

Configuration des utilisateurs LDAP sur Cisco Meeting Server via l'API

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit la configuration de LDAP (Lightweight Directory Access Protocol) sur Cisco Meeting Server via l'API (Application Programming Interface).

Conditions préalables

Application PostMan

Cisco Meeting Server (CMS)

Microsoft Active Directory

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Serveur de réunion Cisco

Microsoft Active Directory

Informations générales

Flux de configuration de haut niveau pour synchroniser LDAP via l'API.

Étape 1. Configurez le paramètre /ldapServers via l'API comme décrit ci-dessous

1. Informations sur l'adresse/le port du serveur LDAP
2. Nom d'utilisateur et mot de passe pour accéder au serveur
3. Sécurisation de la LDAP non sécurisée.

Étape 2 : Configurez le paramètre /ldapMappings via l'API comme décrit ci-dessous

1. objets de propriétés utilisateur LDAP vers des objets utilisateur correspondants cms
2. Par exemple, jid utilisateur cms va mapper à \$sAMAccountName\$@domain.com sur cms et etc.

Étape 3 : Configurez les paramètres /ldapSources via l'API comme décrit ci-dessous pour lier les objets ldapServers et ldapMappings.

Configuration

Étape 1. Configurer /ldapServers

1. Envoyez un POST pour /ldapServers , qui créerait un ID ldapServer. Utilisez un ID /ldapServers unique pour une configuration ultérieure.

POST Send
 https://10.106.80.30:7445/api/v1/ldapservers

2. La réponse au test POST reviendrait au même format <ldapServer id=« 7ca32cc4-389f-46f5-a1b0-0a468af291a4 »>
3. Capturer les informations ci-dessous pour mettre à jour l'ID de serveur LDAP conformément au [Guide de référence de l'API CMS](#)

Parameters	Type/Value	Description/Notes
address *	String	The address of the LDAP server to connect to.
portNumber *	Number	The TCP or TLS port number to connect to on the remote LDAP server.
username	String	The username to use when retrieving information from the LDAP server.
password	String	The password of the account associated with username.
secure *	true false	Whether to make a secure connection to the LDAP server. If "true" then TLS will be used; if "false", TCP will be used.

4. Exemple de méthode POST avec paramètres

POST Send
 https://10.106.80.30:7445/api/v1/ldapservers/7ca32cc4-389f-46f5-a1b0-0a468af291a4?address=10.106.80.4&name=...

Params ● Authorization ● Headers (10) Body Pre-request Script Tests Settings

Query Params

	KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/>	address	10.106.80.4	
<input checked="" type="checkbox"/>	name	DOT4ADserver	
<input checked="" type="checkbox"/>	username	CN=Administrator,CN=Users,DC=S,DC=com	
<input checked="" type="checkbox"/>	portNumber	389	
<input checked="" type="checkbox"/>	secure	false	

5. Exécuter un GET pour vérifier les paramètres configurés

GET https://10.106.80.30:7445/api/v1/ldapServers/7ca32cc4-389f-46f5-a1b0-0a468af291a4

Params Authorization ● Headers (9) Body Pre-request Script Tests Settings

Body Cookies (1) Headers (15) Test Results Status: 200 OK

Pretty Raw Preview Visualize XML

```
1 <?xml version="1.0"?>
2 <ldapServer id="7ca32cc4-389f-46f5-a1b0-0a468af291a4">
3   <address>10.106.80.4</address>
4   <name>DOT4ADserver</name>
5   <username>CN=Administrator,CN=Users,DC=S,DC=com</username>
6   <portNumber>389</portNumber>
7   <secure>>false</secure>
8 </ldapServer>
```

Étape 2 : configuration de /ldapMappings

1. Envoyez un POST pour /ldapMappings pour créer un ID /ldapMappings. Utilisez /ldapMappings ID et configurez les paramètres ci-dessous.

POST https://10.106.80.30:7445/api/v1/ldapMappings Send

2. Capturer les informations ci-dessous pour mettre à jour l'ID de mappage LDAP conformément au [Guide de référence de l'API CMS](#)

Parameters	Type/Value	Description/Notes
jidMapping	String	The template for generating user JIDs from the associated LDAP server's entries, for instance \$sAMAccountName\$@example.com.
nameMapping	String	The template for generating user names from the associated LDAP server's entries; for instance "\$cn\$" to use the common name.
cdrTagMapping	String	The template for generating a users' cdrTag value. Can be set either to a fixed value or be constructed from other LDAP fields for that user. The user's cdrTag is used in callLegStart CDRs. See the Cisco Meeting Server CDR Reference for details.
authenticationIdMapping	String	The template for generating authentication IDs from the associated LDAP server's entries, for instance "\$userPrincipalName\$".
coSpaceUriMapping	String	If these parameters are supplied, they ensure that each user account generated by this LDAP mapping has an associated personal coSpace. The user is automatically added as a member of the coSpace, with permissions defined above
coSpaceSecondaryUriMapping	String	In order for that coSpace to be set up as required, these parameters provide the template for setting the coSpaces' URI, displayed name and configured Call ID. For example, setting coSpaceNameMapping to "\$cn\$ personal coSpace" ensures that each user's coSpace is labelled with their name followed by "personal coSpace".
coSpaceNameMapping	String	Note that the generated coSpace will have its own cdrTag - and it will be the same as the user's cdrTag and cannot be changed other than by changing the cdrTagMapping above and re-syncing. (The coSpace's cdrTag is used in the callStart CDR. See the Cisco Meeting Server CDR Reference for details.)
coSpaceCallIdMapping	String	Note that the normal uniqueness rules apply to the URI and Call IDs of coSpaces set up in this way: it is not valid to have the same URI or Call ID for more than one coSpace set up by a given LDAP mapping, nor is it valid for such a coSpace URI or Call ID to be the same as one currently in use elsewhere on the Meeting Server.

3. Configurer les paramètres ci-dessous pour ldapMappings

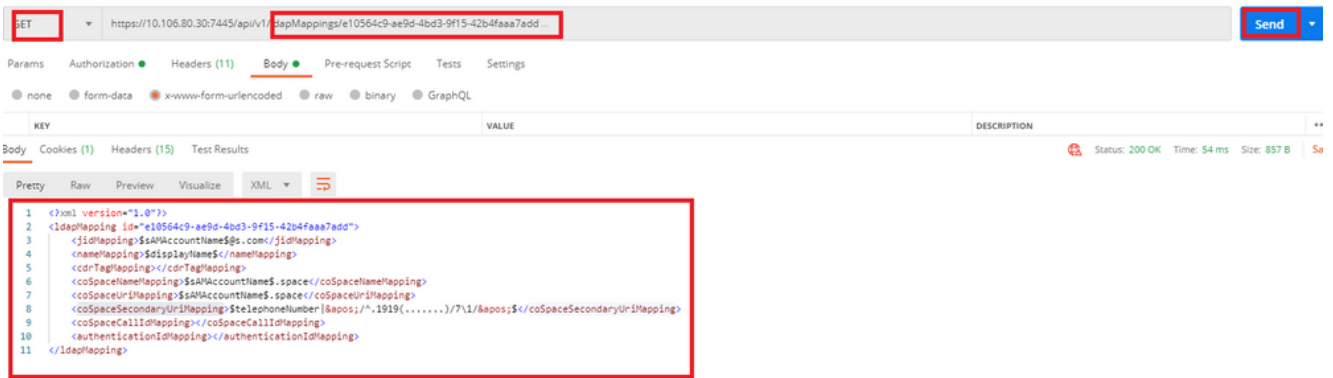
POST https://10.106.80.30:7445/api/v1/ldapMappings/e10564c9-ae9d-4bd3-9f15-42b4faa7add

Params Authorization Headers (11) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> jidMapping	\$sAMAccountName@\$s.com	
<input checked="" type="checkbox"/> nameMapping	\$displayName\$	
<input checked="" type="checkbox"/> coSpaceNameMapping	\$sAMAccountName\$.space	
<input checked="" type="checkbox"/> coSpaceUriMapping	\$sAMAccountName\$.space	
<input checked="" type="checkbox"/> coSpaceSecondaryUriMapping	\$telephoneNumber[?^,1919(.....)]/71/\$	

4. Exécutez une commande GET pour vérifier les paramètres configurés.



Étape 3. Configurer /ldapsources

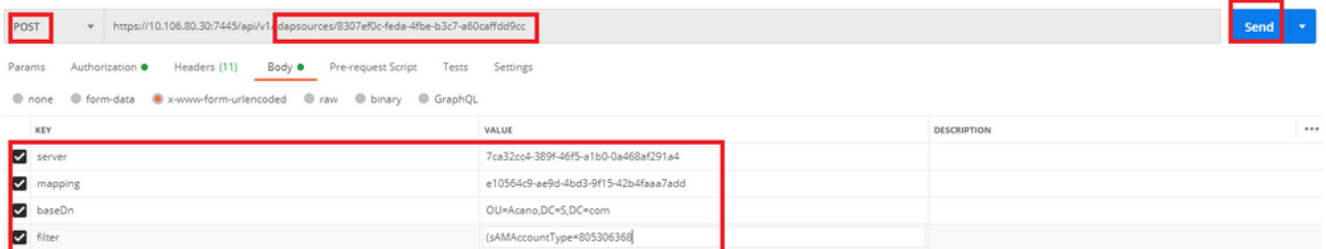
1. Envoyez un POST pour /ldapsources pour créer un ID /ldapsources. Utilisez /ldapsources ID et configurez les paramètres ci-dessous.



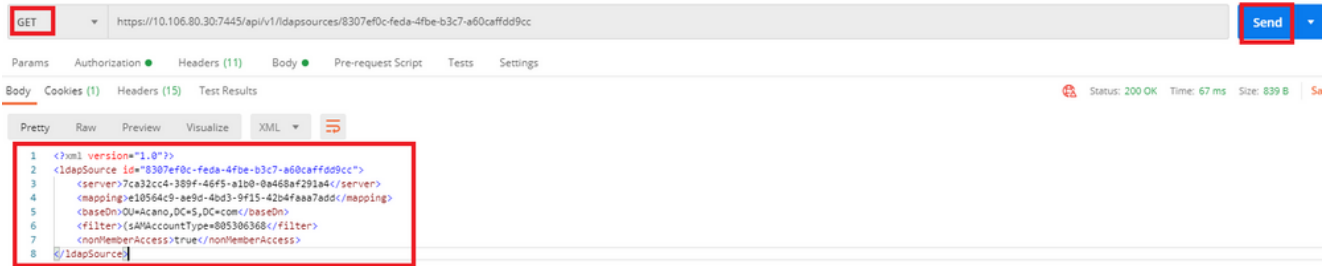
2. Capturer les informations ci-dessous pour mettre à jour l'ID de mappage LDAP conformément au [Guide de référence de l'API CMS](#)

Parameters	Type/Value	Description/Notes
server *	ID	The ID of a previously-configured LDAP server (see above)
mapping *	ID	The ID of a previously-configured LDAP mapping (see above)
baseDn *	String	The distinguished name of the node in the LDAP server's tree from which users should be imported, for instance "cn=Users,dc = <companyname>,dc=com"
filter	String	An LDAP filter string that records must satisfy in order to be imported as users, for instance "(objectClass=person)"
tenant	ID	If supplied, the ID for the tenant to which the LDAP source should be associated. Users imported with this LDAP source will be associated with that tenant
userProfile	ID	If supplied, this is the ID of the user profile to associate with users imported via this LDAP source. This parameter is present from version 2.0 onwards.
nonMemberAccess	true false	This parameter pre-configures newly created spaces to allow or disallow non-member access. Spaces existing before the LDAP sync are not affected. true - no passcode is required to access the space and non-members are able to access the created spaces. This is the default setting and matches behavior before this parameter was introduced in version 2.0. false - ensures the member must configure non-member access and set a passcode as part of the LDAP sync. This setting allows a company to enforce passcode protection for non-member access to all user spaces. For more information, see Section 1.2 .

3. Configurer les paramètres ci-dessous pour ldapSources



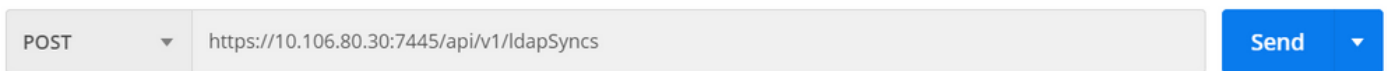
4. Exécutez une commande GET pour vérifier les paramètres configurés.



La configuration est terminée. Nous pouvons effectuer une synchronisation complète maintenant.

Vérification

Étape 1. Envoyer le POST pour /ldapSyncs à partir de l'API et vérifier les journaux des événements



Étape 2. Archiver les journaux des événements si la synchronisation est terminée.

10:50:41.225	Info	10.65.86.71: API user "admin" created new LDAP sync operation c02dbb2b-c63e-4bb8-a39f-bbee2cd9611f
10:50:41.225	Info	LDAP sync operation starting
10:50:41.269	Info	LDAP sync operation: finalising
10:50:41.650	Info	LDAP sync operation c02dbb2b-c63e-4bb8-a39f-bbee2cd9611f complete
10:50:55.705	Info	10.65.86.71: web user "admin" logged in
10:50:55.705	Info	web session 1 now in use for user "admin"
10:53:04.331	Info	1103 log messages cleared by "admin"
10:53:07.569	Info	10.65.86.71: web user "admin" created new LDAP sync operation 50c7034c-9aa7-4e81-a304-4113734ffc11
10:53:07.570	Info	LDAP sync operation starting
10:53:07.594	Info	LDAP sync operation: finalising
10:53:07.943	Info	LDAP sync operation complete

Étape 3. Vérifiez que les utilisateurs sont synchronisés à partir de la source ldap.

Users

Filter Submit Query

Name	Email	Username
Gogi	gogi@s.com	gogi@s.com
Sai acano	saiacano@s.com	Saiacano@s.com
go go	gogo@federation.com	gogo@federation.com
ivrman	ivrman@s.com	ivrman@s.com
joey	joey@s.com	joey@s.com
prashant	prkapur@s.com	prkapur@s.com
sai1 acano	sai1acano@federation.com	sai1acano@federation.com
sankar v		sankar@s.com
shakur 2pac	2pac@s.com	2pac@s.com
user1	user1@acanolab3.com	user1@s.com
user2 2	user2@s.com	user2@s.com

Dépannage

Vérifiez que les paramètres API et les attributs LDAP sont exacts.

La capture de paquets à partir du pont d'appel permet d'isoler les problèmes de connectivité avec LDAP.