

# Configure LDAP in UCS Manager

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Create a Local Authentication Domain](#)

[Create an LDAP Provider](#)

[LDAP Group Rule configuration](#)

[Create an LDAP Provider Group](#)

[Create an LDAP Group Map](#)

[Create an LDAP Authentication Domain](#)

[Verify](#)

[Common LDAP Issues.](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes the configuration for remote server access with LDAP Protocol in our Unified Computing System Manager Domain (UCSM).

## Prerequisites

### Requirements

Cisco recommends knowledge of these topics:

- **Unified Computing System Manager Domain (UCSM)**
- Local and Remote authentication
- **Lightweight Directory Access Protocol (LDAP)**
- **Microsoft Active Directory (MS-AD)**

### Components Used

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

- **Cisco UCS 6454 Fabric Interconnect**
- **UCSM version 4.0(4k)**
- **Microsoft Active Directory (MS-AD)**

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

Lightweight Directory Access Protocol (LDAP) is one of the core protocols developed for directory services which securely manages users and their access rights to IT resources.

Most directory services still use LDAP today, although they can also use additional protocols like Kerberos, SAML, RADIUS, SMB, Oauth, and others.

## Configure

### Before You Begin

Log into Cisco UCS Manager GUI as an administrative user.

### Create a Local Authentication Domain

**Step 1.** In the Navigation pane, click the Admin tab.

**Step 2.** On the Admin tab, expand All > User Management > Authentication

The screenshot shows the Cisco UCS Manager GUI. The left navigation pane is expanded to 'Authentication Domains'. The main content area shows a table of existing authentication domains. The table has the following data:

Name	Realm	Provider Group	Web Session Refresh Period	Web Session Timeout
LDAP	ldap	mxsv	600	7200
Local	local		600	7200
radius	radius		7200	8000
Tacacs	tacacs	Test	600	7200

At the bottom of the table, there is an 'Add' button circled in red.

**Step 3.** Right-click Authentication Domains and select Create a Domain.

**Step 4.** For the Name field, type Local.

**Step 5.** For the Realm, click the Local radio button.

General	Events
<b>Actions</b>	<b>Properties</b>
Delete	Name : Local
	Web Session Refresh Period (sec) : 600
	Web Session Timeout (sec) : 7200
	Realm : <input checked="" type="radio"/> Local <input type="radio"/> Radius <input type="radio"/> Tacacs <input type="radio"/> Ldap
<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

**Step 6.** Click ok.

## Create an LDAP Provider

This sample configuration does not include steps to configure LDAP with SSL.

**Step 1.** In the Navigation pane, click the Admin tab.

**Step 2.** On the Admin tab, expand All > User Management > LDAP.

**Step 3.** In the Work pane, click the General tab.

**Step 4.** In the Actions area, click Create LDAP Provider

The screenshot shows the 'Create LDAP Provider' wizard in the 'General' tab. The 'Actions' list on the left includes 'Create LDAP Provider', 'Create LDAP Provider Group', and 'Create LDAP Group Map'. The 'Properties' section on the right contains the following fields:

- Timeout : 30
- Attribute : [Empty field]
- Base DN : DC=mxsvlab,DC=com
- Filter : sAMAccountName=Suserid

**Step 5.** In the Create LDAP Provider page of the wizard, input the appropriate information:

- In the **Hostname** field, type the IP address or hostname of the AD server.
- In the **Order** field, accept the **lowest-available** default.
- In the **BindDN** field, copy and paste the BindDN from your AD configuration.

For this sample configuration, the BindDN value is **CN=ucsbinding,OU=CiscoUCS,DC=mxsvlab,DC=com**.

- In the **BaseDN** field, copy and paste the BaseDN from your AD configuration. For this sample configuration, the BaseDN value is **DC=mxsvlab,DC=com**.

- Leave the **Enable SSL** check box unchecked.
- In the **Port** field, accept the 389 default.
- In the **Filter** field, copy and paste the filter attribute from your AD configuration.

Cisco UCS uses the filter value to determine if the user name (provided on the logon screen by Cisco UCS Manager) is in AD.

For this sample configuration, the filter value is **sAMAccountName=\$userid**, where \$userid is the user name to enter in the Cisco UCS Manager login screen.

- Leave the **Attribute** field blank.
- In the **Password** field, type the password for the ucsbind account configured in AD.

If you need to go back into the **Create LDAP Provider** wizard to reset the password, do not be alarmed if the password field is blank.

The **Set: yes** message that appears next to the password field indicates that a password has been set.

- In the **Confirm Password** field, retype the password for the ucsbind account configured in AD.
- In the **Timeout** field, accept the 30 default.
- In the **Vendor** field, select the radio button for **MS-AD** for Microsoft Active Directory.

**1** Create LDAP Provider

**2** LDAP Group Rule

**Create LDAP Provider**

Hostname/FQDN (or IP Address) : 10.31.123.60

Order : lowest-available

Bind DN : CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com

Base DN : DC=mxsvlab,DC=com

Port : 389

Enable SSL :

Filter : sAMAccountName=\$userid

Attribute :

Password :

Confirm Password :

Timeout : 30

Vendor :  Open Ldap  MS AD

< Prev Next > Finish Cancel

**Step 6.** Click **Next**

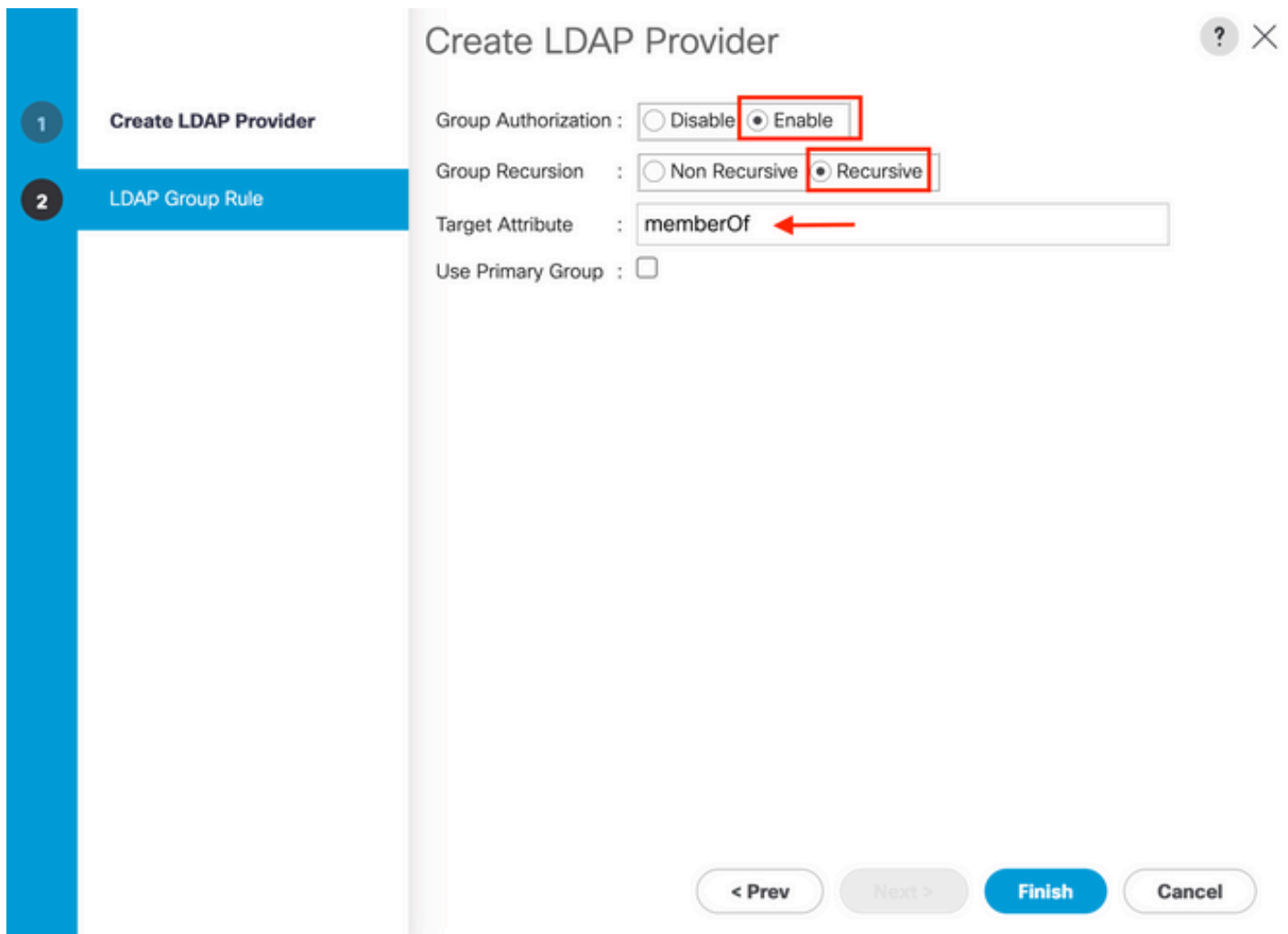
## LDAP Group Rule configuration

**Step 1.** On the LDAP Group Rule page of the wizard, complete the next fields:

- For the **Group Authentication** field, click the **Enable** radio button.
- For the **Group Recursion** field, click the **Recursive** radio button. This allows the system to continue the search down, level by level, until it finds a user.

If the **Group Recursion** is set to **Non-Recursive**, it limits UCS to a search of the first level, even if the search does not locate a qualified user.

- In the **Target Attribute** field, accept the **memberOf** default.



The screenshot shows the 'Create LDAP Provider' wizard configuration page. On the left, a navigation pane highlights step 2, 'LDAP Group Rule'. The main configuration area includes the following fields:

- Group Authorization:** Radio buttons for 'Disable' and 'Enable'. The 'Enable' option is selected and highlighted with a red box.
- Group Recursion:** Radio buttons for 'Non Recursive' and 'Recursive'. The 'Recursive' option is selected and highlighted with a red box.
- Target Attribute:** A text input field containing 'memberOf', with a red arrow pointing to the text.
- Use Primary Group:** An unchecked checkbox.

At the bottom of the configuration area, there are four buttons: '< Prev', 'Next >', 'Finish', and 'Cancel'. The 'Finish' button is highlighted in blue.

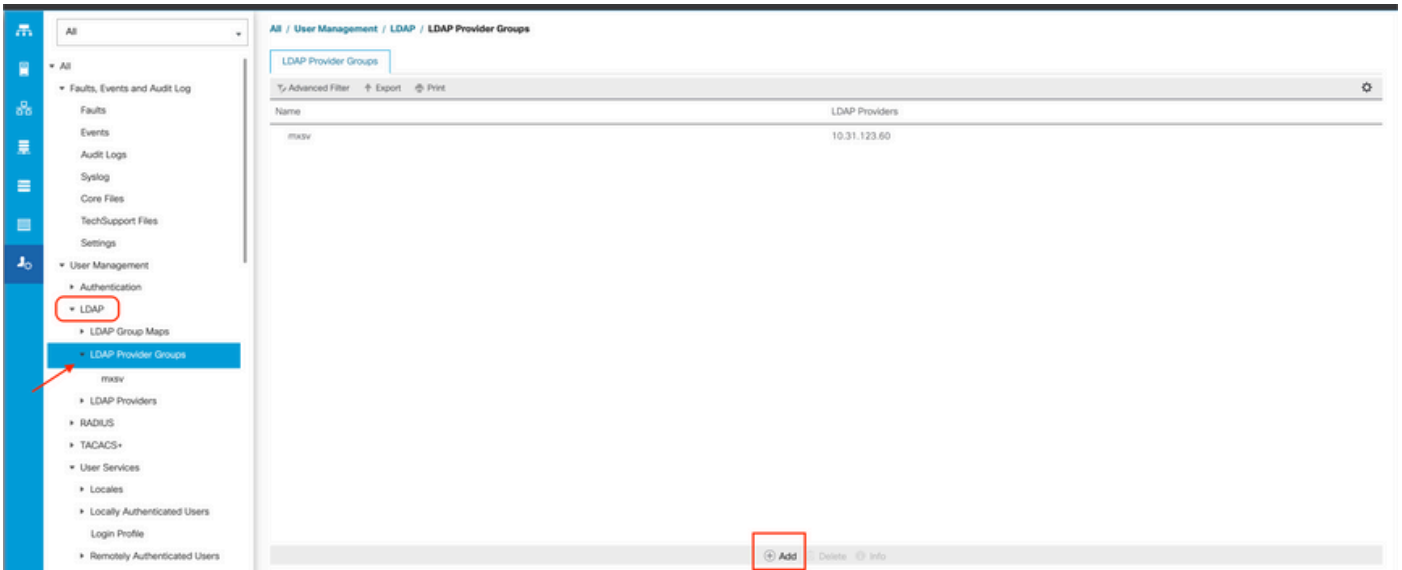
**Step 2.** Click in **Finish**.

**Note:** In a real-world scenario, you would most likely have multiple LDAP providers. For multiple LDAP providers, you would repeat the steps to configure the LDAP Group Rule for each LDAP provider. However, in this sample configuration, there is only one LDAP provider, so this is not necessary.

The IP address for the AD server is displayed in the Navigation pane under **LDAP > LDAP Providers**.

# Create an LDAP Provider Group

**Step 1.** In the Navigation pane, right-click **LDAP Provider Groups** and select **Create LDAP Provider Group**.



**Step 2.** In the **Create LDAP Provider Group** dialog box, fill the information appropriately:

- In the **Name** field, enter a unique name for the group such as **LDAP Providers**.
- In the **LDAP Providers** table, choose the IP address for your AD server.
- Click the **>>** button to add the AD server to your **Included Providers** table.

## Create LDAP Provider Group

Name : mxsv

LDAP Providers		
Hostname	Bind DN	Port
10.31.123....	CN=ucsbind,...	389

>>  
<<

Included Providers	
Name	Order
No data available	

OK Cancel

**Step 3.** Click **OK**.

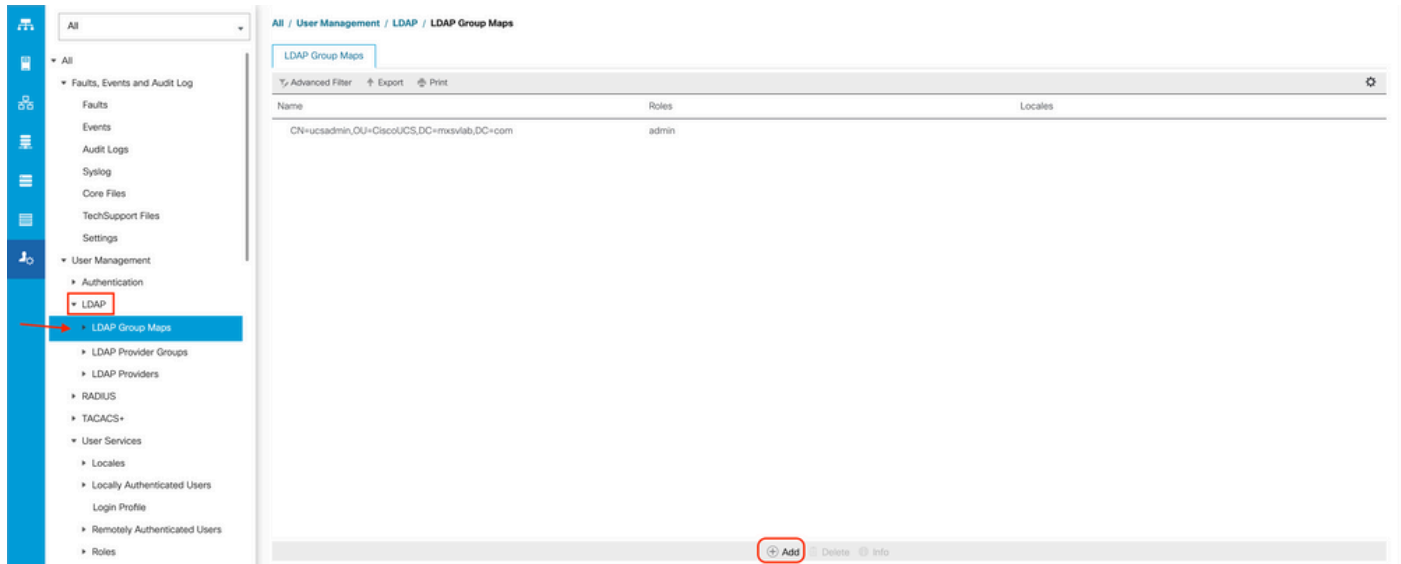
Your provider group appears in the **LDAP Provider Groups** folder.

## Create an LDAP Group Map

**Step 1.** In the Navigation pane, click the **Admintab**.

**Step 2.** On the **Admin** tab, expand **All > User Management > LDAP**.

**Step 3.** In the **Work** pane, click **Create LDAP Group Map**.



**Step 4.** In the **Create LDAP Group Map** dialog box, fill the information appropriately:

- In the **LDAP Group DN** field, copy and paste the value that you have in the AD server configuration section for your LDAP group.

The LDAP Group DN value requested in this step maps to the distinguished name for each of the groups you created in AD under UCS Groups.

For this reason, the Group DN value entered in Cisco UCS Manager must match exactly with the Group DN value in the AD server.

In this sample configuration, this value is **CN=ucsadmin,OU=CiscoUCS,DC=sampldesign,DC=com**.

- In the **Roles** table, click the **Admin** check box and click **OK**.

Click the check box for a role indicates that you want to assign admin privileges to all users who are included in the group map.

# Create LDAP Group Map



LDAP Group DN : CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com

## Roles

- aaa
- admin ←
- facility-manager
- network
- OnlyKVM
- operations
- read-only
- server-compute
- server-equipment
- server-profile
- server-security
- stats
- storage

## Locales

- JaviTest
- JosueLoc
- Test

OK

Cancel

**Step 5.** Create new LDAP group maps (use the information you recorded earlier from AD) for each of the remains roles in the AD server that you want to test.

**Next:** Create your LDAP authentication domain.

## Create an LDAP Authentication Domain

**Step 1.** On the Admin tab, expand All > User Management > Authentication

**Step 2.** Right-click **Authentication** Authentication Domains and select **Create a Domain**.



Name	Realm	Provider Group	Web Session Refresh Period	Web Session Timeout
LDAP	ldap	mxsv	600	7200
Local	local		600	7200
radius	radius		7200	8000
Tacacs	tacacs	Test	600	7200

**Step 3.** In the **Create a Domain** dialog box, complete the next:

- In the **Name** field, type a name for your domain such as LDAP.
- In the **Realm** area, click the **Ldap** radio button.
- From the **Provider Group** drop-down list, select the **LDAP Provider Group** previously created and click **OK**.

### Properties for: LDAP ✕

General

Events

**Actions**

Delete

**Properties**

Name : **LDAP**

Web Session Refresh Period (sec) :

Web Session Timeout (sec) :

Realm :  Local  Radius  Tacacs  Ldap

Provider Group :

The authentication domain appears under **Authentication Domains**.

## Verify

**Ping to LDAP Provider IP or FQDN:**

```
UCS-AS-MXC-P25-02-B-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

```
UCS-AS-MXC-P25-02-B-A(local-mgmt)# ping 10.31.123.60
PING 10.31.123.60 (10.31.123.60) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.60: icmp_seq=1 ttl=128 time=0.302 ms
64 bytes from 10.31.123.60: icmp_seq=2 ttl=128 time=0.347 ms
64 bytes from 10.31.123.60: icmp_seq=3 ttl=128 time=0.408 ms
```

To test authentication from NX-OS, use the `test aaa` command (only available from NXOS).

We validate the configuration of our server:

```
ucs(nxos)# test aaa server ldap <LDAP-server-IP-address or FQDN> <username> <password>
```

```
[UCS-AS-MXC-P25-02-B-A# connect nxos
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
[UCS-AS-MXC-P25-02-B-A(nx-os)# test aaa server ldap 10.31.123.60 admin Cisco123
```

## Common LDAP Issues.

- Basic configuration.
- Wrong password or invalid characters.
- Wrong port or Filter field.

- No communication with our provider due to a Firewall or Proxy rule.
- FSM is not 100%.
- Certificate problems.

## Troubleshoot

### Verify UCSM LDAP configuration:

You must ensure that the UCSM has implemented the configuration successfully because the status of the **Finite State Machine (FSM)** is shown as 100% complete.

### To verify the configuration from the command line of our UCSM:

```
ucs # scope security
ucs /security# scope ldap
ucs /security/ldap# show configuration
[UCS-AS-MXC-P25-02-B-A /security # scope security
[UCS-AS-MXC-P25-02-B-A /security # scope security
[UCS-AS-MXC-P25-02-B-A /security # scope ldap
[UCS-AS-MXC-P25-02-B-A /security/ldap # show configuration
scope ldap
  enter auth-server-group mxsv
    enter server-ref 10.31.123.60
      set order 1
    exit
  exit
  enter ldap-group "CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com"
  exit
  enter server 10.31.123.60
    enter ldap-group-rule
      set authorization enable
      set member-of-attribute memberOf
      set traversal recursive
      set use-primary-group no
    exit
    set attribute ""
    set basedn "DC=mxsvlab,DC=com"
    set binddn "CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com"
    set filter ""
    set order 1
    set port 389
    set ssl no
    set timeout 30
    set vendor ms-ad
    ! set password
  exit
  set attribute ""
  set basedn "DC=mxsvlab,DC=com"
  set filter sAMAccountName=$userid
  set timeout 30
exit
UCS-AS-MXC-P25-02-B-A /security/ldap # █
```

```
ucs /security/ldap# show fsm status
```

```
[UCS-AS-MXC-P25-02-B-A /security/ldap # show fsm status
```

```
FSM 1:  
  Status: Nop  
  Previous Status: Update Ep Success  
  Timestamp: 2022-08-10T00:08:55.329  
  Try: 0  
  Progress (%): 100  
  Current Task:
```

To verify the configuration from the NXOS:

```
ucs# connect nxos  
ucs(nxos)# show ldap-server  
ucs(nxos)# show ldap-server groups
```

```

UCS-AS-MXC-P25-02-B-A# connect nxos
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-B-A(nx-os)# show ldap-server
  timeout : 30
  port : 0
  baseDN : DC=mxsvlab,DC=com
user profile attribute :
search filter : sAMAccountName=$userid
  use groups : 0
recurse groups : 0
group attribute : memberOf
  group map CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com:
    roles: admin
    locales:
total number of servers : 1

following LDAP servers are configured:
10.31.123.60:
  timeout: 30   port: 389   rootDN: CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com
  enable-ssl: false
  baseDN: DC=mxsvlab,DC=com
  user profile attribute:
  search filter:
  use groups: true
  recurse groups: true
  group attribute: memberOf
  vendor: MS AD
UCS-AS-MXC-P25-02-B-A(nx-os)# show ldap-server groups
total number of groups: 2

following LDAP server groups are configured:
group ldap:
  baseDN:
  user profile attribute:
  search filter:
  group membership attribute:
  server: 10.31.123.60 port: 389 timeout: 30
group mxsv:
  baseDN:
  user profile attribute:
  search filter:
  group membership attribute:
  server: 10.31.123.60 port: 389 timeout: 30

```

The most effective method to see errors is to enable our debug, with this output we can see the

groups, the connection, and the error message that prevents communication.

- Open an SSH session to FI and login as a local user and change to NX-OS CLI context and start the terminal monitor.

```
ucs # connect nxos
```

```
ucs(nxos)# terminal monitor
```

- Enable debug flags and verify the SSH session output to the log file.

```
ucs(nxos)# debug aaa all <<< not required, incase of debugging authentication problems
```

```
ucs(nxos)# debug aaa aaa-requests
```

```
ucs(nxos)# debug ldap all <<< not required, incase of debugging authentication problems.
```

```
ucs(nxos)# debug ldap aaa-request-lowlevel
```

```
ucs(nxos)# debug ldap aaa-request
```

```
UCS-AS-MXC-P25-02-B-A# connect nxos
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-B-A(nx-os)# terminal monitor
UCS-AS-MXC-P25-02-B-A(nx-os)# debug ldap all
UCS-AS-MXC-P25-02-B-A(nx-os)# debug aaa all
```

- Now open a new GUI or CLI session and attempt to log in as a remote ( LDAP ) user.
- Once you received a login failure message, turn off the debugs.

## Related Information

- [Technical Support & Documentation - Cisco Systems](#)

- [UCSM LDAP Sample Configuration](#)
- [Cisco UCS C Series GUI Configuration Guide](#)