Step by Step guide for Multiparty Licensing (PMP and SMP) on Cisco Meeting Server

Contents

Introduction

This document describes how to assign Personal Multiparty Plus (PMP+) license or Shared Multiparty Plus (SMP+) license to CMS users.

Prerequisites

CMS (Cisco Meeting Server) now supports multiparty licensing, similar to the multiparty licensing model first introduced on Cisco Conductor and Cisco Telepresence Server. Multiparty licenses can be per user (PMP+ license), or shared (SMP+ license). To ensure the licenses are correctly deployed, there are a number of steps to be taken.

Requirements

Cisco recommends that you have knowledge of these topics:

- CMS
- API client application, or familiarity with REST API coding
- PMP and SMP licenses

Components Used

This document is not restricted to specific software and hardware versions.

Multiparty licenses can only be assigned on CMS through Application Program Interface (API) configuration. Therefore in order to deploy multiparty licenses, it is required to have:

- CMS
- Callbridge license (also known as the CMS release key)

- One or more PMP and/or SMP licenses
- Access credentials to the CMS API
- Postman REST tool

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

Background Information

> **Note**: This document describes the configurational steps using the **Postman REST** client. Note that the appropriate API commands can be applied through any other **REST API** tool of your choice.

The following parameters will be edited in this article:

- **userProfile** - defines whether a user has a PMP license assigned to it (**hasLicense** attribute)
- **ldapServers**, **ldapMappings**, **ldapSources** (optional, used in this example) - at least one of each has to be defined, in order to assign PMP license to a subset of users
- **system profiles** (optional) - to be used if PMP is assigned to all users globally
- **tenant** settings (optional) - to be used if PMP license is assigned per tenant

Configure

PMP licenses are assigned per user, but in CMS you cannot edit attributes of individual users. License assignment is based on a **userProfile** attribute. The **userProfile** cannot be associated with individual users. Instead, **userProfile** can be associated:

- globally: associating the **userProfile** to **/api/v1/system/profiles**
- per tenant: associating the **userProfile** to **/api/v1/tenants/<tenantID>**
- per **ldapSource**: associating the **userProfile** to **/api/v1/ldapSources/<ldapSourceID>** - for this step, you will need to ensure, that LDAP is configured through API alone, and that it is fully configured, including at least one **ldapServer**, at least one **ldapMapping** and at least one **ldapSource**

Any meeting which cannot be linked to a particular user who has an assigned PMP license, will default to using a SMP license instead. The SMP license type does not require any assignment.

Once you have decided to implement **LDAP** through **API**, you will need to remove the **LDAP** configurations from the Web GUI of CMS.

1. Set up LDAP Sources

The LDAP settings in API are divided in three parts: LDAP server(s), LDAP Mappings and LDAP sources, and all of them are required.

The LDAP source is the actual source of users. You must have one LDAP Server and one LDAP mapping defined per source. Several sources can share the same LDAP server, and/or the LDAP mapping.

Step 1. Login to **CMS** and navigate to **Configuration > Active directory.**

- Delete the settings on the webpage. Click on **Submit** and **Sync now**
- Verify that there are no users present anymore under **Status > Users**

Step 2. Create the LDAP server.

- Use the **Postman REST API** tool to **POST** to the **/ldapServers**

address	ldap.example.com
portNumber	389
username	cn=administrator,cn=users,dc=example,dc=com
password	password
secure	False

- Take note of the **Ldap Server ID** in the response header

Step 3. Create the LDAP Mapping.

- Use the **Postman REST API** tool to **POST** to**/ldapMappings**

nameMapping	cn
jidMapping	$sAMAccountName$@example.com
coSpaceUriMapping	$sAMAccountName$.space
coSpaceNameMapping	cn's Meeting Space
coSpaceCallIdMapping	$ipPhone$

- Take note of the**LDAP Mapping ID** returned in the response header

Step 4. Create LDAP sources.

- Use the **Postman REST API** tool to **POST** to **/ldapSources**
- Enter the **Filter** as one line (in the showed example it is broken in three lines for readability).
  Take note of the **Ldap Source ID**

server	<LDAPServerID created in step 1.2>
mapping	<LDAPMappingID created in step 1.3>
baseDN	dc=example,dc=com
Filter	(& (memberof=cn=SMPusers,ou=Demo Users, dc=example,dc=com (! (memberof=cn=PMPusers,ou=Demo Users, dc=example,dc=com)))

This LDAP source will import all users that are in the **SMPUsers LDAP group**, but who are not in the **PMPusers group**.

- Use the **Postman REST API** tool to **POST** to **/ldapSources**
- Take note of the **LDAP Source ID**

server	<LDAPServerID created in step 1.2>
mapping	<LDAPMappingID created in step 1.3>
baseDN	dc=example,dc=com

Filter (memberof=cn=PMPusers,ou=Demo Users, dc=example,dc=com)

This LDAP Source will import all users that are in the **PMPusers group**.

Step 5. Sync users.

- Use the **Postman REST API** tool to **POST** to **/ldapSyncs**

ldapSource <1st LDAPSourceID created in step 1.4>

- Use the **Postman REST API** tool to **POST** to**/ldapSyncs**

ldapSource <2nd LDAPSourceID created in step 1.4>

Step 6. Verify users.

You can run a **GET** on **/ldapSyncs** in order to list the currently ongoing and scheduled **LDAP sync events**. If the **Syncs** have already been performed, the **API** nodes would have already been deleted (this is the default behavior, and it can be changed). You can check a list of imported users through the web admin as well.

2. Create user Profiles and associate them with LDAP sources

Step 1. Create a **userProfile** for SMP users.

- Use the **Postman REST API** tool to **POST** to **/userProfiles**

hasLicense false

Step 2. Create a **userProfile** for PMP users.

- Use the **Postman REST API** tool to **POST** to **/userProfiles**

hasLicense true

Step 3. Set SMP as default.

You must update the **Global Profile** with the **SMP userProfile**.

- Use the **Postman REST API** tool to **PUT** to **/system/profiles**

userProfile <user Profile ID created in step 2.1>

Step 4. Associate PMP licenses with users in **PMPusers group**.

Update the **LdapSource** for the members of **PMPusers AD group** with the PMP user profile.

- Use the **Postman REST API** tool to **PUT** to **/ldapSources/<2nd LDAPSourceID created in step 1.4>**

userProfile <user Profile ID created in step 2.2>

- Repeat the LDAP sync operation, as per step 5

Verify

The successful import of the users can be verified on **CMS** Web GUI page under **Status > Users**.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.