

Konfigurieren von LDAP-Benutzern auf dem Cisco Meeting Server über API

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die Konfiguration von LDAP (Lightweight Directory Access Protocol) auf Cisco Meeting Server über API (Application Programming Interface).

Voraussetzungen

PostMan-App

Cisco Meeting Server (CMS)

Microsoft Active Directory

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Cisco Meeting Server

Microsoft Active Directory

Hintergrundinformationen

Allgemeiner Konfigurationsfluss zur Synchronisierung von LDAP über API.

Schritt 1: Konfigurieren des /ldapServers-Parameters über API wie unten beschrieben

1. LDAP-Serveradresse/-Port-Informationen
2. Benutzername und Kennwort für den Zugriff auf den Server
3. Sicherung von nicht sicherem LDAP

Schritt 2: Konfigurieren des Parameters /ldapMappings über die API wie unten beschrieben

1. LDAP-Benutzereigenschaften-Objekte zu Cms entsprechenden Benutzerobjekten
2. Beispiel: cms user jid wird auf cms und etc. \$sAMAccountName\$@domain.com zugeordnet.

Schritt 3: Konfigurieren von /ldapSources-Parametern mithilfe der API, wie unten beschrieben, um das Objekt ldapServers und ldapMappings zu binden.

Konfiguration

Schritt 1: Konfigurieren von /ldapServers

1. Senden Sie einen POST für /ldapServers, der eine ldapServer-ID erstellen würde. Verwenden Sie für die weitere Konfiguration die eindeutige /ldapServers-ID.

POST

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

Send

2. Die Antwort auf den POST-Test würde im ähnlichen Format zurückgegeben <ldapServer id="7ca32cc4-389f-46f5-a1b0-0a468af291a4">
3. Erfassen Sie die folgenden Informationen, um die LDAP-Server-ID gemäß dem [CMS API-Referenzhandbuch](#) zu aktualisieren.

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. Beispiel für eine POST-Methode mit Parametern

POST

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

Send

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. Durchführen einer GET-Überprüfung, um konfigurierte Parameter zu überprüfen

The screenshot shows a REST client interface. At the top, the method is set to 'GET' and the URL is 'https://10.106.80.30:7445/api/v1/ldapServers/7ca32cc4-389f-46f5-a1b0-0a468af291a4'. Below the URL bar, there are tabs for 'Params', 'Authorization', 'Headers (9)', 'Body', 'Pre-request Script', 'Tests', and 'Settings'. The 'Body' tab is selected, and the response is displayed in 'Pretty' format. The response is an XML document with the following content:

```
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>
```

Schritt 2: Konfigurieren von /ldapMappings

1. Senden Sie einen POST für /ldapMappings, um eine /ldapMappings-ID zu erstellen. Verwenden Sie die /ldapMappings-ID, und konfigurieren Sie die folgenden Parameter.

The screenshot shows a REST client interface. The method is set to 'POST' and the URL is 'https://10.106.80.30:7445/api/v1/ldapMappings'. A blue 'Send' button is visible on the right side of the interface.

2. Erfassen Sie die folgenden Informationen, um die LDAP-Zuordnungs-ID gemäß dem [CMS API-Referenzhandbuch](#) zu aktualisieren.

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. Konfigurieren der folgenden Parameter für ldapMappings

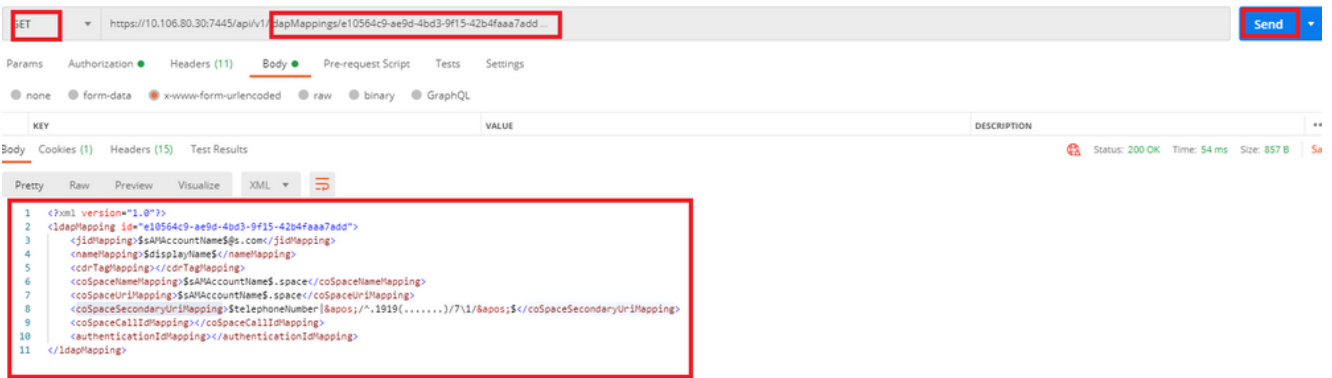
POST https://10.106.80.30:7445/api/v1/ldapMappings/e10564c9-ae9d-4bd3-9f15-42b4faa7add Send

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 7^1919(.....)7/1/\$	

4. Führen Sie ein GET aus, um die konfigurierten Parameter zu überprüfen.



Schritt 3: Konfigurieren von /ldapsources

1. Senden Sie einen POST für /ldapsources, um eine /ldapsources-ID zu erstellen. Verwenden Sie die /ldapsources-ID, und konfigurieren Sie die folgenden Parameter.



2. Erfassen Sie die folgenden Informationen, um die LDAP-Zuordnungs-ID gemäß dem [CMS API-Referenzhandbuch](#) zu aktualisieren.

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. Konfigurieren der folgenden Parameter für ldapSources

POST

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

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

KEY	VALUE	DESCRIPTION
server	7ca32cc4-389f-46f5-e1b0-0a468af291a4	
mapping	e10564c9-ae9d-4bd3-9f15-42b4faa7add	
baseDn	OU=Acano,DC=S,DC=com	
filter	{sAMAccountType=805306368}/filter	

4. Führen Sie ein GET aus, um die konfigurierten Parameter zu überprüfen.

GET

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

Body Cookies (1) Headers (15) Test Results

Pretty Raw Preview Visualize XML

```

1 <?xml version="1.0"?>
2 <ldapSource id="8307ef0c-feda-4fbc-b3c7-a60caffdd9cc">
3   <server>7ca32cc4-389f-46f5-e1b0-0a468af291a4</server>
4   <mapping>e10564c9-ae9d-4bd3-9f15-42b4faa7add</mapping>
5   <baseDn>OU=Acano,DC=S,DC=com</baseDn>
6   <filter>{sAMAccountType=805306368}/filter
7   <nonMemberAccess>true</nonMemberAccess>
8 </ldapSource>

```

Status: 200 OK Time: 67 ms Size: 839 B

Die Konfiguration ist abgeschlossen. Wir können jetzt eine vollständige Synchronisierung durchführen.

Überprüfung

Schritt 1: Senden von POST für /ldapSyncs über API und Überprüfen von Ereignisprotokollen

POST

Schritt 2: Aktivieren Sie Ereignisprotokolle, wenn die Synchronisierung abgeschlossen ist.

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

Schritt 3: Überprüfen Sie, ob die Benutzer von der LDAP-Quelle synchronisiert werden.

Users

Filter

Name	Email	Username
Gogi	gogi@s.com	gogi@s.com
Sai acano	saicano@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

Fehlerbehebung

Überprüfen Sie, ob die API-Parameter und LDAP-Attribute korrekt sind.

Die Annahme von Paketerfassungen von der Call Bridge hilft bei der Isolierung von Verbindungsproblemen mit LDAP.