Cisco Meeting Server

Single Server Simplified Setup Guide

October 26, 2018

Cisco Systems, Inc. www.cisco.com

What's new

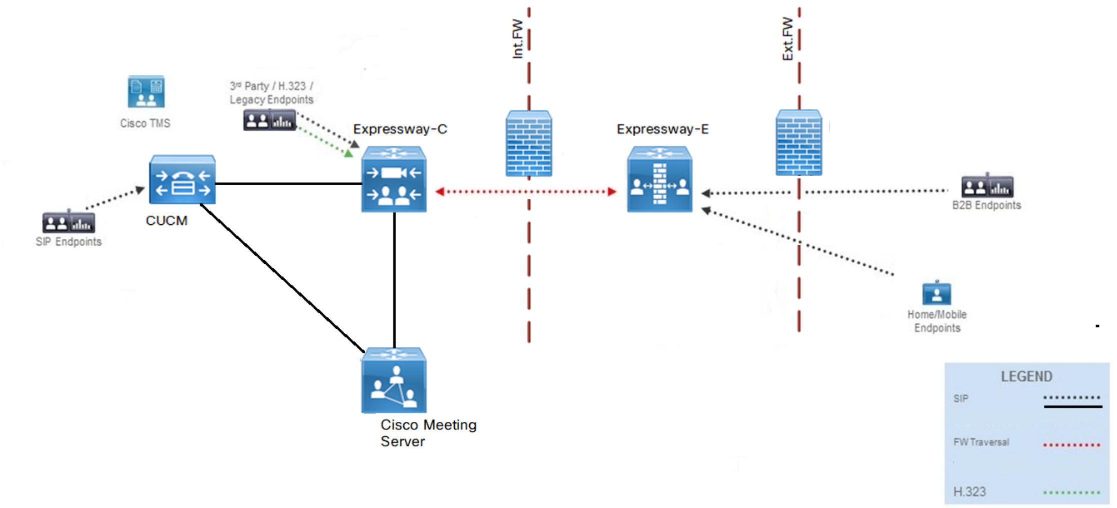
Version	Change
October 25, 2018	First version published.

Contents

1 Introduction

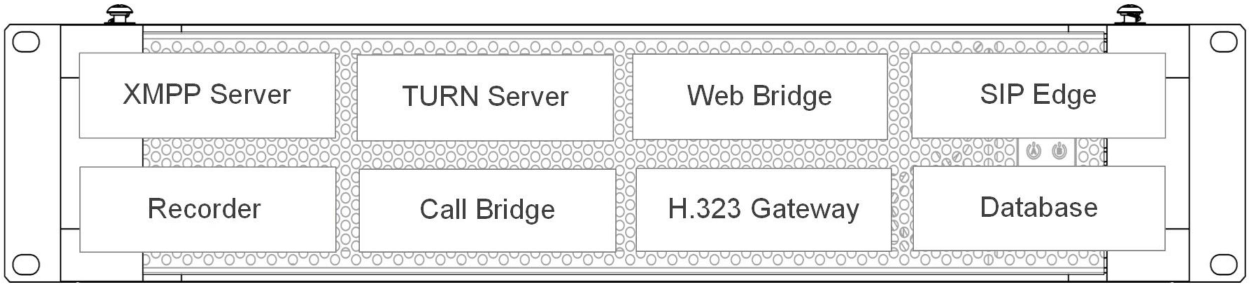
This guide covers a simplified deployment of Meeting Server intended to reduce the time and complexity needed to complete a basic stand-alone installation. This deployment implements a stand-alone conference bridge integrated with Unified CM or Expressway/VCS call control as shown in Figure 1. It is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

Figure 1: Cisco Meeting Server simple deployment



Meeting Server has additional functionality that can be enabled for more advanced deployments, see Figure 2. This includes resilient design, recording, streaming, Microsoft Integration, and so on, but these are not part of this simplified deployment. 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, Web Bridge, and XMPP services.

Figure 2: Meeting Server components



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, we recommend that the following requirements are in place:

- DNS A record should be created for the Meeting Server IP address using an alias you want end-users to be comfortable with; for example: **`meetingserver.company.com`**
- XMPP Domain name should be chosen. This is the domain name user will use to log in for Cisco Meeting App. These configuration tasks assume using the company's top level domain to allow using existing email addresses for XMPP login. If another application has already claimed this name for XMPP, you must use a different domain name, such as a subdomain, for example: **`meet.company.com`**
- To support Cisco Meeting App users, a DNS SRV record for XMPP domain name must be added to your DNS server. An SRV record for **`_xmpp-client._tcp.<xmpp domain>`** for TCP port 5222 is needed. Note: You do not need to do this if you are only using Meeting App for WebRTC.
- SIP Domain for Meeting Server; we suggest using a subdomain, such as **`meet.company.com`**

2.1.1 Software Versions

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

- Meeting Server 2.3 or 2.4
- Cisco Unified CM 10.5.2, 11.0, 11.5, 12.0
- Expressway X8.10 or X8.11

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 the virtual console for the machine.
2. When the initial power on is complete, the Meeting Server login prompt displays.
3. Log in with the user name “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`** command e.g. to display the current configuration on the " a" interface, in the MMP type:

   ```
   iface a
   ```

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

```
iface a 1000 full
```

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

```
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, 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
      ```

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
```

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. To set the hostname, use the command: `hostname <name>`, for example:

   ```
   hostname meetingserver
   ```

3. Type:

   ```
   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 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 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

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

   ```
   version
   ```

2. Before upgrading your Meeting Servers:
   a. take a backup of the current configuration on each of the servers. Use the MMP command **`backup snapshot <name>`**. Save the backup safely to a local server. See the MMP Command Reference guide for full details. Do NOT use the automatic backup file that is created during the upgrade process.

   b. save the cms.lic and certificate files to the local server.

   c. using the Web Admin interface, check the database cluster status, and that all calls (SIP and clients) are working and no fault conditions are listed.

3. To upgrade, first download and extract the appropriate software file from the Cisco website. Click on this link, then click on the appropriate Meeting Server type listed in the right-hand column of the web page and follow any instructions displayed with the download link.
4. 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.x.y is an IP address or domain name.

5. Then to complete the upgrade, connect via SSH to the MMP and type:

   ```
   upgrade
   ```

   Allow several minutes for the server to restart.

6. To verify that the upgrade was successful, SSH into the MMP, log in and type the following command:

   ```
   version
   ```

Task 5: Obtaining and assigning Multiparty licenses

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.

Note: For detailed information on different Meeting Server licensing models, see the Cisco Licensing chapter in the larger deployment guides.

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 following command: **`iface a`**

   Note: This is the MAC address of your VM (i.e. Meeting Server), not the MAC address of the server platform that the VM is installed on (i.e. host server).

   ---

2. Open the Cisco License Registration Portal and register the PAK code and the MAC address of your Meeting Server.
3. The license portal will provide a zipped copy of the license file. Extract the zip file and rename the resulting .lic file to **`cms.lic`**.
4. Using your SFTP client, log into Meeting Server and copy the **`cms.lic`** file to the Meeting Server file system.
5. Restart the Call Bridge using the command **`callbridge restart`**
6. After restarting the Call Bridge, the license status can be checked by typing **`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. SSH into the MMP and log in.

2. To 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, type `ntp status`

See the MMP Command Reference for a full list of `ntp` commands.

Task 7: Generating certificate for Meeting Server

Meeting Server uses x.509 certificates to configure secure (TLS) connections in its services and for some authentication tasks. In this deployment, certificate configuration is required for the Call Bridge, XMPP, 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 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 have the XMPP domain in the Subject Alternate Name (SAN) attribute of the certificate. To generate a Certificate Signing Request (CSR) and private key locally:

1. Log in to the MMP using SSH or console.
2. Type 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 subjectAltName: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 local 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.

   The output from your signing certificate authority should be a PEM encoded certificate file (for example, **`singleCert.crt`**). You will also need a PEM encoded bundle (consisting of root certificate, or intermediate certificates and a root certificate) of the chain of certificate authorities that signed your certificate (for example, **`ca-bundle.crt`**). Your certificate authority may return files to you in a different format, which usually can be repackaged or reformatted with common certificate tools. See the Certificate Guidelines for more information.

4. Upload this PEM encoded bundle (for example: **`ca-bundle.crt`**) to Meeting Server. Using your SFTP client, log into Meeting Server and copy the signed certificate file and certificate authority bundle to the Meeting Server file system.

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

   Note: If you self-sign a certificate, and use it, you may see a warning message that the service is untrusted. To avoid these messages, re-issue the certificate and have it signed by a trusted CA; this can be an internal CA unless you want public access to this component.

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. 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.

2. Configure the Call Bridge to use the certificate, key, and bundle generated in Task 7, using **`callbridge certs <keyfile> <certificatefile> <ca bundle>`**, for example:

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

3. Restart the Call Bridge interface 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 and the Call Bridge service. 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 the Web Bridge for conference users and would like 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 Task 7, 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**).

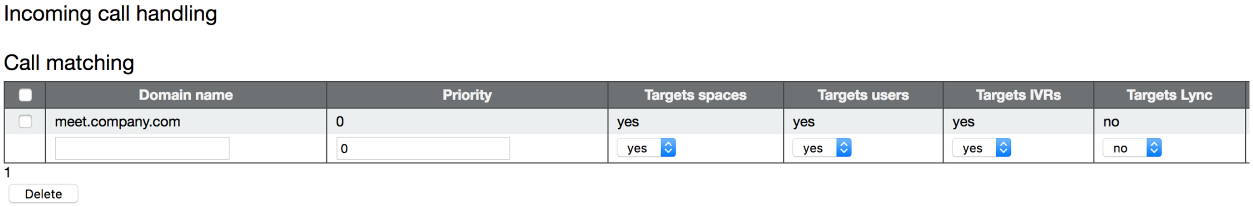
The **SIP media encryption** setting must be compatible with your existing call control and endpoints. The setting recommended for most usages is **allowed** – this allows both encrypted and non-encrypted connections. Take care before setting to **required** if you want to specify encryption is required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

3. On the same page, you can optionally:
    - Choose to enable **SIP call participant labels** if you want site 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.
3. 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 matches incoming calls by checking the value after the " @" symbol with the values in the domain column.

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



Incoming call handling

Call matching

□	Domain name	Priority	Targets spaces	Targets users	Targets IVRs	Targets Lync
□	meet.company.com	0	yes	yes	yes	no
		0	yes	yes	yes	no

1

Delete

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 matches a space is used to form the URI in the invitations created by Cisco Meeting App. It is expected that the highest priority rules are for the deployment as a whole, rather than for individual IP addesses or hostnames.

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**: test

- **Secondary URI**: 881000
- **CallID**: 881000

For secondary URI, use an E.164 value that will be compatible with the dial plan you will be routing to Meeting Server. For CallID, the value can be any number not already in use, in this example, for simplicity, it is set to the same value as the secondary URI.

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**
    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 New** 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 CMS 1*>
- **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** 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 conference 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 2.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 Cisco Unified Communications Manager depending on the number of simultaneous calls.

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

   Note: 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 Cisco Unified Communications Manager **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 Cisco Unified Communications Manager 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 Cisco Unified Communications Manager, 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)
Device pool	The pool you want your device to belong to (as configured in **System > Device Pool** in Cisco Unified Communications Manager
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 Cisco Unified Communications Manager 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 CUCM nodes as well.

6. Click **Save** and apply the configuration.
7. Use the **Trunk List** to confirm that the trunk goes into service after a few minutes.

Configure route patterns (dial plans for outbound calls)

You can configure domain based routing e.g. meet.company.com, and/or number based routing e.g. 88XXXX, to the Meeting Server through the Cisco Unified Communications Manager interface.

Domain based routing example

To route all domain based calls from Cisco Unified Communications Manager to the Meeting Server:

1. Go to **Call Routing** > **Sip Route Pattern**.
2. If none are appropriate, click **Add New**.
3. Complete the following:
    - **Pattern Usage** = Domain Routing
    - **IPv4 pattern** = for example, **meet.company.com**
    - **Description** = anything you want
    - **Route Partition** = the route partition you want this rule to belong to

    Note: Various dial plan rules are attached to a route partition and a Calling Search Space (CSS) comprises a list of route partitions. You can have a different CSS for different people, each phone, or trunk. When a call is made, Cisco Unified Communications Manager goes through each route partition in the CSS until it finds one that has a matching rule.

    - **SIP Trunk / Route List** = the trunk you have already configured.
4. Click **Save**.

Numeric dialing example

This basic example routes 6 digit numbers that start with 88. This example should be modified to match your target dial plan.

1. Go to **Call Routing** > **Route/Hunt** > **Route Pattern**. A list of existing Route Patterns is displayed.
2. If none are appropriate, click **Add New**.
3. Complete the following:
   - **Route pattern** = 88XXXX (Further down the page you can set various transforms, if desired)
   - **Route partition** = the route partition you want this rule to belong to

     Note: : Various dial plan rules are attached to a route partition and a Calling Search Space (CSS) comprises a list of route partitions. You can have a different CSS for different people, each phone, or trunk. When a call is made, Cisco Unified Communications Manager goes through each route partition in the CSS until it finds one that has a matching rule.

   - **Description** = any appropriate text
   - From the **Gateway/Route List** drop-down, select the SIP trunk created in the previous steps
4. Click **Save**.
5. Now call control is configured, you can dial into the Meeting Server test conference 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 2.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

To support the Web Bridge functionality, the XMPP service must also be deployed. This task has 3 steps: enable XMPP service, configure it to work with Call Bridge, and then enable Web Bridge.

Enable XMPP service

1. Establish an SSH connection to the MMP and log in.
2. To configure the XMPP server to use the " a" interface, use the MMP command `xmpp listen <interface whitelist>`

   For example:

   ```
   xmpp listen a
   ```
3. Assign the certificate and private key files that were generated earlier in Task 7, using the command:

   ```
   xmpp certs <keyfile> <certfile> <ca bundle>
   ```

   For example:

   ```
   xmpp certs singleCert.key singleCert.crt ca-bundle.crt
   ```
4. Define the XMPP domain for the deployment with the command `xmpp domain <domain name>`

   For example, where the domain name is company.com:

   ```
   xmpp domain company.com
   ```
5. Enable the XMPP service with the following command:

   ```
   xmpp enable
   ```

   The server should respond with SUCCESS messages if completed successfully.

Add Call Bridge to XMPP Server

The Call Bridge requires a set of credentials to connect to the XMPP server. These credentials are created in the XMPP server and subsequently added to the Call Bridge configuration.

1. Log in to the MMP using SSH or console.
2. Provide a component name for the Call Bridge to use to authenticate, for example. `cb_1` using the MMP command `xmpp callbridge add <component name>`.

   For example

   ```
   xmpp callbridge add cb_1
   ```
3. A secret is generated; for example, you see:

   ```
   cms>xmpp callbridge add cb_1
   Added callbridge: Secret: aB45d98asdf9gabgAb1
   ```

Make a note of the domain, component name and secret generated because they are required when you use the Web Admin interface to configure the Call Bridge access to the XMPP server in Task 16.

Note: If you lose the details, use the MMP command **`xmpp callbridge list`** to display them.

Enable Web Bridge on Interface A

1. Log in to the MMP using SSH or console.
2. Configure the Web Bridge to listen on interface " a" on port 443:

   ```
   webbridge listen <interface[:port]
   ```

   For example:

   ```
   webbridge listen a:443
   ```

3. Configure Web Bridge service with the certificate files generated in Task 7 using the MMP command **`webbridge certs <keyfile> <certfile> <ca bundle>`**, for example:

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

4. The Web Bridge supports HTTPS. It will forward HTTP to HTTPS if configured to use “http-redirect”. To enable HTTP redirect use the following command:

   ```
   webbridge http-redirect enable
   ```

5. For Call Bridge to instruct Web Bridge to trust connections from the Call Bridge, use the MMP command **`webbridge trust <certfile>`** with the combined certificate used earlier. For example:

   ```
   webbridge trust singleCert.crt
   ```

7. Enable the Web Bridge service with the following command:

   ```
   webbridge enable
   ```

   The server should respond with SUCCESS messages if completed properly

Configure Call Bridge to register with the XMPP service

With the XMPP service now running, configure Call Bridge to register with the XMPP service.

The deployment requires the _xmpp-client SRV record be created for your XMPP domain. To support use of Cisco Meeting App for Desktop and iOS, this DNS record must be created in your DNS servers as outlined in the Prerequisites. If not supporting Cisco Meeting App for Desktop and iOS, and only using Cisco Meeting App for WebRTC, this requirement can be replaced by using a local DNS RR record on Meeting Server itself. Do not create this DNS RR record if you create the SRV record in your normal DNS servers.

To create a local DNS RR record:

1. Log into the MMP console using SSH and admin credentials.
2. Create the DNS RR record for the XMPP domain using the following example(ensure you use names to match your deployment):

   ```
   dns add rr "_xmpp-client._tcp.<xmpp domain>. 86400 IN SRV 0 5 5222 <CMS
   FQDN>."
   ```

   For example, if the Meeting Server FQDN is `meetingserver.company.com` and XMPP domain is `company.com`, enter:

   ```
   dns add rr "_xmpp-client._tcp.company.com. 86400 IN SRV 0 5 5222
   meetingserver.company.com."
   ```

   Note: The use of periods " ." at the end of the addresses are required.

3. Clear the DNS cache of the Meeting Server so the new record will be used. In the MMP console, enter the dns flush command: `dns flush`

If you need to remove a local DNS RR record, use the command: `dns del rr _xmpp-client._tcp.<xmpp domain> <type>`, for example: `dns del _xmpp-client._tcp.company.com. srv`

The DNS record can be tested using the MMP commands.

1. Flush the existing DNS cache, enter: `dns flush`.
2. Enter `dns lookup` command on the SRV record created:

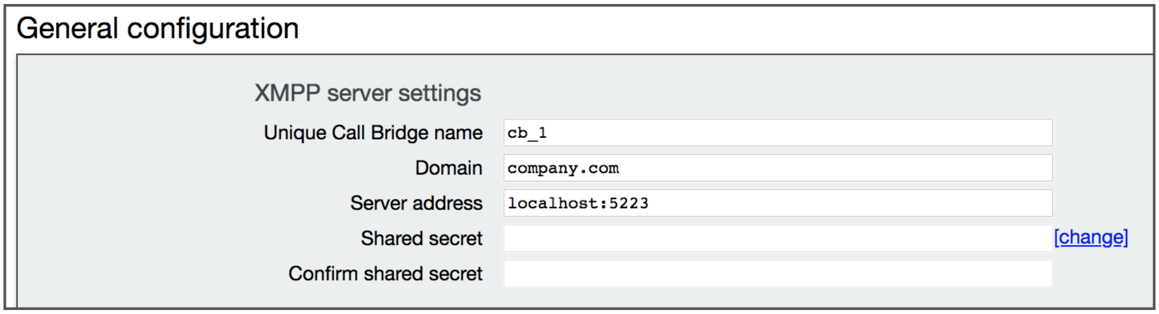
   ```
   dns lookup srv _xmpp-client._tcp.company.com
   ```

The result should point to the FQDN of the Meeting Server and resolve to the Meeting Server's IP address.

Configure XMPP Server settings via Web Admin Interface

1. Log in to the Web Admin Interface and configure the XMPP server settings as follows:

   a. Go to **Configuration > General**



General configuration

XMPP server settings

Unique Call Bridge name	cb_1
Domain	company.com
Server address	localhost:5223
Shared secret	[change]
Confirm shared secret	

   b. Complete the fields in the XMPP Server Settings section.

- **Unique Call Bridge name** (this is the component name set up previously, no domain part is required, as shown):

  `cb_1`

- **Domain** (this is the XMPP server domain set up previously):

  `company.com`

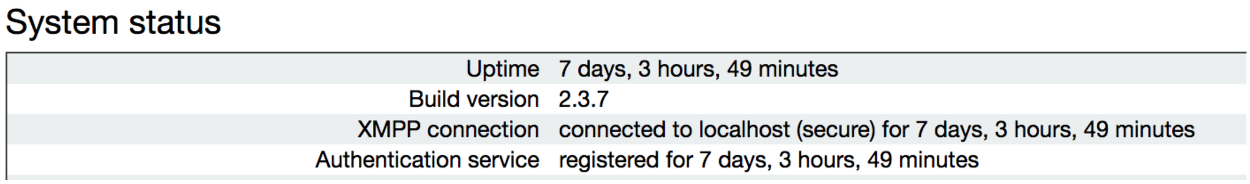
- **Server Address** is the IP address or hostname of the XMPP server, with an optional <port> (default is 5223):

  `localhost:5223`

- **Shared secret**: as generated during the XMPP server configuration. Click **Change link** to edit the password fields.

c. Click **Submit** to save your configuration.

5. Go to **Status > General** and verify the server connection.
   You should see details similar to the following in the **XMPP Connection** field:



System status

Uptime	7 days, 3 hours, 49 minutes
Build version	2.3.7
XMPP connection	connected to localhost (secure) for 7 days, 3 hours, 49 minutes
Authentication service	registered for 7 days, 3 hours, 49 minutes

Configuring Web Bridge for Call Bridge

To enable Guest access to the Web Bridge, the Call Bridge must be configured to locate the Web Bridge.

1. Log in to the Web Admin Interface using your browser and go to **Configuration > General**.
2. Set **Guest Account Client URI** to the HTTPS URL for your Meeting Server. For example: `https://meetingserver.company.com`
3. Set **Guest Account JID domain** to your XMPP domain. For example: `company.com`
4. Set the Web Bridge URI – go to **External Access** and enter 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 invites to invited users.

5. Click **Submit** to save your changes.
6. Confirm the Call Bridge is not reporting errors for the Web Bridge – go to **Status > General** and check that there are no alarms in the **Fault conditions** panel.

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

1. Using a browser (supported by Cisco Meeting App for WebRTC), 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 Task 13. 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

Importing users from an LDAP directory allows conference participants to log into Cisco Meeting App using their own account to manage their spaces and join meetings. Participants can also join meetings as 'guest' users, however, guest users cannot manage meetings or create/manage spaces.

Note: This task does **not** need to be completed if you only wish to enable Guest access.

The LDAP import in Meeting Server allows you to specify which users to target from an existing directory, and the values to use for the resulting accounts. The import also optionally supports creating a personal space for each imported user. Which users and specific values to import is a deployment-specific decision.

As an example configuration, we will import all users from Active Directory, set their login that they will use for Meeting App, and create a space for each user.

LDAP Settings description

- **LDAP Server Location/Port**: network location of the LDAP Server
- **LDAP Username/Password**: credentials used to connect to the LDAP server. Uses LDAP DN syntax
- **Base Distinguished Name**: 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 values that the administrator defines. The Mappings can use regex expressions and LDAP property names to construct transformations of the imported LDAP values. The Field Mappings used are:

- **Display Name**: Name shown for the user in user searches and directories
- **Username**: XMPP JID the user will login with – must result in the format of ***`<value>@<xmpp domain>`*** and the result must be unique

- **Space Name**: Label given to the auto-generated space for that user
- **Space URI user part**: Defines the user portion of the URI for the auto-generated space for that user – result must be unique
- **Space secondary URI user part**: Defines a secondary URI for the auto-generated space for the user (optional) – result must be unique
- **Space call ID**: 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

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

2.1.2 Configuring LDAP Import

These steps are required if you want users to log into the Web Bridge to use the Cisco Meeting App for WebRTC.

1. Log into the Web Admin interface of Meeting Server with your administrator account.
2. Go to **Configuration > Active Directory**

   Configure the **Active Directory Server Settings** 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.
3. Configure the **Active Directory Server Settings** values. Example values below must be updated to match your environment.
   - **Address**: *pdc1.company.com*
   - **Port**: 636
   - **Secure Connection**: Mark Checkbox
   - **Username**: *john.doe@company.com*
   - **Password**: <*Password for supplied user*>

   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
4. Configure the **Import Settings**. Example values below must be updated to match your environment.

- **Base distinguished name**: `cn=Users,dc=company,dc=com`
- **Filter**: `(&(sAMAccountType=805306368)(sAMAccountName=*)(mail=*))`

Note: Change the **Base distinguished name** 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 than10,000) 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.

5. Configure the **Field Mapping Expressions**. The Username example must be edited to match your configured XMPP domain.
   - **Display Name**: `$cn$`
   - **User name**: `$sAMAccountName$@company.com`
   - **Space Name**: `$cn$ space`
   - **Space URI user part**: `$sAMAccountName$.space`
   - **Space Secondary URI user part**: [leave blank]
   - **Space call id**: [leave blank]
6. Click **Submit** to save the changes.
7. Click **Sync Now** to start the LDAP import.

   After a minute or two, go to **Status > Users** which should display the users created by the LDAP import. And **Configuration > Spaces** 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. Go to **Configuration > Active Directory** and modify your import settings and click **Sync Now** to retry the import.

   For further tips and examples around the LDAP Import settings, see " LDAP Tips and Examples" on page 35.

2.1.3 Confirm Web Bridge 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 as Guest** 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 format is shown in the **XMPP ID** column for each user.

3. Once logged in successfully, the WebRTC App will load and the user can open their existing space, dial out to remote participants, or have other participants dial into the space.

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 2.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. Cisco Expressway must be running X8.9 or later. For more information, see *Cisco Expressway Options with Cisco Meeting Server* and/or *Microsoft Infrastructure (Expressway X8.9.2)* or if running X8.10 see *Cisco Expressway Web Proxy for Cisco Meeting Server (X8.10)* and *Cisco Expressway Session Classification Deployment Guide (X8.10)*.

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

A.3 LDAP Tips and Examples

Important points to note:

- 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

A.3.1 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=co
  m))
  ```
- 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 XMPP domain, for example:
  `$mail|'/\@.*//'$@meet.company.com`

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

Example uses XMPP domain of company.com

- **Display Name**: `$cn$`
- **User name**: `$sAMAccountName$@company.com`
- **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=*)(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

Example uses XMPP domain of company.com

- User name: `$sAMAccountName$@company.com`
- 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))`

A.3.2 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))
```

A.4 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 Expressway Options with Cisco Meeting Server and/or Microsoft Infrastructure (Expressway X8.9.2) or if running X8.10 see Cisco Expressway Web Proxy for Cisco Meeting Server (X8.10) and Cisco Expressway Session Classification Deployment Guide (X8.10):

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

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 are considered un-Controlled copies and the original on-line version should be referred to for latest version.

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

Cisco Trademark