge 3 requires the creation of a `/api/v1/webBridges` object in the Meeting Server API with the URL parameter configured using the format `c2w://<NetworkAddress>:<port>`. This guide will use the API configuration option available in the Web Admin interface to complete the task.
 - a. Log in to the Meeting Server Web Admin interface and select **Configuration > API**:
 - b. Using the **Filter** input box, type `webBridges` to filter the list view, as shown here:



- c. Locate the required row from the resulting list of API objects and tap the ► after `/api/v1/webBridges`

- d. Click **Create new** to create a new webBridge object, the following parameter fields display as shown here:



The screenshot shows the Cisco Web Admin interface. At the top, there is a navigation bar with 'Status', 'Configuration', and 'Logs' tabs. Below the navigation bar, there is a link to '« return to object list'. The main heading is '/api/v1/webBridges'. Below this, there is a form with the following fields:

- url: (URL)
- resourceArchive: (URL)
- tenant: Choose
- tenantGroup: Choose
- idEntryMode: <unset> [dropdown]
- allowWeblinkAccess: <unset> [dropdown]
- showSignIn: <unset> [dropdown]
- resolveCoSpaceCallIds: <unset> [dropdown]
- resolveLyncConferencelds: <unset> [dropdown]
- callBridge: Choose
- callBridgeGroup: Choose

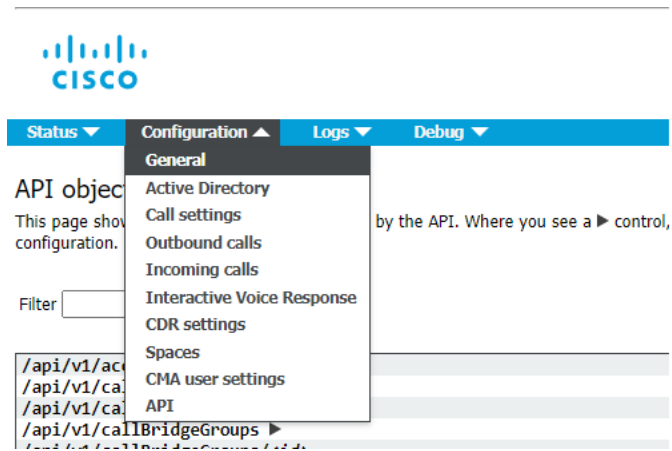
At the bottom of the form, there is a 'Create' button.

- e. Fill in the **url** field using the format **c2w://<FQDN>:9999** with the FQDN value used when creating the Meeting Server's certificate in [Task 7](#). Example:

c2w://meetingserver.company.com:9999

Note: The FQDN entered here must match the CN or SAN values of the certificate assigned to the c2w interface of Web Bridge 3 and must resolve to the IP of the server.

- f. Click **Create** to save the new Web Bridge entry.
- g. From the Web Admin interface select **Configuration > General**, as shown here:



- h. Scroll to locate the **Web Bridge URI** setting under **External Access** and configure it to the HTTPS URL for your Meeting Server. For example:

https://meetingserver.company.com

Note: This value will change if you opt to add Expressway web proxy. It is the address that is advertised in invitations created to invite users to meetings.

- i. Click **Submit** to save your changes.
- j. Confirm the Call Bridge is not reporting errors for the Web Bridge. From the Web Admin interface, select **Status > General** and check that there are no alarms in **Fault conditions** or recent errors under **Recent Errors and Warnings**.

Once you have confirmed that there are no faults, you can test the Web Bridge functionality using guest access.

1. Using a supported browser, enter the web address to your Meeting Server. For example, **https://meetingserver.company.com**.
2. Click the **Join Meeting** link and when prompted, enter the CallID that was set up in your test space in "Creating a test space" on page 19. Enter a name for the guest user, and join the call. The WebRTC app should load and allow the user into the space. You can also connect other computers to the test meeting, or dial in with SIP participants to populate the meeting.

Task 17: Configuring user import (Optional)

Importing users from an LDAP directory allows end-users to log into Cisco web app using their own account to manage their spaces and join meetings. Participants can also join meetings via a web browser as 'guest' users, however, guest users cannot manage meetings or create/manage spaces.

Note: This task is optional and does **not** need to be completed if you only wish to enable Guest access. If you don't wish to enable user logins to web app, skip this task.

Note: Completing this task requires significant use of the Meeting Server API. We recommend that you use the Cisco Meeting Server Installation Assistant to configure your deployment if you are not comfortable with API tasks. Alternatively, you can complete this setup by deploying Cisco Meeting Management to configure user import.

The Meeting Server LDAP import settings allow you to specify which user records to target from an existing directory and how to configure matching users in Meeting Server. The import optionally supports creating a personal space for each imported user. Which users and specific values to import is a deployment-specific decision.

For the simplified deployment example, we will import all users from Active Directory, set their login that they will use for web app, and create a space for each user.

Meeting Server LDAP settings explained

- **LDAP Server Location/address:** network location of the LDAP Server
- **name:** a label to help identify objects in the API
- **LDAP Username/Password:** credentials used to connect to the LDAP server. Uses LDAP DN syntax
- **Port/portNumber:** The network port to use when connecting to the LDAP server.
- **Secure:** When enabled, connection will use LDAPS instead of LDAP.
- **Base Distinguished Name/baseDN:** LDAP location where Meeting Server's search will start. Uses LDAP DN syntax
- **Filter:** Search filter that defines which LDAP objects to include in the search. Uses LDAP filter syntax

For each user matched by the above search settings, Meeting Server creates a user in Meeting Server using the Field Mapping expressions the administrator defines. The Mappings can use regex expressions and LDAP property names to construct results based on the imported user's LDAP values. The commonly used Field Mappings are:

- **Display Name/nameMapping:** Name shown for the user in user searches and directories in Meeting Server
- **Username/jidMapping:** The username the user will use to login to web app – the result must be unique for each user
- **Space Name/coSpaceNameMapping:** Label given to the auto-generated space for that user

- **Space URI user part/coSpaceUriMapping:** Defines the user portion of the URI for the auto-generated space for that user – result must be unique for each user
- **Space secondary URI user part/coSpaceSecondaryUriMapping:** Defines a secondary URI for the auto-generated space for the user (optional). Usually used to assign a E164 style URI to the space – result must be unique for each user
- **Space call ID/coSpaceCallIdMapping:** Sets the call ID for the auto-generated space for the user (optional). If not defined, a random call ID is generated automatically – result must be unique for each user

To create mappings that are unique to each user, the mappings usually include references to the LDAP properties found in the LDAP server for the user. These references can be made using the syntax `$propertyName$`, for example `$sAMAccountName$` or `$mail$`

All field mappings except **Username** are optional. If no Space related field mappings are defined, no space will be created for the imported users.

Configuring LDAP import

To ensure this configuration is compatible with Cisco Meeting Manager and Space templates (introduced in Meeting Server 2.9) the LDAP import will be defined using the Meeting Server API.

1. Log in to the Meeting Server Web Admin interface and select **Configuration > API**:
2. Using the **Filter** input box, type **ldapServers** to filter the list view. Locate the required row from the resulting list of API objects and tap the ► after **/api/v1/ldapServers**
3. Click **Create new** to configure a new ldapServers object.

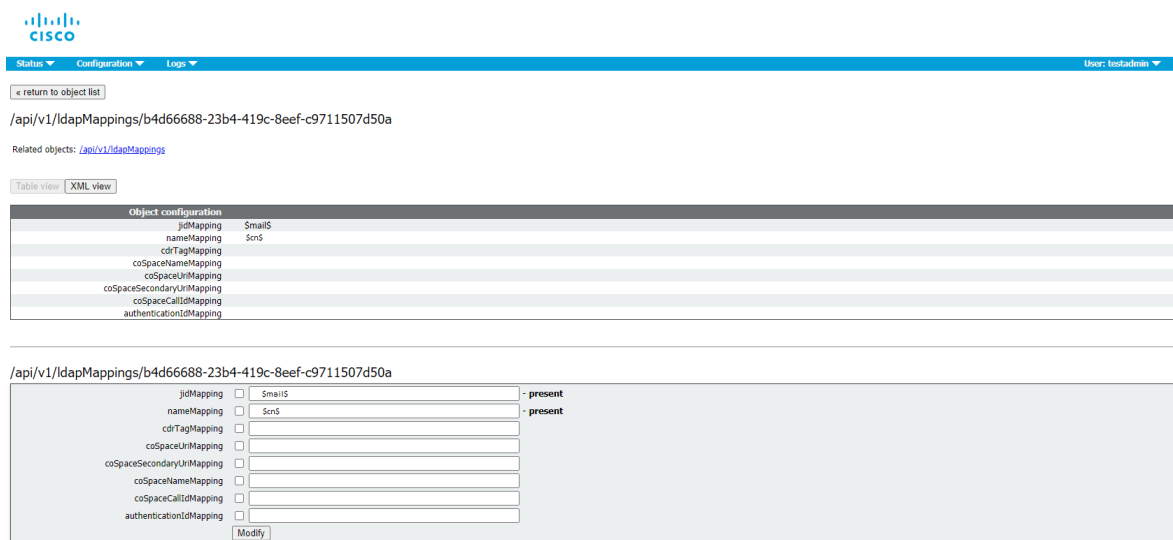
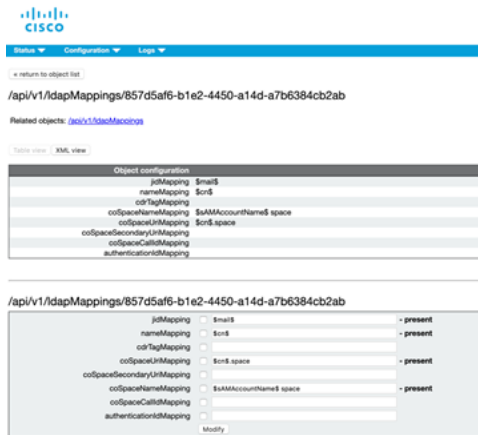
Configure the LDAP values to point to a domain controller in your Windows environment. The username should be in the LDAP DN format, but for Active Directory servers, you can use the simpler UPN format, i.e. **username@domainFQDN**. The username supplied does not need to be an administrator or have special access, it just needs to be a valid domain user to read the directory.

4. Configure the server values. Example values below must be updated to match your environment. The checkbox next to each value will automatically mark when the field is edited.
 - **address:** *pd11.companv.com*
 - **name:** Enter a label for this set of settings. Example: Americas PDC
 - **portNumber:** 636
 - **username:** *john.doe@company.com*
 - **password:** *<Password for supplied user>*

- **secure**: set to **true**
- **usePagedResults**: leave unset unless using Oracle Internet Directory. If using Oracle Internet Directory, set to **false**

Note: For environments with multiple domains, using a Global Catalog server instead of a Domain Controller is recommended. Global Catalog Servers listen on TCP 3268 and Secure 3269.

5. Make sure the checkbox is marked for each value you set or change and click **Create** to save your new object. The screen will redraw to show the values set.
6. Click **return to object list** to return to the full list of API objects.
7. Using the **Filter** input box, type **ldapMappings** to filter the list view. Locate the required row from the resulting list of API objects and tap the ► after **/api/v1/ldapMappings**
8. Click **Create new** to configure a new ldapMappings object.
9. Configure the **Field Mapping Expressions**. These values can be customized to your deployment. The simplified deployment recommendation is to use the user's existing email address for username (jidMapping) and to create spaces for all imported users.
 - jidMapping: **\$mail\$**
 - nameMapping: **\$cn\$**
 - coSpaceUriMapping: **\$sAMAccountName\$.space**
 - coSpaceNameMapping: **\$cn\$ space**
10. Make sure the checkbox is marked for each value you set or change and click **Create** to save your new object. The screen will redraw to show the values set.



11. Click **return to object list** to return to the full list of API objects.
12. Using the **Filter** input box, type **ldapSources** to filter the list view. Locate the required row from the resulting list of API objects and tap the ► after **/api/v1/ldapSources**
13. Click **Create new** to configure a new ldapSources object.
14. The **server** parameter must be set to the ID of the ldapServers object created in earlier steps. Click **Choose** next to an entry to display a selection helper window from which you can select the ID of existing objects, click **Select** for the entry of the ldapServer object created in the earlier steps of this task. The window will close and copy the ID to the text box automatically.
15. The **mapping** parameter must be set to the ID of the ldapMappings object created in earlier steps. Click **Choose** and in the new window, click **Select** for the entry of the ldapMappings object created in the earlier steps of this task. The window will close and copy the ID to the text box automatically.

- Configure the **baseDn** and **filter** parameters. These values define the search performed in the LDAP server when importing users. The example values below must be updated to match your environment. Contact your Domain Administrator if you need assistance on which values should be used for your environment:

baseDn: `cn=Users,dc=company,dc=com`

filter: `(&(sAMAccountType=805306368)(sAMAccountName=*)(mail=*))`

Note: You must change the **baseDN/Base** to your own domain names, however, you can use this **Filter** example as it appears here.

Note: If your directory has a large number of users (more than 10,000) or you do not want to enable all users, the Base distinguished name and Filter should be changed to target a more specific group or set of users. Importing a large number of users increases the time required to complete the LDAP sync.

Note: This example creates spaces for users that do not include a PIN and allow guest access. If you wish to deny access to these spaces by default, set **nonMemberAccess** to false in the **LdapSources** object

- Make sure the checkbox is marked for each value you set or change and click **Create** to save your new object. The screen will redraw to show the values set.

The screenshot shows the Cisco configuration interface for an LDAP source object. The top navigation bar includes 'Status', 'Configuration', and 'Logs'. Below the navigation bar, there is a breadcrumb trail: '/api/v1/ldapSources/1dc39985-7df9-416e-a2ad-acb231fcce5'. The 'Related objects' section shows a link to '/api/v1/ldapSources'. The 'Table view' and 'XML view' tabs are visible. The 'Object configuration' table lists the following parameters:

Object configuration	
server	8fa58ae4-7112-4ce2-89ab-dab10f3ec93a
mapping	857d5af8-b1e2-4450-a14d-a7b6384cb2ab
baseDn	cn=Users,dc=company,dc=com
filter	(&(sAMAccountType=805306368)(mail=*))
nonMemberAccess	true

Below the table, the configuration is shown in a form view. The parameters are listed with their values and a 'Choose' button next to each. The 'nonMemberAccess' parameter is set to 'true' and has a 'present' checkbox checked. The 'Modify' button is at the bottom.

The LDAP configuration for importing users is now complete and ready for an LDAP sync to be run.

Running the LDAP import

With the **LdapServer**, **LdapMapping**, and **LdapSource** objects created, the **Ldap import/sync** process must be ran to import users. The sync process should be re-run anytime you want user

changes in the LDAP server to be updated in Meeting Server.

1. Log in to the Meeting Server Web Admin interface and select **Configuration > Active Directory**:
2. Click **Sync Now** at the bottom of the page. **Sync Now** can still be used even though the configuration on this page is not used. LDAP Syncs can also be initiated by creating an `/api/v1/ldapSyncs` object in the API.

After a minute or two, go to **Status > Users** which should display the users created by the LDAP import. The **Configuration > Spaces** page should display the spaces that were created for the imported users.

If the user list is empty, go to **Logs > Event Log** and locate the entries starting with **LDAP sync operation**. Any errors about attributes missing or duplicate entries means your Field Mappings or search criteria needs adjusting to avoid errors. If needed, you can use **Configuration > API** to modify any of the values you previously setup, then repeat the LDAP sync.

For further tips and examples around the LDAP Import settings, see [LDAP Tips and Examples](#).

Confirm Web Bridge 3 logins

1. To verify your Web Bridge and LDAP deployment, go to the Meeting Server's web interface <https://meetingserver.company.com> using a supported WebRTC App browser.

The welcome screen should display with **Sign In** and **Join Meeting** buttons.

2. Click **Sign In** and log in using a username that was included in the LDAP import. The password is the user's password from the LDAP directory.

Ensure you enter the username as imported. If you are unsure of the format, log into the Web Admin interface, go to **Status > Users**; the username for each user is shown in the **XMPP ID** column for each user.

3. Once logged in successfully, the web app loads and the user can join their existing space, and have other participants dial into the space.
4. If you are not able to see the **Sign In/Join** buttons or otherwise not able to log in, use the **Logs > Event Log** page to look for details on the failure.

Task 18: Configuring space templates

CoSpace templates are used to define the kind of spaces users can create in the Meeting Server web app. This functionality is specific to Web bridge 3 and does not apply to Web Bridge 2/Meeting App scenarios.

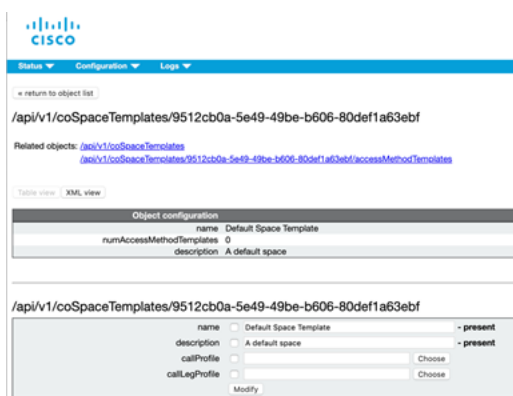
This configuration is optional, but without it, users logged into web app can use existing spaces, but not create new spaces. This task is not applicable to your deployment if you did not complete Task 17 to import users.

Note: Completing this task requires use of the Meeting Server API. We recommend that you use the Cisco Meeting Server Installation Assistant to configure your deployment if you are not comfortable with API tasks. Alternatively, you can complete this setup by deploying Cisco Meeting Management and using its user provisioning features.

This simplified deployment example will create the minimal Space Template intended just to enable users to create their own spaces. It will define labels and a default URI format for the space, but nothing more. The template will be applied to all imported users.

Create Space Template

1. Log in to the Meeting Server Web Admin interface and select **Configuration > API**.
2. Using the **Filter** input box, type **coSpaceTemplates** to filter the list view. Locate the required row from the resulting list of API objects and tap the ► after **/api/v1/coSpaceTemplates**
3. Click **Create new** to configure a new coSpaceTemplates object.
4. Fill in the name and description fields. These fields can be customized to your preference. Suggested values for the simplified deployment are:
 - **name:** Default Space Template
 - **description:** A default space
5. Make sure the checkbox is marked for each value you set or change and click **Create** to save your new object. The screen will redraw to show the values set.



6. Under **Related Objects**, click the long hyperlink for accessMethodTemplates (as seen in figure above) to access the accessMethodTemplates for the newly created space template. As none exist yet, clicking the link will take you directly to the page to create a

new accessMethodTemplate.

7. Fill in the name and uriGenerator fields. These fields can be customized to your preference. Suggested values for the simplified deployment are:
 - **name:** Default Access Method
 - **uriGenerator:** \$.space
8. Make sure the checkbox is marked for each value you set or change and click **Create** to save your new object. The screen will redraw to show the values set.

The Space Template is now defined but must be linked to a LDAP Source via a ldapUserCoSpaceTemplateSources object to be applied to users.

Link Space Template to a LDAP Source

1. Log in to the Meeting Server Web Admin interface and select **Configuration > API**.
2. Using the **Filter** input box, type **ldapUser** to filter the list view. Locate the required row from the resulting list of API objects and tap the ► after **/api/v1/ldapUserCoSpaceTemplateSources**
3. Click **Create new** to configure a new ldapUserCoSpaceTemplateSources object.
4. The CoSpaceTemplate parameter must be set to the ID of the Space Template object created in prior steps. Click **Choose** next to the parameter field and in the new window click **Select** for the entry of the CoSpaceTemplate object created in the earlier steps of this task. The window will close and copy the ID to the text box automatically.
5. The ldapSource parameter must be set to the ID of the ldapSource object created in Task 17. Click **Choose** next to the parameter field and in the new window click **Select** for the entry of the ldapSource object created Task 17. The window will close and copy the ID to the text box automatically.
6. Make sure the checkbox is marked for each value you set or change and click **Create** to save your new object. The screen will redraw to show the values set.

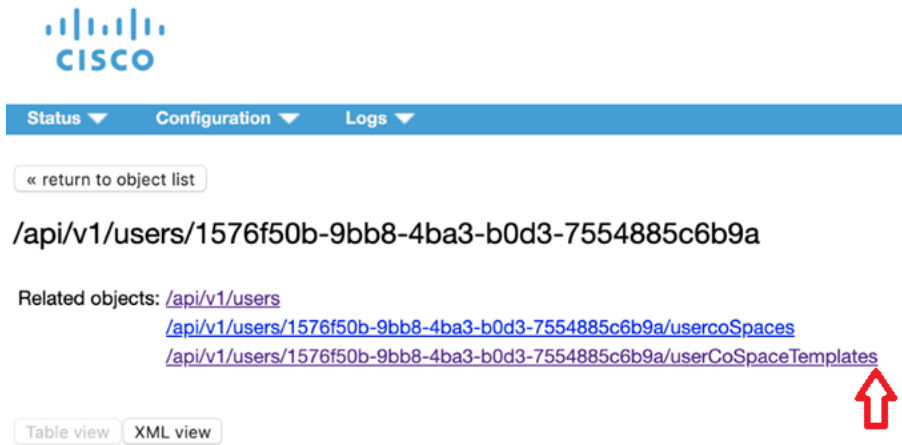
This configuration is complete, but the changes will not apply to users until a LDAP sync is performed.

7. Log in to the Meeting Server Web Admin interface and select **Configuration > Active Directory**. Click **Sync now** at the bottom of the page.

After the sync completes, you can confirm the template has been applied to users by reviewing their **/api/v1/users** object in the API object viewer.

1. Log in to the Meeting Server Web Admin interface and select **Configuration > API**.
2. Using the **Filter** input box, type **users** to filter the list view. Locate the required row from the resulting list of API objects and tap the ► after **/api/v1/users**

- Click on the hyperlink of any of the users to view the object's details. Under **Related objects**, if the linking was successful the user should have a line for coSpaceTemplates.



Users who have Space Templates linked to their user record will now have a **Create Space** button when logged into the web app page.

Finish Installation

With all of the previous tasks done, the Meeting Server installation is now completed and ready for use. If you wish to enable the ActiveControl permissions as offered in the Installation Assistant, see the steps in [Appendix C](#).

Consider deploying Cisco Meeting Manager to enhance your Meeting Server deployment with operator controls, licensing monitoring and space template configuration.

Appendix A Additional information

A.1 Firewall ports information

Open the appropriate Firewall ports, for example: TCP 445, TCP 80, TCP 443, TCP 5222, TCP 5061, UDP 3478, UDP 32768-65535, TCP 32768-65535.

See Appendix B of [Cisco Meeting Server x.x, Single Combined Server Deployment Guide](#) for all port information.

A.2 Adding firewall traversal and external networks

SIP and Lync calls can traverse local firewalls using the Cisco Expressway, you will need to configure trust between the Call Bridge and the Cisco Expressway. For more information, see "Cisco Meeting Server with Cisco Expressway Deployment Guide".

Go to: <https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>

A.3 Microsoft deployment information

For an example deployment, see: "Cisco Meeting Server clustered with on-premises Microsoft Lync or Skype for Business"

For more information on Microsoft deployments, see "Cisco Meeting Server with Cisco Expressway Deployment Guide"

Go to: <https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html>

Appendix B LDAP Tips and Examples

B.1 Tips on Meeting Server LDAP Mappings

Important points to note regarding LDAP mappings Cisco Meeting Server:

- Case sensitivity: the LDAP attribute names are case sensitive. For example, when using `cn` or `$sAMAccountName$`
- **Username:** Required field. All *resulting* user names as imported must be unique (includes the full string)—any duplicates (or empty values) will cause the import to be aborted.
- **Space name:** Optional field. Does not require uniqueness.
- **Space URI user part:** Optional field. All *resulting* space URIs must be unique within the tenant (in spaces and user JIDs).
- **Space secondary URI user part:** Optional field. All *resulting* space URIs must be unique within the tenant (in spaces and user JIDs).
- **Space Call ID:** Optional field. All *resulting* Call IDs must be unique

B.2 Tips on LDAP

- To find the LDAP path or Domain Name of a specific user or location, use the **Users & Computers** Snap In on Windows, navigate to the object, and select **Properties**. Select the **Attribute Editor** tab, and find the attribute you want to look up in the list.
- Missing attributes on a user can cause an import to abort, so it is always good practice to put the attributes you depend on in the ldap filter so objects without those attributes are excluded.
- If using Active Directory, using the filter `(sAMAccountType=805306368)` automatically limits your search to just user objects and reduces load on the AD server.
- Filter example to import members of a security group recursively, use a filter such as:
`(&(objectclass=person
(memberof:1.2.840.113556.1.4.1941:=cn=groupName,cn=Users,dc=company,dc=com))`
- Filter example to exclude a specific user, use a filter such as:
`(&(sAMAccountType=805306368)(sAMAccountName=*)(!(cn=Joe Smith)))`
- Regex example to take the left side of the email address (portion before the @) and append it to your domain, for example:
`$mail|' /\@.* //' '$@meet.company.com`

Example 1: Import all Active Directory Users, set JID based on sAMAccountName, and create a space

- Display Name: `cn`
- User name: `$mail$`
- space Name: `cn space`
- space URI user part: `cn.space`
- space Secondary URI user part: [leave blank]
- space call id: [leave blank]
- Use LDAP base: `cn=Users,dc=company,dc=com`
- Use LDAP filter: `(&(sAMAccountName=*)(mail=*)(sAMAccountType=805306368))`

Example 2: Import all users that are members of a specific Active Directory group, `cn=CMSAdmins,cn=Users,dc=company,dc=com` and create spaces for each

- User name: `$mail$`
- space Name: `cn space`
- space URI user part: `cn.space`
- space Secondary URI user part: (leave blank)
- space call id: (leave blank)
- Use LDAP base: `cn=Users,dc=company,dc=com`
- Use LDAP filter: `(sAMAccountType=805306368)`
`(memberOf:1.2.840.113556.1.4.1941:=cn=CMSAdmins,cn=Users,dc=company,dc=com)`

B.3 Common user LDAP filters

To import users that belong to a specific group, you can filter on the `memberOf` attribute. For example:

```
memberOf=cn=apac,cn=Users,dc=Example,dc=com
```

This imports both groups and people that are members of the APAC group.

To restrict to people (and omit groups), use:

```
(&(memberOf=cn=apac,cn=Users,dc=Example,dc=com)(objectClass=person))
```

Using an extensible matching rule (`LDAP_MATCHING_RULE_IN_CHAIN / 1.2.840.113556.1.4.1941`), it is possible to filter on membership of any group in a membership hierarchy (below the specified group); for example:

```
(&(memberOf:1.2.840.113556.1.4.1941:=cn=apac,cn=Users,dc=Example,dc=com)(objectClass=person))
```

Other good examples which you can adapt to your LDAP setup include:

Filter that adds all Person and User except the ones defined with a !

```
(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))(!(cn=Guest))(!(cn=krbtgt)))
```

Filter that adds same as above (minus krbtgt user) and only adds if they have a sAMAccountName

```
(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))(!(cn=Guest))(sAMAccountName=*))
```

Filter that adds same as above (Including krbtgt user) and only adds if they have a sAMAccountName

```
(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))(!(cn=Guest))(!(cn=krbtgt))(sAMAccountName=*))
```

This filter only imports specified users within (|) tree

```
(&(objectCategory=person)(objectClass=user)(|(cn=accountname)(cn=anotheraccountname)))
```

Global Catalog query to import only members of specified security group (signified with =cn=xxxxx)

```
(&(memberOf:1.2.840.113556.1.4.1941:=cn=groupname,cn=Users,dc=example,dc=com)(objectClass=person))
```

Appendix C ActiveControls CallLeg Profiles

C.1 Purpose

The Cisco Meeting Server has a ‘default off’ security posture for services and user permissions. This means that unless explicitly configured for the meeting or user, advertised features or abilities may not be available.

As part of the Cisco Meeting Server Installation Assistant, there is the option to enable a set of commonly used permissions to enable the ActiveControl feature set for Cisco devices. This section shows how to add the same configuration to a deployment configured using the manual simplified deployment in this guide.

C.1.1 Settings Included

The settings suggested to be included are part of Meeting Server’s CallLegProfiles and are:

- **muteOthersAllowed** enabled
- **disconnectOthersAllowed** enabled
- **changeLayoutAllowed** enabled
- **callLockAllowed** enabled
- **setImportanceAllowed** enabled
- **recordingControlAllowed** enabled
- **streamingControlAllowed** enabled
- **addParticipantAllowed** enabled

Enabling the full set of ActiveControls for supported devices as the system default is achieved by creating a CallLegProfile with the above settings enabled, and then setting the profile as a System profile.

C.2 Configuration

1. Log in to the Meeting Server Web Admin interface and select **Configuration > API**:
2. From the list of API objects, tap the ► after **/api/v1/system/profiles**
3. Under **Object configuration** there should be an entry for **callLegProfile** – Click on the ID/Link to open that existing callLegProfile object and skip to [Step 6](#). If no callLegProfile is listed, continue to the next step.

Note: If you followed all previous tasks in this simplified deployment guide, you would have created a CallLegProfile seen here under System Profiles which includes settings such as sipMediaEncryption. Your changes here will be merged with those existing settings.

4. From the list of API objects, tap the ► after `/api/v1/callLegProfiles`
5. Click **Create new** to configure a new callLegProfile object.
6. A new page displays with all the available parameters – use the drop-down menus to set the following parameters to **true**. (Editing an entry automatically checks the checkbox for the entry to indicate it as set or changed.)
 - disconnectOthersAllowed
 - addParticipantAllowed
 - muteOthersAllowed
 - changeLayoutAllowed
 - callLockAllowed
 - setImportanceAllowed
 - recordingControlAllowed
 - streamingControlAllowed

Note: If you followed all previous tasks in this simplified deployment guide, there will be settings already listed at the top of the page under **Object Configuration**. Your changes will be merged with those existing settings.

7. Click **Modify** at the bottom of the list to save your new profile (Or **Create** if no existing profile was used). The resulting page will show a summary of the settings enabled.

CISCO

Status Configuration Logs

◀ return to object list

/api/v1/callLegProfiles/7b3857b1-da5e-47bc-8229-4cc16098976a

Related objects: /api/v1/callLegProfiles
/api/v1/callLegProfiles/7b3857b1-da5e-47bc-8229-4cc16098976a/usage

Table view XML view

Object configuration	
sipMediaEncryption	optional
muteOthersAllowed	true
disconnectOthersAllowed	true
telepresenceCallsAllowed	false
sipPresentationChannelEnabled	true
changeLayoutAllowed	true
bfcMode	serverOnly
callLockAllowed	true
setImportanceAllowed	true
recordingControlAllowed	true
streamingControlAllowed	true
addParticipantAllowed	true

Write this object to "/api/v1/system/profiles"

8. Click **Write this object to “/api/v1/system/profiles”** at the bottom of the page to save this profile as the system default. The page will refresh to show the system profiles with the CallLegProfile parameter updated to the ID of the profile that you have edited.

This completes the configuration and the changes will take effect immediately.

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.

© 2018–2020 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL:

www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)