



Cisco Meeting Server

Installation Assistant 2.9

Installation and Configuration

May 27, 2020

Contents

- Change History 4
- Introduction 5
- Prerequisites 6
 - Client computer requirements 6
 - Cisco Meeting Server requirements 6
 - External Dependencies 7
- Installation 8
 - Installing the software 8
- Running the software 9
 - Running the utility 9
 - Closing the utility 9
 - Persistent file storage 9
- Configuring a Meeting Server using Installation Assistant 10
 - Staging 10
 - New Meeting Server Instances 10
 - Existing Meeting Server Instances 10
 - License File 11
 - Meeting Server DNS Entries 11
 - Configuring a server 11
 - After pushing the configuration 13
 - Running the tool multiple times 13
 - Troubleshooting 13
 - Closing Installation Assistant 13
 - Uninstalling the software 14
- Panel Reference 15
 - Certificate 15
 - CA Signed Certificate 15
 - Use Existing Certificate and Key 17
 - Self Signed Certificate 18
 - License 18
 - Uploading the license 18
 - Network 19

Deleting a DNS or NTP server	20
Call Bridge	20
Conferencing User	20
Customizing the LDAP Search and user mappings	22
Web Bridge	24
Security	24
Push Configuration	25
Cisco Legal Information	27
Cisco Trademark	28
2 Glossary	29

Change History

Table 1: Change History

Date	Change	Reason
May 27, 2020	Release of software	Version 2.9

Introduction

The Installation Assistant is a tool to simplify the creation of a simple Cisco Meeting Server installation for demonstrations, lab environments, or as the starting point for basic installations. The tool configures Meeting Server based on the best practice deployment described in the [Cisco Meeting Server Single Server Simplified Deployment guide](#). It is a standalone tool that uses a browser interface to collect information about your setup and then pushes that configuration to the server without you needing to use utilities to access the API, sFTP or the Meeting Server's command line interface.

Installation Assistant configures Meeting Server to be a SIP MCU capable of making and receiving calls and optionally enables the web based Cisco Meeting App. The app allows users to join meetings using just a browser.

Note: For Cisco Meeting App, guest access alone can be enabled or optionally imported LDAP users can also be enabled.

Installation Assistant is intended to be used on an empty, non-configured Meeting Server. It is not a management tool for Meeting Server, nor is it for re-configuring existing Meeting Server installations. The tool is built for configuring Meeting Server 2.9 virtual machines only. It is not for use with the X-series products or the Cisco Meeting Server 2000 platform.

Prerequisites

Client computer requirements

The Installation Assistant must be run on a computer separate from Meeting Server

Table 2: Software requirements for client computer

Operating System	Browser	Disk space	Remarks
Windows 10 Windows Server 2012/2016/2019	Edge, Chrome and Firefox	150 MB	Requires Microsoft C++ 2017/2019 Runtime Distributable installed. Download from Microsoft link, https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads . Windows 10 computers should have the C++ runtime engine already enabled and do not need a separate installation. If the Installation Assistant tool crashes at startup, check that the redistributable is available on the computer.
Apple OSX Mojave Apple OSX Catalina	Safari, Chrome and Firefox	150 MB	NA

In addition:

- The client computer should not have any services that would conflict with TCP port 8000 running locally,
- The client computer must be able to reach the Meeting Server to be configured over the network, using the following ports:
 - TCP 22
 - TCP 443
 - TCP Port to be configured for Webadmin (recommend 445)

Cisco Meeting Server requirements

- Meeting Server must be a Cisco Meeting Server 1000 or Virtual Machine instance. Installation Assistant is not compatible for use with Cisco Meeting Server 2000 or Acano platforms.
- Meeting Server must be running software 2.9.x (any maintenance release of 2.9). Newer or older versions are not supported for Installation Assistant 2.9.

- Meeting Server must be a default setup that has not yet been configured except for its network address and administrator account.

External Dependencies

To complete the installation tasks you will also need:

- Addresses for your network's DNS and NTP servers
- The address of the SIP Proxy you will use with Meeting Server
- The SIP domain picked out that you will use with Meeting Server
- The license file from Cisco or your Partner for your Meeting Server instance
- If configuring user imports, you will need the connection details to your network's LDAP directory including location, credentials, and LDAP user location details.
- If configuring the server with certificates (recommended) you should have a FQDN picked for the Meeting Server and defined in your DNS server records.
- If configuring the server with certificates (recommended) you will need to have your certificate request signed by your Certificate Authority of choice. The Installation Assistant can help generate the certificate request or you can use an existing certificate and key pair.

Installation

Installing the software

The Installation Assistant must be installed on a computer separate from the Meeting Server, and is used locally on that computer. See the "Client computer requirements" on page 6.

Windows Installation:

1. Download and extract the compressed version of the product that is InstallAssistant for your operating system to its own folder.

Apple OSX Installation:

1. Download the InstallAssistantOSX.dmg file to your computer. Double click InstallAssistantOSX.dmg to mount and open the disk image.
2. Drag the Cisco InstallAssistant-2.9 icon to your Applications folder.
3. In the Application folder, double click on InstallAssistant
Note: In Mac OS Catalina, gatekeeper will not allow to run the Installation Assistant app as it is not notarized.
4. Click on 'Security & Privacy' . In the 'Allow apps downloaded from' section, click 'Open Anyway'

Running the software

The Installation Assistant is a stand-alone utility using your web browser for its user interface. The software uses an application window where the software runs, and automatically opens your web browser to view the software's interface. (On Windows, this application window will be a terminal window).

Running the utility

Windows – Double click the 'server.exe' icon in the folder of extracted Installation Assistant files. The Installation Assistant tool opens a console window which runs the utility and automatically opens your default browser to <https://localhost:8000> to view the tool's interface

Apple OSX – Double click the Installation Assistant-2.9 icon in your Applications folder. The Installation Assistant will open an application window which runs the utility and automatically opens your default browser to <https://localhost:8000> to view the tool's interface

Note: Starting with the Catalina (10.15.3) operating system version, opening the application may take more time with a 'Verifying...' status message before the application opens. You may get an exception saying that the app cannot be opened because Apple cannot scan it for malicious software. This notice is due to the packaging of the software and is expected. To proceed, click 'OK' and open your 'Security & Privacy' Control panel. There will be a notice that the Installation Assistant was blocked, click 'Open Anyway' and click 'Open' when prompted.

Closing the utility

Close your browser's window and click the close icon on the application window that was opened. **Note:** you must manually close the application window, just closing the browser will not quit the Installation Assistant process

Persistent file storage

The Installation Assistant is intended to be a stand-alone utility without any configuration of its own. But to support the ability to close and return to the utility later to complete tasks, certificate and license file details will be saved in an encrypted format to the client machine in the User's directory. Once a configuration is completed, or you are no longer going to use the Installation Assistant, these files can be removed.

Windows User Storage Location: **C:\Users\<username>\InstallAssistant**

Apple OSX User Storage Location: **/Users/<username>/Library/Application Support/InstallAssistant**

Configuring a Meeting Server using Installation Assistant

Staging

Installation Assistant is only for configuring new, empty servers. Before a Meeting Server can be used with Installation Assistant, three tasks must be addressed:

- ensure the Meeting Server is empty
- obtain the license file
- configure the Meeting Server DNS entries

New Meeting Server Instances

The Meeting Server must have its Virtual Machine deployed and running, an admin account enabled, and its IPV4 'a' interface configured. No other configuration should be performed. The ['Installation Guide for Cisco Meeting Server 1000 and Virtualized Deployments'](#) describes how to deploy a Meeting Server instance or configure a Cisco Meeting Server 1000 appliance. Chapter 3 in the guide describes configuring the server, DO NOT go beyond configuring the 'a' interface (step 2). The server can have a Cisco Meeting Server license loaded, but is not required.

Existing Meeting Server Instances

If a Meeting Server instance has been previously configured or has been used with the Installation Assistant tool but not completed its configuration successfully, it must be factory reset and set to the same configuration state as a new server before it can be used with the Installation Assistant. You cannot use Installation Assistant on top of a prior configuration. To reset the server:

1. Retrieve your existing Cisco Meeting Server license by SFTPing to the server and retrieve the cms.lic file from the server so you have a local copy
2. Log into the MMP interface of Meeting Server with an administrator account and issue the command **factory_reset full** and confirm when prompted. The server will reset itself to default configuration and reboot.
3. Log into the MMP interface of the Meeting Server and login with username **admin** password **admin**.
4. Set a new admin password when prompted.
5. Configure the ipv4 settings for the 'a' interface. See the ['Installation Guide for Cisco Meeting Server 1000 and Virtualized Deployments.'](#)

Note: When following the configuration steps in the above guide, DO NOT go beyond configuring the 'a' interface.

License File

License files are fulfilled by using the Cisco Licensing Portal, using your PAK information from your order and your virtual machine's MAC address. For evaluation/demo licenses, you will be supplied the license directly as a compressed license file. Installation Assistant helps you load the license file to the Meeting Server, but obtaining the file is done external to the tool. You can connect to a Meeting Server without a license file, but you will not be able to move to configuration until a license file is successfully loaded to Meeting Server.

Meeting Server DNS Entries

Installation Assistant only configures the Meeting Server, it does not configure external systems like DNS or SIP proxies. If certificates or hostnames are to be used with Meeting Server, it is recommended you have these DNS entries added to your DNS servers before attempting to use the Installation Assistant.

Configuring a server

The following outlines the major steps to configure a server. For more details about an individual panel or setting, refer to the [Panel Reference](#) portion of this guide.

1. Open the Installation Assistant utility on your client computer, the tool's interface will open in your web browser's window.
2. Click '**Configure Server**' to provide the address and login details to your Meeting Server.
 - a. In the **Configure Server** screen, enter the Meeting Server's address.
 - b. Enter the username configured on the Meeting Server.

Note: By default, 'admin' is used as the username.

- c. Enter your password configured on the Meeting Server.
- d. Enter a passphrase which will be used to securely store the files that the Installation Assistant handles. This passphrase is needed if you close and re-launch the Installation Assistant.

Note: If you re-open the tool after a previous attempt, re-enter the passphrase used previously, otherwise, enter a passphrase of your choice. If you forget your passphrase, delete your files and start again.

Note: It is important that you remember your passphrase. If you forget the passphrase, you must delete the contents from:

Windows user: **C:\Users\`<username>\InstallAssistant`**

MAC user: **/Users/`<username>/InstallAssistant`**

and start a new configuration.

3. Click **Connect**

Note: The **Connect** button is enabled, only after the server address, username and password details are given.

4. The tool allows you to select your Web Bridge deployment. By default, Web Bridge 3 is selected.
5. Select the Web Bridge deployment and click Apply. The tool's configuration view is displayed.
 - If you choose your deployment type as Web Bridge 3, the configuration is based on Windows email address. If Web bridge 2 is selected, the configuration is based on XMPP domain and Windows email address.
6. The Configuration is divided into panels and you must provide the relevant information to complete the configuration. Use the list on the left menu to shift between panels.

Note: The **Certificate** and **License** panels must be completed before the other panels are enabled.

7. Navigate through the panels and complete the fields as prompted. Once all the panels have been completed, the final panel - '**Push Configuration**' requires validation of the provided settings.
8. Review and validate your settings and when ready, click '**Push Configuration**' to push the configuration to the server.

Note: If there is a problem pushing the configuration to the server, a log page is displayed to aid in support of diagnosing the issues.

9. After the configuration is complete, Click **Exit** and you can close the browser window and the console window to exit the tool. Do not forget to close the console window, else the tool's background services will continue to run.

After pushing the configuration

1. Once push configuration is successful, the services that you chose to configure will be configured and enabled. You can access the Web Admin via **https://fqdn:<webadminport>**. If Web Bridge was enabled then it can be accessed via **https://fqdn** and a Test space called **TestCospace** is created on Meeting Server.
2. Ensure you can connect into the Web Admin interface of the server and login. The default is **https://fqdn:445**.
3. Ensure your Call Control is configured to send and receive calls from Meeting Server using the domain names that you have configured.
4. You have a test space defined on the server, update the URI via the Web Admin interface, dial in from an endpoint and test it.
5. If you have enabled importing of users, then synchronizing LDAP changes must be done manually using the '**Sync Now**' button in the Meeting Server Web Admin interface under **Configuration >Active Directory**.
6. If you have enabled Web Bridge, then users can browse to **https://fqdn** to join the meetings.

Running the tool multiple times

Once a configuration has been pushed to a server, the Installation Assistant must not be used to push configuration to the server again unless the server has been factory reset. With the exception of the license file, the Installation Assistant does not change the Meeting Server's configuration until the **Push Configuration** button is clicked. So starting and stopping the tool and connecting to the same Meeting Server is acceptable as long as push configuration has not been attempted.

Troubleshooting

For troubleshooting, you can use the logs which are stored in the following path

Windows: `\C:\InstallAssistantWin\InstallAssistant\portal\logs` on your machine.

Apple OSX: `/Users/<username>/InstallAssistant/logs`

Please refer to this link for troubleshooting information <https://meeting-infohub.cisco.com/faq/category/25/cisco-meeting-server.html>

Closing Installation Assistant

Windows: Close the command prompt window.

Apple OSX: Close the Installation Assistant window.

Uninstalling the software

To remove the Installation Assistant software from the local computer, delete the **InstallAssistant** directory from:

Windows user: **C:\Users\<>username>/**

Apple OSX user: **/Users/<username>/**

Panel Reference

Certificate

The Certificate panel allows you to select which method to specify the X.509 certificate necessary for Meeting Server, and provides a guided process to create new certificate requests for those looking to create new certificates. The Installation Assistant supports using both certificates signed by a Certificate Authority and the use of self-signed certificates. The certificates panel will automatically adapt the options shown based on your selection of using CA signed certificates or self-signed certificates.

Note: Self-signed certificates are not supported for all functionality, they are a security risk and are not recommended.

The recommended path is to use a X.509 certificate signed by a Certificate Authority trusted by your organization. The Certificate Authority can be an internal or public certificate authority. For more details on how Meeting Server uses certificates and their requirements, please refer to the [Cisco Meeting Server, Certificate Guidelines Single Combined Server Deployments Guide](#).

CA Signed Certificate

When the CA Signed Certificate method is selected, there are two available paths:

- **New Certificate via CSR** – The Installation Assistant will guide you through creating a certificate signing request to supply to your Certificate Authority, and they in turn will supply you with a signed certificate.
- **Supply an existing certificate and key** – Upload an existing certificate and key pair you have prepared external to Installation Assistant.

New certificate via CSR

This option guides you through creating a new certificate by creating a Certificate Signing Request (CSR) to provide to your Certificate Authority.

Completing this process requires:

1. Providing details for the certificate in the Installation Assistant and downloading the resulting CSR file.
2. Supplying the CSR to your Certificate Authority and they will return a signed certificate. You will also need the chain of public certificates that represents the Certificate Authority, which they will provide.
3. The resulting files are then uploaded to the Installation Assistant which will handle configuring Meeting Server with the supplied files.

Note: You are free to close the Installation Assistant tool after downloading your CSR. Once you have obtained the signed certificate from the Certificate Authority, relaunch the Installation Assistant and return to the Certificate panel to complete the upload process (see step 4 below).

Steps for creating a new certificate request (CSR):

1. In the Certificates Panel, select Certificate Type '**CA Signed**' and under Certificate Upload Options select '**New Certificate via CSR**'
2. Click '**Generate CSR**' and complete the fields with the details to use for your Meeting Server. The fields are described below. When complete, click the '**Generate**' button to return to the certificate panel. The Generate button is only enabled after you have entered all the required details.

Note: If there is an existing generated certificate, and you click '**Generate CSR**' then the existing file will be over written with the new details, as Installation Assistant does not allow multiple CSR files to be generated.

Table 3: Fields required for a Certificate Signing Request

Field Name	Description	Values
FQDN for Meeting Server	It is the CN value for your certificate and must be defined in the DNS server.	Enter the FQDN of the server.
SIP domain for Meeting Server	It is recommended to use a sub-domain.	Enter the SIP domain of the server to align with the routing rules.
Login domain for Web/Cisco Meeting App users (XMPP Domain)	It is the domain portion of the username, that is used to log into the Cisco Meeting App web app (needed only if you want to enable user login Cisco Meeting App web app). It is recommended that you have different login domain and SIP domain names. Note: If Web Bridge 3 deployment is selected, the XMPP domain is not available as login is done, by using the email address.	Enter the Login domain only if you intend to enable Cisco Meeting App web access (for guests or users).

3. The completed CSR will be shown in the Certificate Panel. Click **Download CSR** to save the resulting CSR to a file on your local drive.
4. Give the CSR to your Certificate Authority to be signed. They will return a signed certificate file. You will also need the certificate chain bundle for that Certificate Authority.
5. Once you have your signed certificate and certificate chain files, return to the Certificate Panel if necessary and click '**Upload Files**' to upload the Certificate/ Bundle. Two fields are shown to specify the certificate and CA certificate chain. Use the '**Select File**' link to locate

the specific file on your local computer. The certificate files must have one of the following extensions (CER,CRT,PEM,DER) and must be encoded as PEM or DER.

6. Once both files are specified, the **'Upload'** button is enabled. Click **'Upload'** and the files will be sent to the Installation Assistant and verified.
7. If successful, the certificate and its details will be shown under **'Available Certificates'** and the Certificate Panel will be marked as complete in the Navigation Tree.

Error Scenarios

- If the upload fails due to server/ technical issue, then an error notification is displayed and you must re-upload the certificate files.
- If the given certificate is incorrect, an error notification is displayed and the **Upload** button is disabled. You have to select and upload the correct certificate and CA certificate chain.

Use Existing Certificate and Key

Installation Assistant provides you with an option to utilize an existing private key and signed certificate for the Meeting Server, rather than generate a CSR via the tool. This is done by using the option **Supply an existing certificate and key**.

You are required to provide the certificate, private key, and CA certificate chain. The certificate files must have one of the following extensions (CER,CRT,PEM,DER) and must be encoded as PEM or DER.

Steps for using an existing certificate:

1. In the Certificates Panel, select Certificate Type **'CA Signed'** and under Certificate Upload Options select **'Supply an existing certificate and key'**
2. Three fields are shown for specifying the certificate, private key, and CA certificate chain. Use the **'Select File'** link to locate the specific file on your local computer. The certificate files must have one of the following extensions (CER,CRT,PEM,DER) and must be encoded as PEM or DER.
3. Once all three files are specified, the **'Upload'** button is enabled. Click **Upload** and the files will be sent to the Installation Assistant and verified

If successful, the certificate and its details will be shown under **Available Certificate** and the Certificate Panel will be marked as complete in the Navigation Tree.

Error Scenarios

- If the upload fails due to server/ technical issue, then an error notification is displayed and you must re-upload the certificate files.
- If the given certificate is incorrect, an error notification is displayed and the **Upload** button is disabled. You have to select and upload the correct certificate and CA certificate chain.

Self Signed Certificate

Self signed certificates are certificates that are signed by the local entity. There is no governing authority validating the certificate. Self-signed certificates are valid, but not recommended due to lack of security and restricted access to functionality. For more information on how Meeting Server uses certificates and their requirements, please refer to the [Cisco Meeting Server Certificate Guidelines](#).

Note: Currently the Installation Assistant does not support configuration of Web Bridge and Conferencing Users when self signed certificate has been chosen.

Note: Self signed certificate details are not stored by the tool, hence it is recommended that you complete the configuration in one go.

Steps for using a self-signed certificate:

1. In the Certificate panel, select **Self signed** and click **Apply**. The Certificate Panel will be marked as complete in the Navigation Tree.

License

An active license file is required to configure and enable the features of Cisco Meeting Server. License files are obtained from the Cisco Licensing Portal using your server's MAC address and the PAK information from your Meeting Server purchase.

Uploading the license

Note: You will receive the xxxx.lic file in a .zip format via email. You must unzip the file before uploading to Installation Assistant.

In the License panel you must upload the active license that must be run on the Cisco Meeting Server. The **Select License** option allows you to locate and upload a new license file.

1. Click **Select license file**.

After the license file is selected and only if the file format is in supported format is the file uploaded. You can view the new license in the **Preview License** option.

Note: The license file name is automatically renamed to the supported format i.e. **cms.lic**.

2. You can view the available service details and click **Open** after providing the correct file.
3. Click '**Preview License**' to view the services that are available with the new license file.

Note: Uploading a new license file will replace the previous license file on the server and any entitlements that it had enabled.

- Click **'Upload'** to save the new license file, or click **'Cancel'** to retain the services activated by the license currently in this server.
-

Note: If you have uploaded an invalid license file, an error message is displayed . You must upload the correct license file in .lic format.

Network

The Network panel allows you to configure the core network settings for the server.


Note: You may need to contact your network administrator for guidance on these settings.

- Configure the following :

Fieldname	Description	Action
Meeting server FQDN	FQDN of the server	Enter a valid FQDN. For example: meetingserver.example.com
NTP Server	You need to configure at least one NTP server by giving either FQDN or IP address. Note: You can configure up to 5 NTP servers.	Click 'Add server' . The address of your NTP server is added to Cisco Meeting Server
Time zone	Local time zone of your server	Select your preferred timezone.
DNS server	You need to configure at least one DNS server by giving either FQDN or IP address. Note: You can configure up to 5 DNS servers.	Enter the IP address of the server and click 'Add server' . The address of your DNS server is added to Cisco Meeting Server Note: Ensure to enter the correct DNS server address in '10.77.89.100' format.
Webadmin port	Configure the TCP port number that the Meeting Server Web Admin Interface listens on. It is recommended to use a port other than 443, so the user facing Web interface (Web Bridge) can use the default HTTPS port.	Enter the port number.

- Ensure that all the details are entered before saving your settings. Click **Save**. The network settings are saved.

Deleting a DNS or NTP server

1. Click  to delete the DNS/ NTP server.

Call Bridge

The Call Bridge panel allows you to configure the settings for the Call Bridge service.

1. Enter the following details:

Field Name	Action
SIP Proxy	Enter the FQDN or IP address of the SIP Proxy that will receive outbound calls from the Meeting Server.
Encryption	Select the encryption mode (TLS) for the connection.
SIP Domain	Enter the SIP domain to which the Meeting Server should respond and is for the inbound rules of Meeting Server.
Media encryption for SIP calls	Select the required option from the drop-down list.
ActiveControl	<p>Enable ActiveControl permissions for all the participants.</p> <p>When this option is enabled, it creates a callLegProfile and systemProfile to enable ActiveControls for participants by default. Note: these settings are not enabled by default in the Meeting Server.</p>

2. Click **Save** to save the settings.

Note: Ensure that all the details are entered to save your settings successfully.

Conferencing User

The Conferencing user panel is an optional configuration which enables the import of users from Active Directory. Importing users allows users to log into the Cisco Meeting App to manage their spaces and join meetings. This panel is only viewable if Web Bridge has been enabled.

Importing users requires:

- Defining the connection properties to connect to your Active Directory server
- Specifying the LDAP location from which users will be imported

- Defining the search filter and property mapping for how LDAP user values are translated to Meeting Server user values. Installation Assistant has default values that works for most environments, but you have the option to override those defaults if necessary.

If you wish to import users from Active Directory:

1. Select the checkbox under **Enable users for Cisco Meeting App**. Additional configuration settings will be displayed.
2. Enter the XMPP domain name for the server in the field provided. This domain must be in the SAN list of your X.509 certificate. If you have the '**Generate CSR**' option to load the certificate, the XMPP domain from that panel will automatically be copied here. This setting will make up the domain portion of the username that users will use to log into Cisco Meeting App.
Note: If Web Bridge 3 deployment is selected, the XMPP domain field is not available as login is done, by using the email address.
3. Fill in the **LDAP Connection Settings** fields with the values for connecting to your Active Directory controller. A **Save** button will be displayed once all required fields are completed.

Details on each setting are provided in the following table:

Table 4: Configuring the LDAP connection

Field Name	Description	Inputs
Protocol	Sets if the connection uses LDAP or LDAP with TLS. LDAPS is recommended	Select either LDAP or LDAPS as appropriate for your environment
Server address	The network address of the LDAP server to connect to.	The FQDN or IP Address of your LDAP server
Port	The TCP port on the LDAP server to connect to. The default for LDAP is 389 or 3268.	A valid port number. The default value is 636 for LDAPS and 389 for LDAP.
Username	The username of the user that will connect to the LDAP server. This user only needs read rights to the directory. Note: If Web Bridge 3 deployment is selected, the default username is in the '\$mail\$' format.	The LDAP Distinguished Name (DN) or UPN of the user to authenticate with. This field cannot be left blank
Password	The password of the user specified.	Password of the user. This field cannot be left blank.

Field Name	Description	Inputs
Search base	The location in the LDAP directory from where import search queries will start from. For assistance with this value, contact your Domain Administrator.	The LDAP Distinguished Name (DN) of the directory location where searches should start. This field cannot be left blank
Assign PMP licenses to users	If enabled, imported users will be marked to be entitled to a PMP+ license. Do not enable if you have not purchased PMP+ licenses for all users being imported.	Enable to tag each imported user as having a PMP+ entitlement.
Override default user filter and field mapping details	Installation Assistant uses a default LDAP Search Filter and user field mappings that should work for most environments. This option when enabled, offers you the ability to view and customize these settings to fit your environment.	Enable to view or customize the LDAP search filter, and or LDAP user field mappings.

Customizing the LDAP Search and user mappings

Installation Assistant uses a default LDAP Search Filter and user field mappings that should work for most environments. The default, filters on users that have an email address defined, a username, and will set their Meeting Server username to <Windows username>@<XMPPdomain>.

Enabling the override option will display the individual configuration fields used for import and show the settings Installation Assistant is using by default. When Override is enabled, users have the ability to customize these values to fit their environment.

The user mapping expressions define how to set the properties of a user when importing them into Meeting Server. The expressions use variables along with static text so that a user's properties in LDAP can be used when creating the user in Meeting Server. The use of LDAP properties is critical to ensure properties that are required to be unique per user (such as username or URI) are not duplicated. LDAP properties are referenced by their property name enclosed with the \$ symbol. Example: The LDAP property 'mail' is referenced by \$mail\$ in the field mapping expressions.

Table 5: LDAP Import settings

Field Name	Description	Inputs
LDAP search filter	Defines the criteria of which LDAP users will be matched to be imported.	LDAP search string. Must use LDAP search syntax
Display name	The name shown for the user in directories and searches.	Mapping expression. Example: \$cn\$

Field Name	Description	Inputs
User name	<p>The XMPP username that the user will use to log into Cisco Meeting App. This must be in the format where the username ends with @<XMPP Domain Name> and <XMPP Domain Name> matches the domain name defined in the rest of the Installation Assistant steps.</p> <p>The resulting value must be unique across all users and spaces.</p>	<p>Mapping expression.</p> <p>Example: <code>\$sAMAccountName\$@company.com</code></p> <p>This field cannot be blank and the result must be unique for each imported user</p>
Space name	<p>Label given to space automatically created for user.</p> <p>Leave blank if not creating spaces for imported users.</p>	<p>Mapping expression.</p> <p>Example: <code>\$cn\$ Meeting space</code></p>
Space URI	<p>Left hand portion of URI for the space automatically created for the user.</p> <p>Result must be unique per user and not conflict with usernames or other spaces. Leave blank if not creating spaces for imported users..</p>	<p>Mapping expression.</p> <p>Example: <code>\$cn\$.space</code></p>
Space secondary URI	<p>Left hand portion of a second URI for the space automatically created for the user.</p> <p>Result must be unique per user and not conflict with usernames or other spaces. Optional field. Leave blank if not creating spaces for imported users.</p>	<p>Mapping expression.</p> <p>Example: <code>\$cn\$.room</code></p>
Space callID	<p>Sets the call ID for the space automatically created for the user.</p> <p>Result must be unique across all spaces. Optional field, Cisco Meeting Server will assign IDs automatically if left blank.</p> <p>Leave blank if not creating spaces for imported users.</p>	<p>Mapping expression.</p>
Authentication ID mapping	<p>Mapping property assigned to the imported user. Used in smartcard login scenarios.</p> <p>Leave blank unless specifically deploying certificate based logins.</p>	<p>Mapping expression.</p> <p>Example: <code>\$userPrincipalName\$</code></p>

1. Click **Save** to save the settings.

Note: Ensure that all the details are entered to save your settings successfully.

Web Bridge

You have the option to enable the Web Bridge feature of Meeting Server. Enabling the Web Bridge in the Web Bridge panel will enable participants to join meetings as guests using the web based Cisco Meeting App. If Web Bridge is enabled, you also have the option to enable the import of users from Active Directory so users can login and manage spaces using the Cisco Meeting App web app. Enabling authenticated users is configured in the Conference User panel which is only enabled if Web Bridge has been configured to be enabled.

To enable the Web Bridge feature, in the Web Bridge panel:

1. Select the **Enable Web Bridge** checkbox.
2. If Web Bridge 2 is selected, in the XMPP domain name text field, provide the XMPP domain to use in Meeting Server. This setting must match the login domain configured in Generated CSR steps (if used) and be in the Subject Alternative Names (SAN) list in your Meeting Server certificate.
Or
If Web Bridge 3 is selected, enter the Call Bridge to Web Bridge (c2w) listening port number, that has to be opened, which would allow the Call Bridge to connect to the Web Bridge (the default port number is 9999).
3. Click **Save**.

Note: When Web Bridge is enabled, the Installation Assistant creates a local DNS RR entry in Meeting Server for the required XMPP SRV record. This local entry is only resolvable by Meeting Server, and is only intended to support the local Web Bridge in this simplified setup. The local DNS RR entry can be deleted and replaced by proper SRV records in your DNS server if necessary.

Security

The Security option allows you to create another user in the Meeting Server, if you lose access to your default administrator account.

1. Select '**Create backup user account**' to create a recovery account.
2. Provide the new username, password and confirm the password.

Note: The password must not be blank and username should not be admin.

3. Click **Save**. The login credential is created and saved.

Push Configuration

The Push Configuration panel allows you to check all the details of the respective panels that you have configured on Installation Assistant. It also allows you to send your details to the Cisco Meeting Server to complete the configuration process. You must validate the settings before pushing the configuration. The **Push configuration** button is enabled after successful completion of the validation. If the validation is unsuccessful, go to the specific panels and update the conflicting settings.

1. Check the panel configuration details and click '**Validate settings**'.
2. After successful validation, the **Push configuration** option is enabled.
3. Click **Push configuration** button to send your details to the Cisco Meeting Server to complete the configuration process.

Note: If the provided certificate does not contain all the required fields then the following error message is displayed '**Validation failed as the given certificate does not contain XMPP/ SIP domain details required to import users and access their space. Upload the correct certificate or disable Conferencing User and Web Bridge panel settings and then validate the configuration details.**'

If you want to deploy Web Bridge 2, the certificates will be validated to check, if they contain the FQDN and SIP/XMPP domain

If you want to deploy Web Bridge 3, the certificates will be validated to check, if they contain the FQDN and SIP/XMPP domain. Additionally, the app checks if the extended key usage field, if specified in the Certificate contains both TLS Web Server Authentication and TLS Web Client Authentication.

4. Enter the encryption passphrase to encrypt /decrypt the private keys. Note: This field must not be blank.

The Installation Assistant checks the information provided in the panels and if any errors are found they are displayed. You must make the required changes and validate the configuration details.

5. On successful validation, the **Push configuration** button is enabled. Click on the **Push configuration** button to start the configuration.

Note: If validation is unsuccessful, return to the specific panels and update the conflicting settings.

6. Once the configuration is pushed successfully to Cisco Meeting Server, the Installation Assistant displays the summary details. You can also download the logs . Exit the tool

without making any further changes. The panels are available when you re-open the Installation Assistant.

Note: If the push configuration to the Cisco Meeting Server is unsuccessful, you must check the log details for more information. Click **Download logs** to download and view the log details file.

Note: If push configuration fails and you wish to reuse the Installation Assistant on a server that has already been configured, then you must factory reset the Meeting Server and re-configure the IP address, before using the Installation Assistant again on the same server. Factory reset is done by logging into the MMP command line of the server using **ssh**, and issuing the **'factory_reset full'** command. The Factory reset command will remove the license file and network configuration, so ensure that the information is captured before factory resetting the server.

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.

© 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)

2 Glossary

M

My Term

My definition