Cisco Meeting Server

Multi-tenancy considerations

January 02, 2019

Contents

Change History

Date	Change Summary
January 02, 2019	Removed version number from title.
October 02, 2018	Minor change to documentation map for version 2.4.
November 03, 2017	Added note to section XMPP multi-domains.

1 Introduction

In this document, the term “coSpace has been replaced with “space”.

The Cisco Meeting Server supports multi-tenancy; this refers to sub-dividing the capacity of the server into a set of “islands”, where each island has all of the functionality of the unit as a whole, but has no access to the resources (for instance users, spaces, or active calls) of other tenants. For example, if users that are associated with a tenant search for a space, they only see spaces associated with their own tenant.

The multi-tenancy provision is through the Cisco Meeting Server API. (For details of features that support multi-tenancy, see the Cisco Meeting Server API Reference Guide.)

This document describes setting up multi-tenancy usage.

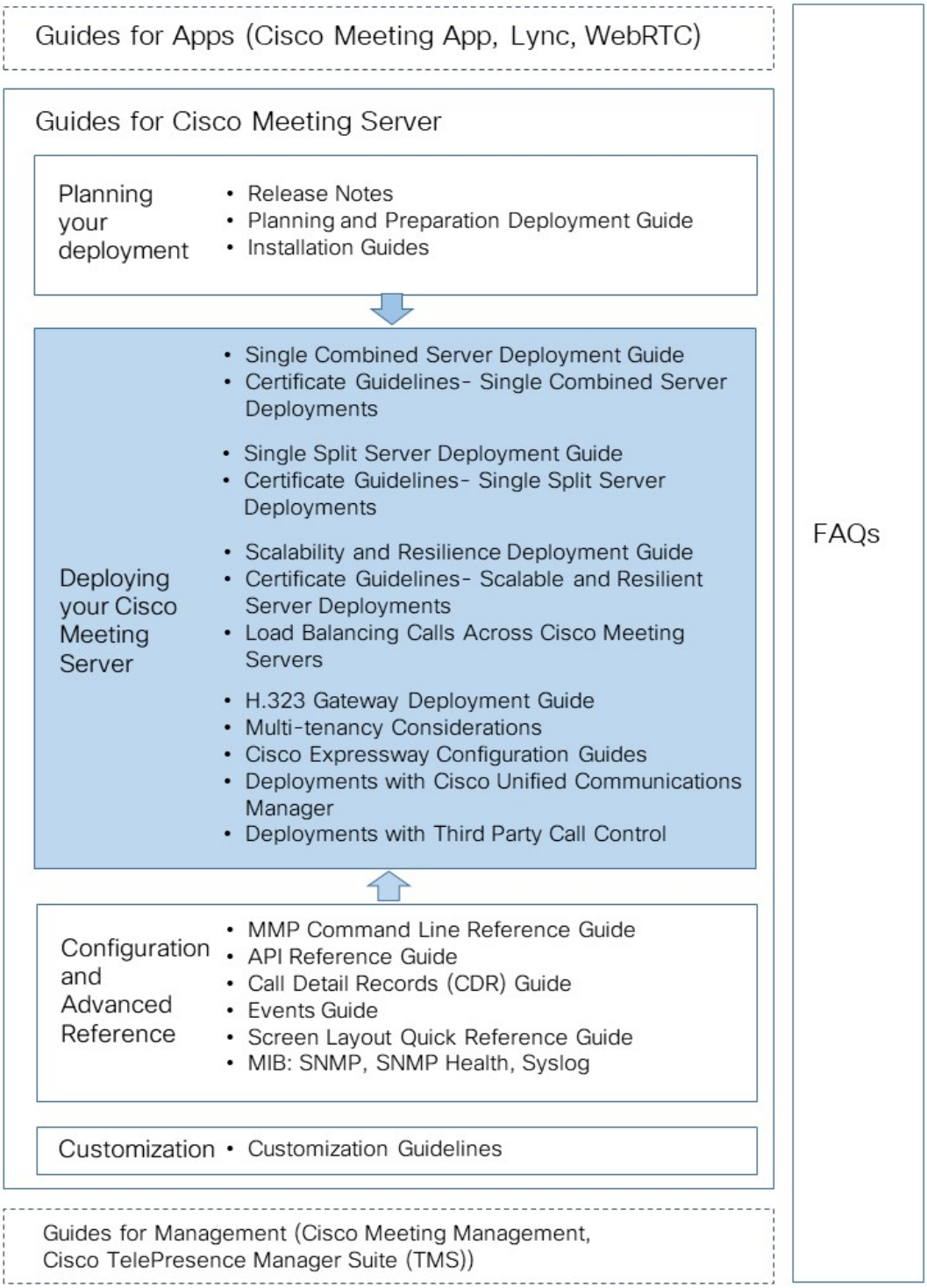
Note: When using multi-tenancy, not every user or space (and therefore not every call) has to be associated with a tenant.

Note: The recording facility on the Meeting Server supports multi-tenancy. At the end of recording a meeting, the recording is automatically converted to MP4. The converted file is suitable for placing within a document storage/distribution system, for example, in a network file system (NFS) used for multi-tenancy, they are stored in the NFS folder tenants/<tenant ID>/spaces/<space ID>. For more information on recording, see the Meeting Server API guide and the deployment guides.

1.1 How to use this Document

This document is part of the documentation set (shown in Figure 1) for the Cisco Meeting Server.

Figure 1: Overview of guides covering the Cisco Meeting Server



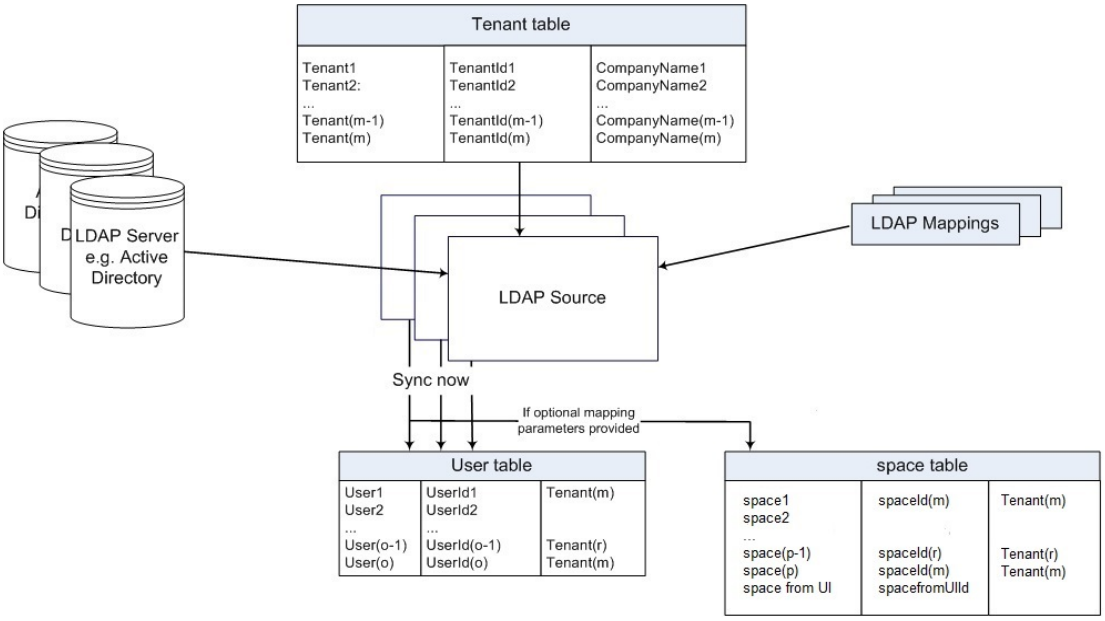
1.2 Multi-tenancy Basics

Figure 2 shows an outline of the multi-tenancy process. The Tenant table is fundamental to multi-tenancy and therefore to all tenant operations. Use the API to create, modify and delete tenants.

LDAP Sources can be associated with a tenant (but need not be). If an LDAP Source is associated with a tenant, then after the LDAP synchronization with that source, any imported LDAP users will also be associated with that tenant – and if user spaces are created as part of the process, they are also associated with the tenant.

As a consequence, all calls made by these users, or for these spaces are also associated with the tenant.

Figure 2: Outline multi-tenancy process



Note: The letters m to r show that the number of entries in each table is not necessarily the same; for example, there are likely to be several users per tenant.

Note: The space table may contain spaces set up through the Cisco Meeting App – not only those created through LDAP Server synchronization.

2 Suggested Procedure

To provide multi-tenancy, follow these steps. The appendix provides an example.

1. Set up your tenant table using the API POST operation for creating tenants (see the API Reference).
2. Set up the LDAP Servers, LDAP Mappings and LDAP Sources using the API.
   - LDAP Server configuration provides location and authentication, and is independent of multi-tenancy. Equally multi-tenancy does not necessarily require more than one LDAP Server if sub-OUs or subdomains are associated with a particular tenant; clearly, the LDAP Source configuration must be configured appropriately
   - LDAP Mapping configuration defines the form of user account names created on synchronization and is independent of multi-tenancy. If the optional cospaceUriMapping, cospaceNameMapping and cospaceCallIdMapping API parameters are provided, then a space will be created for every user who is created during synchronization. This very powerful functionality is described in the API Reference guide.
   - LDAP Source configuration defines which LDAP Source and LDAP mapping to use, the set of Active Directory or OpenSSL users to consider for import and the filter pattern to apply in order to decide whether to import individual users. LDAP Sources can be associated with a tenant – and therefore the API POST operation may need to contain a tenant id parameter if you are using multi-tenancy.

   Note: Each user and space must be able to be dialed; that is, requires a unique URI. Therefore ensure that your LDAP Servers, LDAP Mappings and LDAP Sources are set up to make this happen.

3. Synchronize LDAP sources, either through the API (recommended) or Web Admin Interface:
   - POST operation on the "/ldapSyncs" node. See the API Reference for details. If the synchronization completed successfully, the response includes a "Location" of the form "/api/v1/ldapSyncs/<LDAPsync ID>".
   - Log in to the Web Admin Interface, go to **Configuration > Active Directory** and click **Sync now**. Check that the synchronization completed successfully. For example, check the syslog to verify that the process completed without errors and check the **Status > Users** page in the Web Admin Interface to ensure that user names are as intended.
4. If you are using the Cisco Meeting App, check that spaces are set up as expected.

3 Configuring Tenants

In addition to users, spaces and their calls (and call legs) being associated with a tenant; there are several objects that can be configured per tenant, these are:

- Web Bridge
- IVR
- Inbound dial plan rules
- Participants – tenantParticipantLimit
- External access methods
- External directory search
- Access query
- Profiles

Use the Cisco Meeting Server API to configure these objects, details are in the API Reference Guide.

3.1 Multiple deployments on a server

Multi-tenancy is supported where multiple deployments can be hosted on the same server. This feature is provided via the following features:

- tenants can be assigned to a tenant group. This provides a mechanism for splitting tenants into separate independent groups. Each group consists of one or more tenants. Set tenant groups up through the API, refer to the API Reference Guide for details.
- IVRs and web bridges can now be created for a group of tenants as well as for an individual tenant through the API, refer to the API Reference Guide for details.
- tenanted dial plans, this enables the outgoing dial plan to have rules set that are tenant specific. Outbound connections can have tenant specific Local From Domain to allow call back to reach the correct tenant. See section "Tenanted dial plans" on the next page.
- tenanted call IDs. Call IDs must be unique within a tenant group, but maybe reused for different tenant groups.
- XMPP multi-domains. XMPP multi-domains enables a single Cisco Meeting Server to host multiple XMPP domains. See Section 3.4

.

3.2 Tenanted dial plans

Different dial plan rules for forwarding calls and for outbound calls can be setup for tenants through the API, details are in the API Reference Guide. This is applicable to single tenant and multi-tenant deployments.

3.2.1 Forwarding rules

Forwarding rules can have a tenant associated with them. When a forwarding rule with an associated tenant is used, the call (conference) spawned by that rule is associated with the same tenant.

3.2.2 Outbound dial plan rules

You can associate an outbound dial plan rule with a tenant. Once associated, the only call legs that can be placed using that rule are those that originate from calls (conferences) associated with the same tenant, or associated with no tenant.

3.3 Tenant call limits

This feature enables an administrator to limit the number of calls a tenant can make to ensure that a tenant does not consume all of the resources. This feature works across distributed deployments and is applicable to single tenant and multi-tenant deployments.

To set the tenant call limit, set participantLimit on the /tenants/<tenant id>/ API object. Details are in the API Reference Guide.

Note: Call limits may be exceeded when simultaneous calls occur to different Call Bridges.

3.4 XMPP multi-domains

XMPP multi-domain enables a single Cisco Meeting Server to host multiple XMPP domains. For example, both example.com and example.org can exist on the same server. It is possible to configure multiple tenants with the same XMPP domain (as in previous releases), or each tenant with their own domain, or mix these schemes.

Note: It is strongly recommended that multiple XMPP domains are not used for a single tenant, or in cases where tenants are not used.

To configure multiple domains for the XMPP server to listen to, use the MMP command:

```
xmpp multi_domain add <domain name> <key-file> <crt-file> [<crt-bundle>]
```

where:

<key-file> is the private key that you created for the XMPP server

<crt-file> is the signed certificate file for the XMPP server

[<crt-bundle>] is the optional certificate bundle as provided by the CA

Refer to the Certificate Guidelines for background information on certificates.

Note:
1) You also need to add a DNS SRV record for each additional XMPP domain, and to add the domain to the Incoming Calls page on the Web Admin interface (Configuration>Incoming calls).

2) Restart the XMPP server for the configured multiple domains to take effect.

3) The XMPP server will not start if the private key or certificate files are missing or invalid

To list the domains that the XMPP server is listening to, use the command:

xmpp multi_domain list

To delete a domain that the XMPP server is listening to, use the command:

xmpp multi_domain del <domain name>

Appendix A Multi-tenancy Configuration Example

This appendix assumes that you have followed the instructions in theCisco Meeting Server Installation Guide completely. If this is not the case, then do so now before following this example.

In this example:

- Postman is used as the tool to access the API
- Cisco Meeting Server Web Admin Interface IP address is192.168.1.101.
- Active Directory Server IP address is 192.168.1.10

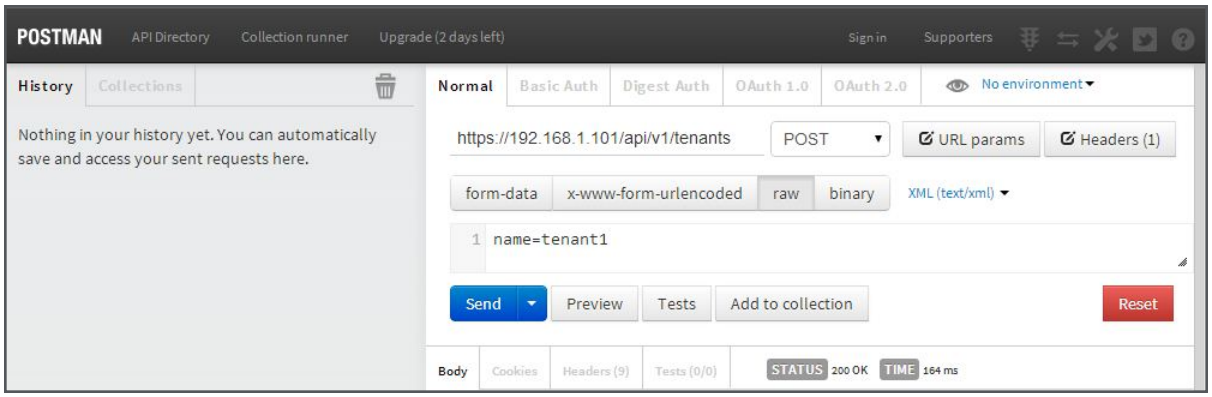
For full details of the API functionality see the Cisco Meeting Server API Reference Guide.

A.1 Creating Tenants

Creating is a POST operation on the "/tenants" node.

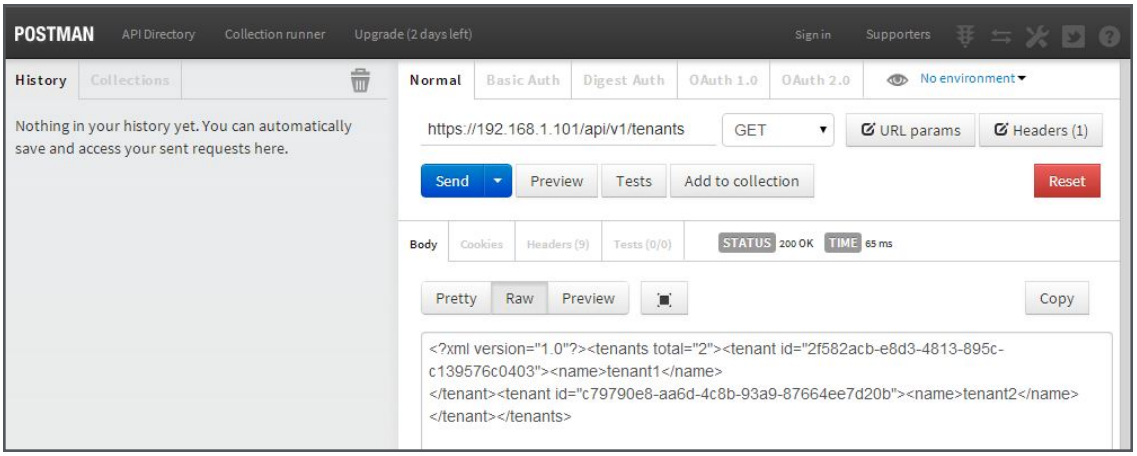
1. Create two tenants, tenant1 and tenant2:
   - Perform two POST operations with the Post URL https://192.168.1.101/api/v1/tenants
   - The body message is "name=tenant1" for the first POST and then "name=tenant2".

   If the POST operation is successful, 200OK status is seen as below.



2. Perform a GET operation as a check. Each tenant has its own tenant ID, as shown below
   - Tenant1 ID = 2f582acb-e8d3-4813-895c-c139576c0403

- Tenant2 ID = c79790e8-aa6d-4c8b-93a9-87664ee7d20b



A.2 Creating an LDAP Server

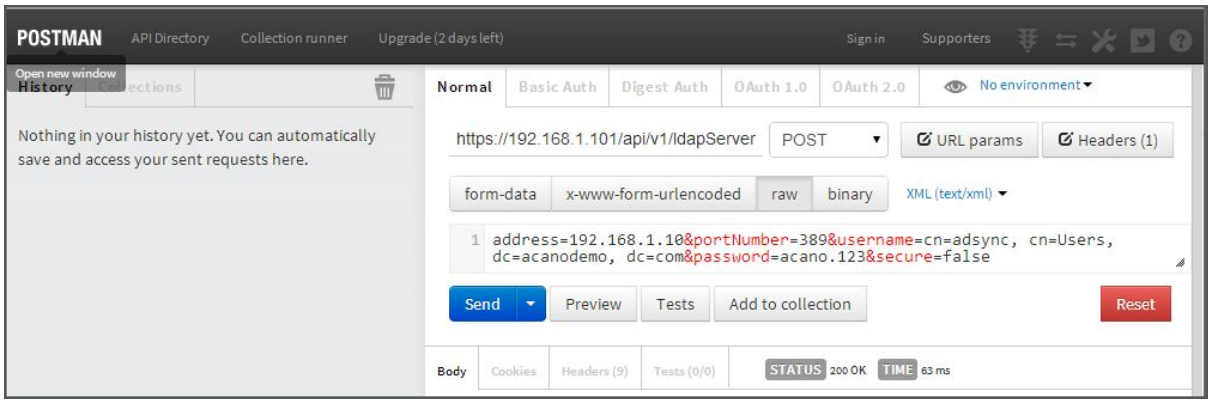
Creating is a POST operation performed on the "/ldapServers" node.

This example creates an LDAP server with the following:

- LDAP server address: 192.168.1.10
- Port: 389
- Username: cn=adsync, cn=Users, dc=acanodemo, dc=com
- Password: <password_of_user_adsync>

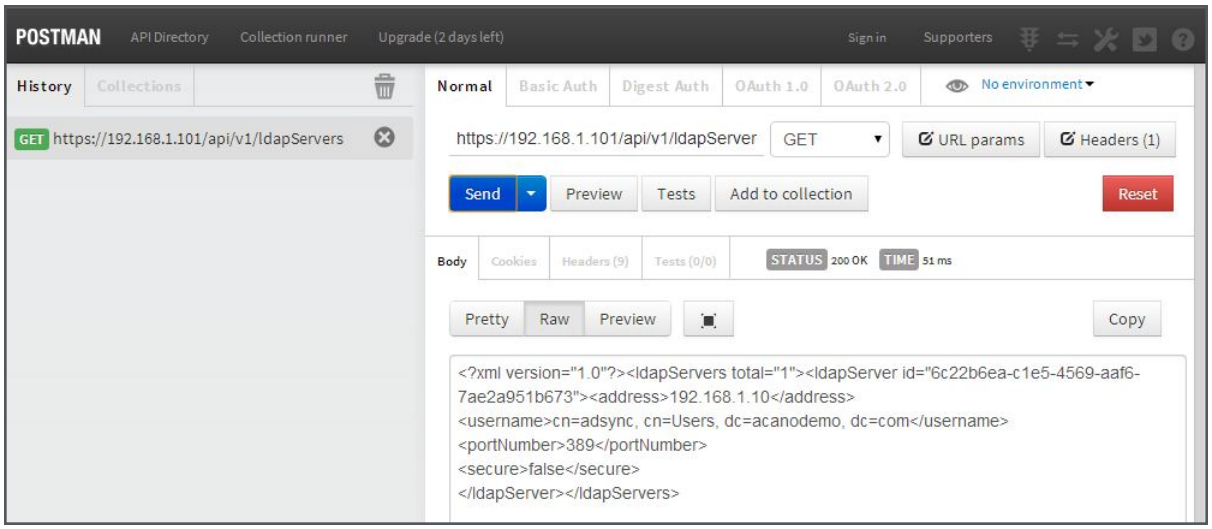
3. Perform a Post operation with
   - the Post URL https://192.168.1.101/api/v1/ldapServers
   - body message is "address=192.168.1.10&portNumber=389&username=cn=adsync, cn=Users, dc=acanodemo, dc=com&password=acano.123&secure=false"

   If the POST operation is successful, a 200OK status is seen, as below.



4. Perform a GET operation as a check. The LDAP server ID:

   LDAP server ID = 6c22b6ea-c1e5-4569-aaf6-7ae2a951b673



A.3 Creating an LDAP Mapping

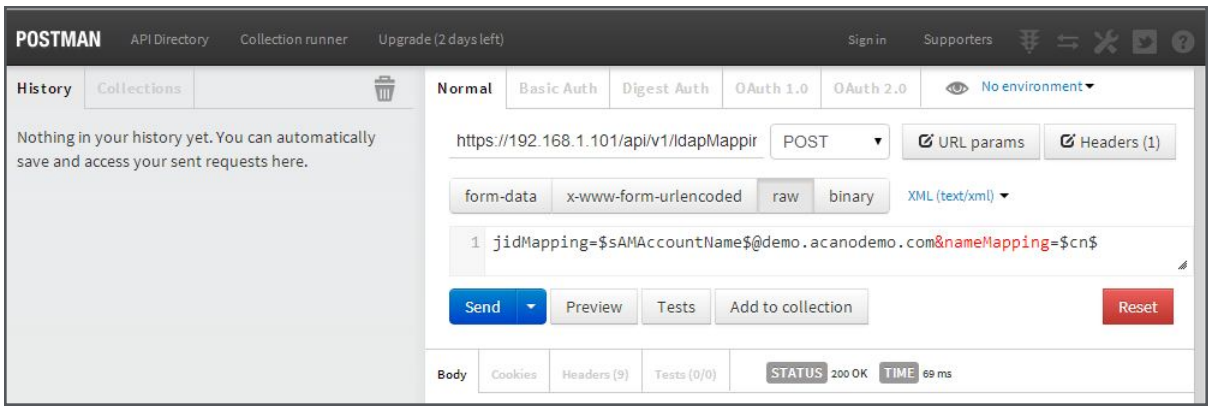
Creating is a POST operation on the "/ldapMappings" node.

In this example the LDAP mapping will map:

- Display name: cn
- Username: $sAMAccountName$@demo.acanodemo.com

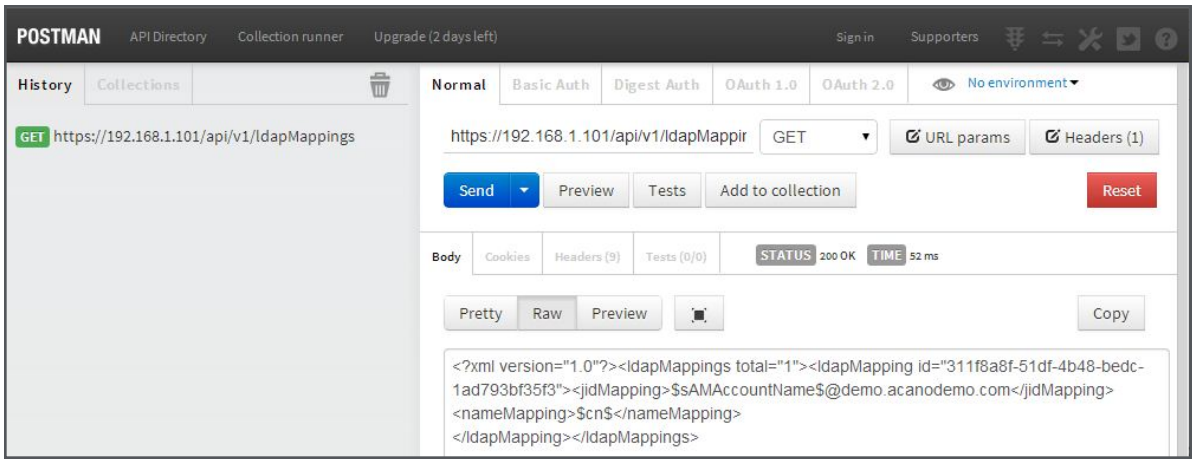
5. Perform a Post operation with
   - the Post URL https://192.168.1.101/api/v1/ldapMappings
   - body message is "jidMapping=$sAMAccountName$@demo.acanodemo.com&nameMapping=cn "

   If the POST operation is successful, a 200OK status is seen, as below.



6. Perform a GET operation as a check.

   LDAP mapping ID = 311f8a8f-51df-4b48-bedc-1ad793bf35f3



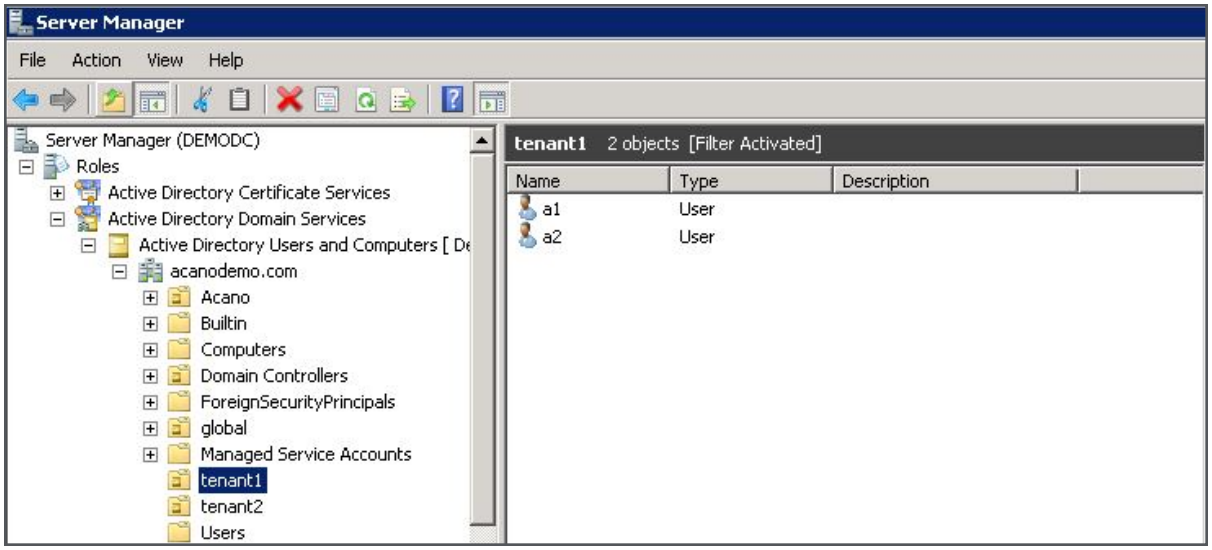
A.4 Creating an LDAP Source

Creating is a POST operation on the "/ldapSources" node.

This example creates an LDAP source for tenant1 with:

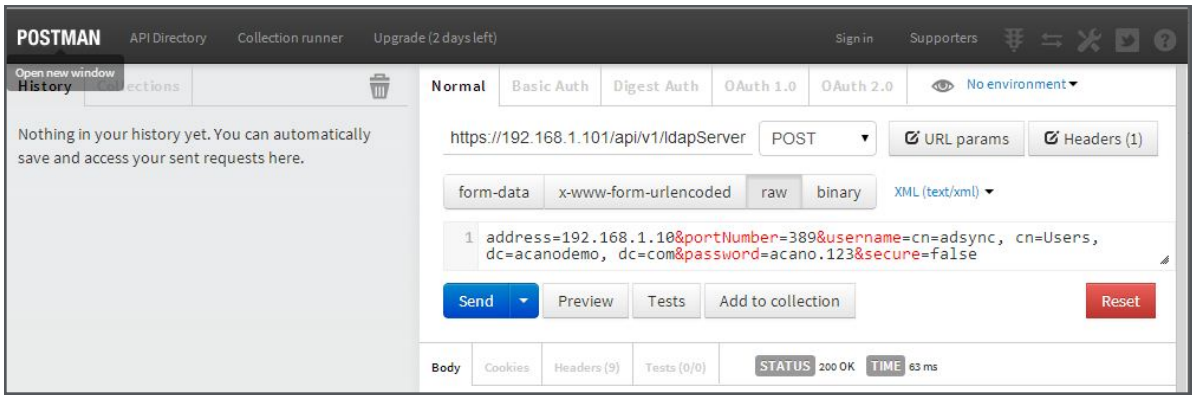
- LDAP Server ID: 6c22b6ea-c1e5-4569-aaf6-7ae2a951b673
- LDAP Mapping ID: 311f8a8f-51df-4b48-bedc-1ad793bf35f3
- Tenant1 ID: 2f582acb-e8d3-4813-895c-c139576c0403
- BaseDn: ou=tenant1,dc=acanodemo,dc=com
  (create an OU=tenant1 and create users a1, a2 under it)
- Filter: objectClass=person

See the Directory Information Tree below.

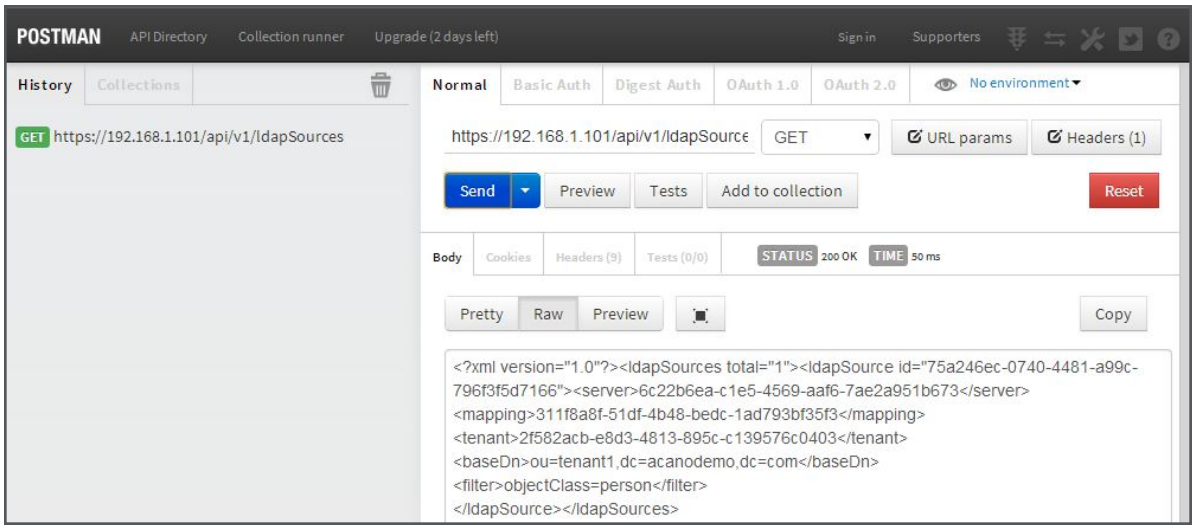


7. Perform a Post operation with
   - Post URL https://192.168.1.101/api/v1/ldapSources
   - body message is "server=6c22b6ea-c1e5-4569-aaf6-7ae2a951b673&mapping=311f8a8f-51df-4b48-bedc-1ad793bf35f3&baseDN=ou=tenant1,dc=acanodemo,dc=com&filter=objectClass=person&tenant=2f582acb-e8d3-4813-895c-c139576c0403 "

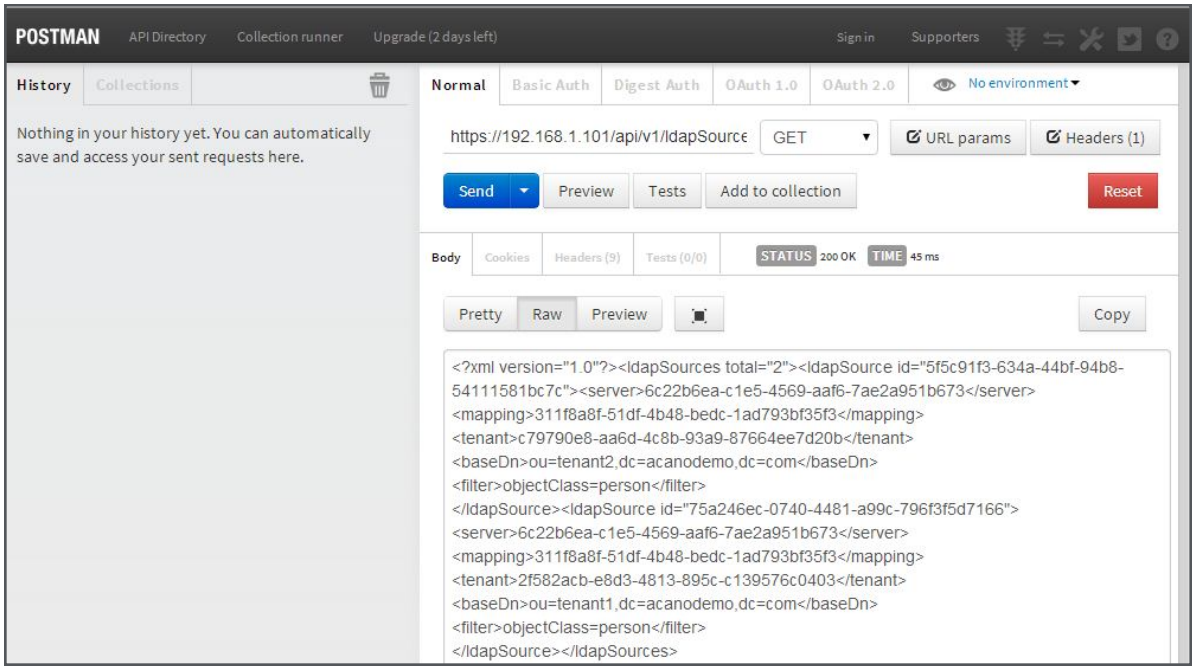
   If the POST operation is successful, a 200OK status is seen as below.



8. Perform a GET operation as a check. The LDAP Source has its ID.



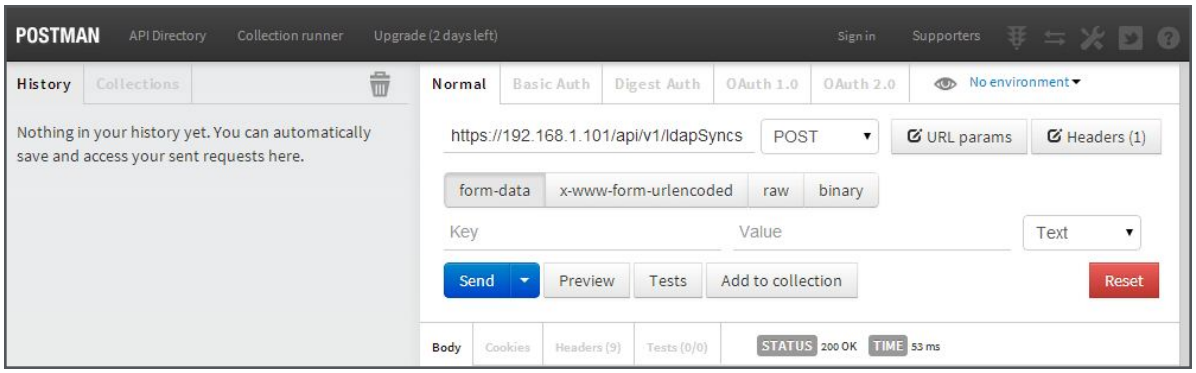
9. Create the second LDAP Source for tenant2 by following the steps above.
10. After performing a GET operation, you see the two LDAP Sources each with their own ID.



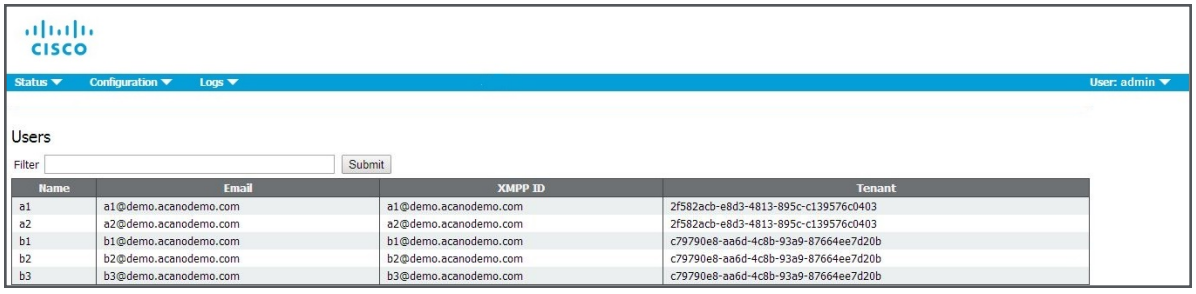
Note: To import from a security group, see the Cisco Meeting Server Support FAQs.

A.5 Performing an LDAP Sync to Import Users from Tenants

11. Perform a Post with Post URL https://192.168.1.101/api/v1/ldapSyncs and no body message.



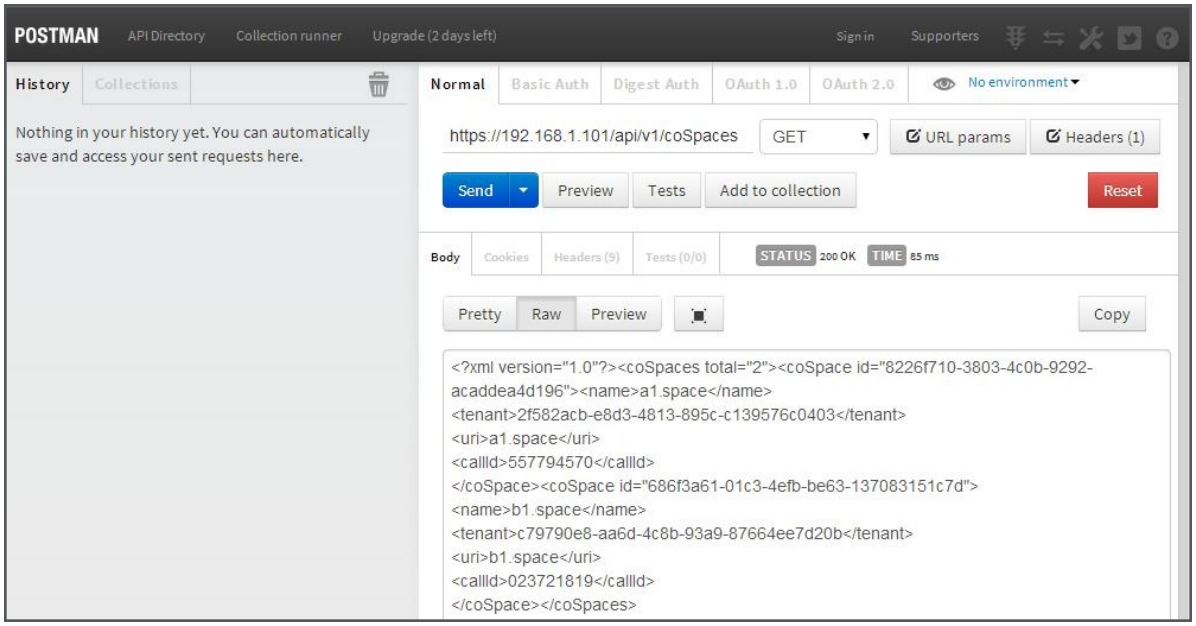
12. Verify the Sync operation by going to the Web Admin Interface Status > Users page. In this example, users a1 and a2 are tagged with tenant1's ID, while users b1, b2 and b3 are tagged with tenant2's ID.



A.6 Creating spaces

15. Sign in on a Cisco Meeting App as user a1.
16. Create a space called a1.space.
17. Sign in on a Cisco Meeting App as user b1.
18. Create a space called b1.space.
19. Using Postman check that a1.space is tagged with tenant1, and b1.space is tagged with tenant2.

Note: The API object for spaces is still called /coSpaces.



A.7 Testing Multi-tenancy

20. Log in on a Cisco Meeting App as a1, and join a1.space.
21. On a different Cisco Meeting App, log in as user b1 and join b1.space.

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.

Cisco Trademark