

How to Configure LDAP Import on CMS Version 3.0

Contents

[Introduction](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Meeting Server LDAP settings](#)

[Configuration](#)

[IdapServers](#)

[IdapMappings](#)

[IdapSources](#)

[LDAP import](#)

[Verify](#)

[Additional information](#)

Introduction

This document describes how to import users from an Lightweight Directory Access Protocol (LDAP) directory. This allows end-users to Log in via Cisco web app with their own account to manage their spaces and join meetings.

Contributed by Jefferson Madriz and Octavio Miralrio, Cisco TAC Engineers.

Requirements

Cisco recommends that you have knowledge of these topics:

- Active Directory
- CMS version 3
- Application Programming Interface (API)

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

Components Used

The information in this document is based on these software and hardware versions:

- CMS version 3.0
- Windows LDAP directory

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

Meeting Server LDAP settings

LDAP Server Location/address: network IP address of the LDAP Server.

Name: a label to help identify objects in the API.

LDAP Username/Password: credentials used to connect to the LDAP server.

Port/portNumber: The network port to use when connecting to the LDAP server.

Secure: When enabled, connection uses secure LDAP.

Base Distinguished Name/baseDN: LDAP location where Meeting Server search for users.

Filter: Search filter that defines which LDAP objects to include in the search.

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

Display Name/nameMapping: Name shown for the user in user searches and directories in Meeting Server.

Username/jidMapping: The username the user use to Log in via web app, the result must be unique for each user

Space Name/coSpaceNameMapping: Label given to the auto-generated space for that user

Space URI user part/coSpaceUriMapping: Defines the user portion of the Uniform Resource Identifier (URI) for the autogenerated space for that user, result must be unique for each user.

Space secondary URI user part/coSpaceSecondaryUriMapping: Defines a secondary URI for the auto-generated space for the user (optional). Usually used to assign a E164 style URI to the space, result must be unique for each user.

Space call ID/coSpaceCallIdMapping: Sets the call ID for the auto-generated space for the user (optional). If not defined, a random call ID is generated automatically, result must be unique for each user

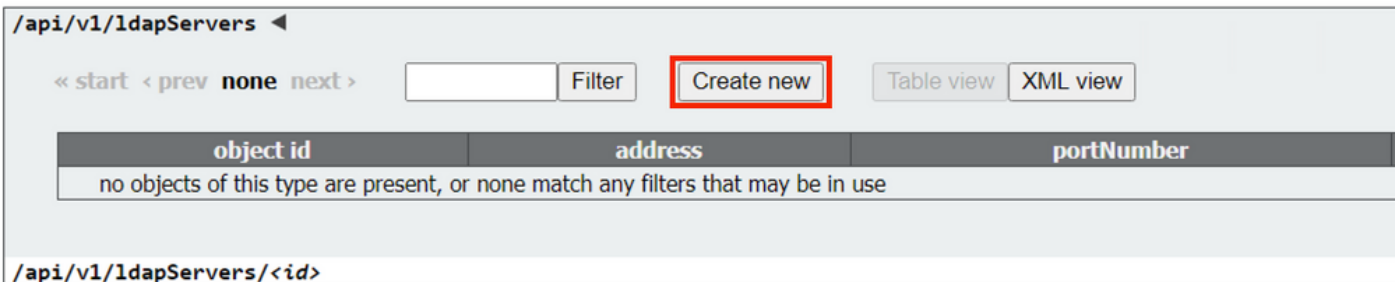
Configuration

For the simplified deployment example, in this example is shown import of all users from Active Directory. The import optionally supports creation of a personal space for each imported user. This configuration can be made with Webadmin, or API, it's not possible to have both configure at the same time.

IdapServers

1. Log in to the Meeting Server Webadmin interface
2. Navigate to **Configuration > API**.
3. Use the **Filter** input box, enter **IdapServers** to filter the list view.
4. Select the arrow next to the **/api/v1/IdapServers** object.
5. Click **Create new** to configure a new **IdapServers** object.

Filter (2 of 116 nodes)



6. Enter the server values. Example values below must be updated to match your environment.
address: 10.15.13.90 (or FQDN)
name: MXC Users
portNumber: 3268
username: CN=user1,OU=CMSusers,DC=mx,DC=lab
password: <Password for supplied user>
secure: set to true

Object configuration	
address	10.15.13.90
name	MXC Users
username	CN=user1,OU=CMSusers,DC=mx,DC=lab
portNumber	3268
secure	true

7. Click **return to object list** to return to the full list of API objects.

IdapMappings

1. Use the **Filter** input box, enter **IdapMappings** to filter the list view.
2. Select the arrow next to **/api/v1/IdapMappings**.
3. Select **Create new** to configure a new **IdapMappings** object.
4. Configure the Field Mapping Expressions. These values can be customized to your deployment. The simplified deployment recommendation is to use the user's email address for username (jidMapping) and to create spaces for all imported users.

jidMapping: \$mail\$

nameMapping: \$cn\$

coSpaceUriMapping: \$sAMAccountName\$.space

coSpaceNameMapping: \$cn\$ space

Object configuration	
jidMapping	\$mail\$
nameMapping	\$cn\$
cdrTagMapping	
coSpaceNameMapping	\$cn\$ space
coSpaceUriMapping	\$sAMAccountName\$.space
coSpaceSecondaryUriMapping	
coSpaceCallIdMapping	
authenticationIdMapping	

5. Click **return to object list** to return to the full list of API objects.

IdapSources

1. Use the **Filter** input box, enter **IdapSources** to filter the list view.
2. Select the arrow next to **/api/v1/IdapSources**.
3. Select **Create new** to configure a new **IdapSources** object.
4. The **server** parameter must be set to the ID of the **IdapServers** object created in earlier steps.
5. The **mapping** parameter must be set to the ID of the **IdapMappings** object created in earlier steps.
6. Configure the **baseDn** and **filter** parameters. These values define the search performed in the LDAP server when users are imported.

baseDn OU=CMSusers,DC=mx,DC=lab

filter (&(objectCategory=person)(sAMAccountName=*))

or (&(sAMAccountType=805306368)(sAMAccountName=*)(mail=*))

Object configuration	
server	d23ff491-6b35-4fdf-91e3-9587a5956340
mapping	c02e12dc-7482-4167-9e05-a4312f5e8133
baseDn	OU=CMSusers,DC=mx,DC=lab
filter	(&(objectCategory=person)(sAMAccountName=*))
nonMemberAccess	true

Note: : If your directory has a large number of users (more than 10,000) or you do not want to enable all users, the Base distinguished name and Filter can be changed to target a more specific group or set of users. Consult this with your LDAP administrator.

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

LDAP import

With the **IdapServer**, **IdapMapping**, and **IdapSource** objects created, the LDAP import/sync process must be run to import users. The sync process must be re-run anytime you want user changes in the LDAP server to be updated in Meeting Server.

1. Log in to the Meeting Server Webadmin interface.
2. Navigate to **Configuration > Active Directory:**
3. Select **Sync Now** at the bottom of the page.

Note: Sync Now can still be used even though the configuration on this page is not used.

Verify

After a minute or two, navigate to **Status > Users** which now displays the users created by the LDAP import.

Navigate to **Configuration>Spaces** and validate the spaces that were created for the imported users are displayed.

Users

Filter

Name	Email	XMPP ID
user1@mx.c.lab	user1@meet.mx.c.lab	
user2@mx.c.lab	user2@meet.mx.c.lab	

1

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

Additional information

[LDAP Tips an Examples](#)