

# Configurare LDAP in UCS Manager

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Crea un dominio di autenticazione locale](#)

[Crea un provider LDAP](#)

[Configurazione regola gruppo LDAP](#)

[Crea un gruppo di provider LDAP](#)

[Creare una mappa di gruppo LDAP](#)

[Crea un dominio di autenticazione LDAP](#)

[Verifica](#)

[Problemi LDAP comuni.](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## Introduzione

Questo documento descrive la configurazione per l'accesso remoto al server con il protocollo LDAP Unified Computing System Manager Domain (UCSM).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- **Unified Computing System Manager Domain (UCSM)**
- **Autenticazione locale e remota**
- **Lightweight Directory Access Protocol (LDAP)**
- **Microsoft Active Directory (MS-AD)**

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- **Cisco UCS 6454 Fabric Interconnect**

- UCSM versione 4.0(4k)
- Microsoft Active Directory (MS-AD)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

**Lightweight Directory Access Protocol (LDAP)** è uno dei protocolli di base sviluppati per i servizi di directory che gestisce in modo sicuro gli utenti e i relativi diritti di accesso alle risorse IT.

La maggior parte dei servizi di directory utilizza ancora il protocollo LDAP, anche se può utilizzare anche protocolli aggiuntivi come Kerberos, SAML, RADIUS, SMB, Oauth e altri.

## Configurazione

Operazioni preliminari

Accedi Cisco UCS Manager GUI come utente amministrativo.

Crea un dominio di autenticazione locale

Passaggio 1. Nella scheda **Navigation** fare clic sul pulsante **Admin** scheda.

Passaggio 2. Nella scheda **Admin**, espandere **All > User Management > Authentication**

The screenshot shows the Cisco UCS Manager GUI. On the left is a navigation menu with a tree structure. The 'Authentication Domains' option is highlighted with a red box. On the right, the main content area displays the 'Authentication Domains' configuration page. At the bottom of this page, the 'Add' button is highlighted with a red box.

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

Passaggio 3. Clic con il pulsante destro del mouse **Authentication Domains** e selezionare **Create a Domain**.

Passaggio 4. Per il **Name** campo, tipo **Local**.

Passaggio 5. Per il **Realm**, fare clic sul pulsante **Local** pulsante di opzione.

## Properties for: Local



**General** | Events

---

**Actions** | **Properties**

Delete

Name : **Local**

Web Session Refresh Period (sec) :

Web Session Timeout (sec) :

Realm :  Local  Radius  Tacacs  Ldap

OK Apply Cancel Help

Passaggio 6. Fare clic su **OK**.

## Crea un provider LDAP

In questa configurazione di esempio non è inclusa la procedura per configurare LDAP con SSL.

Passaggio 1. Nella scheda **Navigation** fare clic sul pulsante **Admin** scheda.

Passaggio 2. Nella scheda **Admin** , espandere **All > User Management > LDAP**.

Passaggio 3. Nella scheda **Work** fare clic sul pulsante **General** scheda.

Passaggio 4. Nella scheda **Actions** fare clic su **Create LDAP Provider**



Passaggio 5. Nella scheda **Create LDAP Provider** della procedura guidata, immettere le informazioni appropriate:

- Nella scheda **Hostname** digitare l'indirizzo IP o il nome host del server AD.
- Nella scheda **Order** , accettare il **lowest-available** predefinito.

- Nella scheda **BindDN** copiare e incollare BindDN dalla configurazione AD.

Per questa configurazione di esempio, il valore BindDN è CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com.

- Nella scheda **BaseDN** copiare e incollare il nome distinto base dalla configurazione AD.

Per questa configurazione di esempio, il valore BaseDN è DC=mxsvlab,DC=com.

- Lasciare **Enable SSL** deselezionata.
- Nella scheda **Port** accettare il valore predefinito 389.
- Nella scheda **Filter** , copiare e incollare l'attributo di filtro dalla configurazione AD.

Cisco UCS utilizza il valore del filtro per determinare se il nome utente (fornito nella schermata di accesso da **Cisco UCS Manager**) è in Active Directory.

Per questa configurazione di esempio, il valore del filtro è sAMAccountName=\$userid, dove \$useridis **user name** per accedere al **Cisco UCS Manager** schermata di accesso.

- Lasciare **Attribute** campo vuoto.
- Nella scheda **Password** digitare la password per l'account ucsbind configurato in Active Directory.

Se è necessario tornare al **Create LDAP Provider wizard** per reimpostare la password, non generare alcun avviso se il campo della password è vuoto.

OSPF (Open Shortest Path First) **Set: yes** il messaggio visualizzato accanto al campo della password indica che è stata impostata una password.

- Nella scheda **Confirm Password** digitare nuovamente la password per l'account ucsbind configurato in AD.
- Nella scheda **Timeout** , accettare il 30 valore predefinito.
- Nella scheda **Vendor** , selezionare il pulsante di opzione per MS-ADfor Microsoft Active Directory.

Passaggio 6. Fare clic su **Next**

## Configurazione regola gruppo LDAP

Passaggio 1. Nella scheda **LDAP Group Rule** della procedura guidata, completare i campi seguenti:

- Per il **Group Authentication** fare clic sul pulsante **Enable** pulsante di opzione.
- Per il **Group Recursion** fare clic sul pulsante **Recursive** pulsante di opzione.

In questo modo il sistema può continuare la ricerca verso il basso, livello per livello, fino a trovare un utente.

Se il **Group Recursion** è impostato su **Non-Recursive**, limita UCS a una ricerca di primo livello, anche se la ricerca non individua un utente qualificato.

- Nella scheda **Target Attribute** , accettare il **memberOf** predefinito.

1 Create LDAP Provider

2 LDAP Group Rule

### Create LDAP Provider

Group Authorization :  Disable  Enable

Group Recursion :  Non Recursive  Recursive

Target Attribute : memberOf

Use Primary Group :

< Prev Next > Finish Cancel

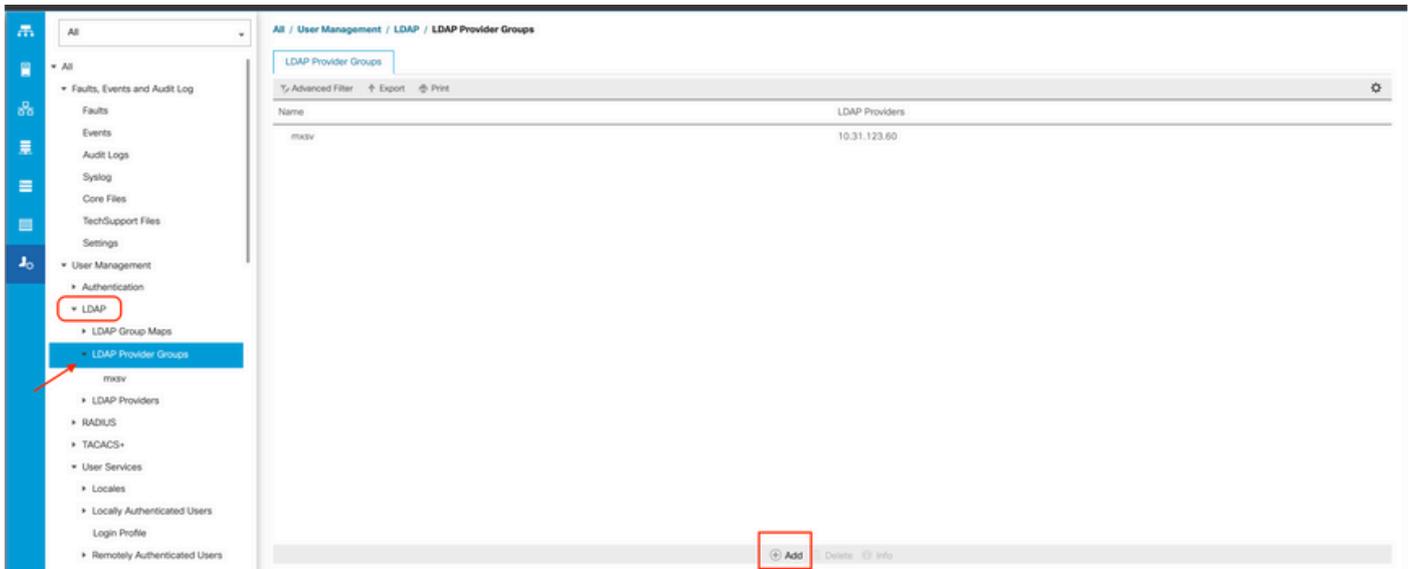
Passaggio 2. Fare clic su **Finish**.

Nota: in uno scenario reale, è molto probabile che siano presenti più provider LDAP. Per più provider LDAP, ripetere i passaggi per configurare la regola di gruppo LDAP per ogni provider LDAP. Tuttavia, in questa configurazione di esempio, esiste un solo provider LDAP, quindi questa operazione non è necessaria.

L'indirizzo IP del server AD viene visualizzato nel riquadro di spostamento sotto LDAP>LDAP Providers.

## Crea un gruppo di provider LDAP

Passaggio 1. Nel riquadro di spostamento fare clic con il pulsante destro del mouse **LDAP Provider Groups** e selezionare **Create LDAP Provider Group**.



Passaggio 2. Nella scheda **Create LDAP Provider Group** , compilare le informazioni in modo appropriato:

- Nella scheda **Name** immettere un nome univoco per il gruppo, ad esempio **LDAP Providers**.
- Nella scheda **LDAP Providers** scegliere l'indirizzo IP del server AD.
- Fare clic sul pulsante **>>** per aggiungere il server AD al **Included Providers** tabella.

## 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

Passaggio 3. Fare clic su OK.

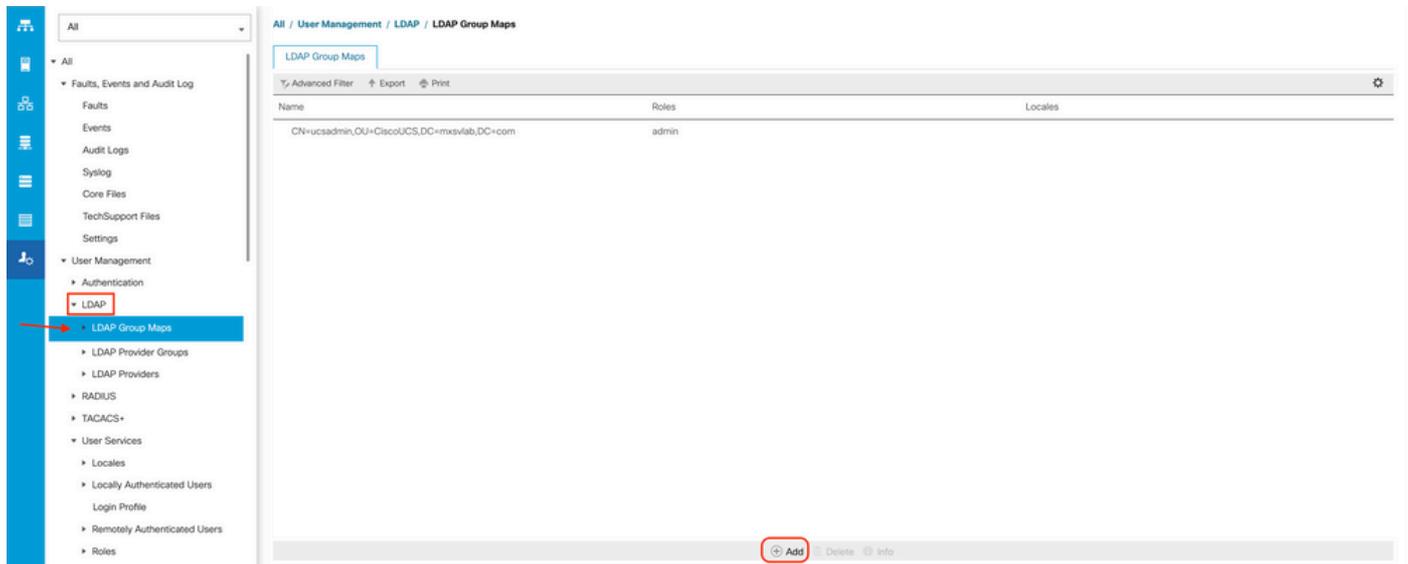
Il gruppo di provider viene visualizzato nel **LDAP Provider Groups** cartella.

Creare una mappa di gruppo LDAP

Passaggio 1. Nel riquadro di spostamento fare clic sul pulsante **Adminscheda**.

Passaggio 2. Nella scheda **Admin** , espandere **All > User Management > LDAP**.

Passaggio 3. Nel riquadro di lavoro fare clic su **Crea LDAP Group Map**.



Passaggio 4. Nella scheda **Create LDAP Group Map** , compilare le informazioni in modo appropriato:

- Nella scheda **LDAP Group DN** copiare e incollare il valore presente nella sezione **Configurazione server AD** per il gruppo LDAP.

Il valore del DN del gruppo LDAP richiesto in questo passaggio corrisponde al nome distinto di ciascuno dei gruppi creati in Active Directory in Gruppi UCS.

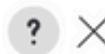
Per questo motivo, il valore del DN gruppo immesso in Cisco UCS Manager deve corrispondere esattamente al valore del DN gruppo nel server AD.

In questa configurazione di esempio, questo valore è **CN=ucsadmin,OU=CiscoUCS,DC=sampldesign,DC=com**.

- Nella scheda **Roles** fare clic sul pulsante **Admin** e fare clic su **OK**.

Fare clic sulla casella di controllo relativa a un ruolo per indicare che si desidera assegnare privilegi di amministratore a tutti gli utenti inclusi nella mappa del gruppo.

# 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

Passaggio 5. Creare nuove mappe di gruppi LDAP (utilizzare le informazioni registrate in precedenza da AD) per ognuno dei ruoli rimanenti nel server AD che si desidera verificare.

Successivo: creare il dominio di autenticazione LDAP.

## Crea un dominio di autenticazione LDAP

Passaggio 1. Nella scheda Admin , espandere All > User Management > Authentication

Passaggio 2. Clic con il pulsante destro del mouse Autenticazione Authentication Domains e selezionare Create a Domain.

Authentication Domains

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

Buttons: Add, Delete, Info

Passaggio 3. Nel &nbsp;Create a Domain completare il seguente passaggio:

- Nella scheda **Name** digitare un nome per il dominio, ad esempio LDAP.
- Nella scheda **Realm** fare clic sull'icona **Ldap** pulsante di opzione.
- Dal **Provider Group** selezionare la casella di controllo **LDAP Provider Group** creato in precedenza e fare clic su 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 :

OK
Apply
Cancel
Help

Il dominio di autenticazione viene visualizzato in **Authentication Domains**.

## Verifica

Esegui ping su **LDAP Provider IP** o **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
```

Per verificare l'autenticazione da NX-OS, utilizzare il `test aaa` (disponibile solo da NXOS).

Viene convalidata la configurazione del server:

```
<#root>
```

```
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
```

## Problemi LDAP comuni.

- Configurazione di base.
- Password o caratteri non validi.
- Porta o campo Filter errato.
- Nessuna comunicazione con il provider a causa di una regola del firewall o del proxy.
- Gli FSM non sono al 100%.
- Problemi relativi ai certificati.

## Risoluzione dei problemi

Verificare la configurazione LDAP UCSM:

È necessario verificare che UCSM abbia implementato la configurazione correttamente perché lo stato **Finite State Machine (FSM)** viene visualizzato come completato al 100%.

Per verificare la configurazione dalla riga di comando del modulo UCSM:

```
<#root>
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 # █
```

```
<#root>
```

```
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:
```

Per verificare la configurazione da NXOS:

```
<#root>
```

```
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
```

Il metodo più efficace per visualizzare gli errori è quello di abilitare il debug. Con questo output è possibile visualizzare i gruppi, la connessione e il messaggio di errore che impedisce la comunicazione.

- Aprire una sessione SSH su FI e accedere come utente locale, modificare il contesto CLI di NX-OS e avviare il terminal monitor.

```
ucs # connect nxos
```

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

- Abilitare i flag di debug e verificare l'output della sessione SSH nel file di log.

```
<#root>
```

```
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 ←
```

- Aprire una nuova sessione GUI o CLI e tentare di accedere come utente remoto ( LDAP ).
- Dopo aver ricevuto un messaggio di accesso non riuscito, disattivare i debug.

## Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems](#)
- [Configurazione di esempio per LDAP UCSM](#)
- [Cisco UCS serie C GUI Configuration Guide](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).