



Managing User Accounts

This chapter includes the following sections:

- [Configuring Local Users, on page 1](#)
- [Disabling Strong Password, on page 3](#)
- [Password Expiry, on page 4](#)
- [Configuring Password Expiry for Users, on page 5](#)
- [LDAP Servers, on page 6](#)
- [Configuring the LDAP Server, on page 6](#)
- [Configuring LDAP in Cisco IMC, on page 7](#)
- [Configuring LDAP Groups in Cisco IMC, on page 9](#)
- [Configuring Nested Group Search Depth in LDAP Groups, on page 11](#)
- [LDAP Certificates Overview, on page 12](#)
- [Setting User Search Precedence, on page 18](#)
- [Viewing User Sessions, on page 18](#)
- [Terminating a User Session, on page 19](#)

Configuring Local Users

Before you begin

You must log in as a user with admin privileges to configure or modify local user accounts.

Procedure

	Command or Action	Purpose
Step 1	Server# scope user <i>usernumber</i>	Enters user command mode for user number <i>usernumber</i> .
Step 2	Server /user # set enabled { yes no }	Enables or disables the user account on the Cisco IMC.
Step 3	Server /user # set name <i>username</i>	Specifies the username for the user.
Step 4	Server /user # set password	You are prompted to enter the password twice.

	Command or Action	Purpose
		<p>Note When strong password is enabled, you must follow these guidelines while setting a password:</p> <ul style="list-style-type: none"> • The password must have a minimum of 8 and a maximum of 14 characters. • The password must not contain the User's Name. • The password must contain characters from three of the following four categories: <ul style="list-style-type: none"> • English uppercase characters (A through Z) • English lowercase characters (a through z) • Base 10 digits (0 through 9) • Non-alphabetic characters (!, @, #, \$, %, ^, &, *, -, _, +, =) <p>when strong password is disabled, you can set a password using characters of your choice (alphanumeric, special characters, or integers) within the range 1-20.</p>
Step 5	Server /user # set role { readonly user admin }	<p>Specifies the role assigned to the user. The roles are as follows:</p> <ul style="list-style-type: none"> • readonly—This user can view information but cannot make any changes. • user—This user can do the following: <ul style="list-style-type: none"> • View all information • Manage the power control options such as power on, power cycle, and power off • Launch the KVM console and virtual media • Clear all logs • Toggle the locator LED

	Command or Action	Purpose
		<ul style="list-style-type: none"> • Set the time zone • Ping an IP address • admin—This user can perform all actions available through the GUI, CLI, and IPMI.
Step 6	Server /user # commit	Commits the transaction to the system configuration.

Example

This example configures user 5 as an admin:

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name john
Server /user *# set password
Warning:
Strong Password Policy is enabled!

For CIMC protection your password must meet the following requirements:
  The password must have a minimum of 8 and a maximum of 14 characters.
  The password must not contain the User's Name.
  The password must contain characters from three of the following four categories.
    English uppercase characters (A through Z)
    English lowercase characters (a through z)
    Base 10 digits (0 through 9)

Please enter password:
Please confirm password:
Server /user *# set role readonly
Server /user *# commit
Server /user # show
User  Name                Role      Enabled
-----
5     john                    readonly yes
```

Disabling Strong Password

The Cisco IMC now implements a strong password policy wherein you are required to follow guidelines and set a strong password when you first log on to the server for the first time. The Cisco IMC CLI provides you option which allows you to disable the strong password policy and set a password of your choice by ignoring the guidelines. Once you disable the strong password, an Enable Strong Password button is displayed. By default, the strong password policy is enabled.

Before you begin

You must log in as a user with admin privileges to perform this action.

Procedure

	Command or Action	Purpose
Step 1	Server# scope user-policy	Enters user policy command mode.
Step 2	Server /user-policy # set password-policy { enabled disabled }	At the confirmation prompt, enter y to complete the action or n to cancel the action. Enables or disables the strong password.
Step 3	Server /user-policy # commit	Commits the transaction to the system configuration.

Example

This example shows how to disable strong password:

```
Server# scope user-policy
Server /user-policy # set password-policy disabled
Warning: Strong password policy is being disabled.
Do you wish to continue? [y/N] y
Server /user-policy *# commit
Server /user-policy #
```

Password Expiry

You can set a shelf life for a password, after which it expires. As an administrator, you can set this time in days. This configuration would be common to all users. Upon password expiry, the user is notified on login and would not be allowed to login unless the password is reset.

**Note**

When you downgrade to an older database, existing users are deleted. The database returns to default settings. Previously configured users are cleared and the database is empty, that is, the database has the default username - 'admin' and password - 'password'. Since the server is left with the default user database, the change default credential feature is enabled. This means that when the 'admin' user logs on to the database for the first time after a downgrade, the user must mandatorily change the default credential.

Password Set Time

A 'Password set time' is configured for every existing user, to the time when the migration or upgrade occurred. For new users (users created after an upgrade), the Password Set time is configured to the time when the user was created, and the password is set. For users in general (new and existing), the Password Set Time is updated whenever the password is changed.

Configuring Password Expiry for Users

Procedure

	Command or Action	Purpose
Step 1	Server # scope user-policy	Enters the user policy command mode.
Step 2	Server /user-policy # scope password-expiration	Enters the password expiration command mode.
Step 3	Server /user-policy/password-expiration # set password-expiry-duration <i>integer in the range 0-3650</i>	The time period that you can set for the existing password to expire (from the time you set a new password or modify an existing one). The range is between 0 to 3650 days. Entering 0 disables this option.
Step 4	Server /user-policy/password-expiration * # set notification-period <i>integer in the range 0-15</i>	Notifies the time by when the password expires. Enter a value between 0 to 15 days. Entering 0 disables this option.
Step 5	Server /user-policy/password-expiration * # set grace-period <i>integer in the range 0-5</i>	Time period till when the existing password can still be used, after it expires. Enter a value between 0 to 5 days. Entering 0 disables this option.
Step 6	Server /user-policy/password-expiration * # set password-history <i>integer in the range 0-5</i>	The number of occurrences when a password was entered. When this is enabled, you cannot repeat a password. Enter a value between 0 to 5. Entering 0 disables this option.
Step 7	Server /user-policy/password-expiration * # commit	Commits the transactions.
Step 8	(Optional) Server /user-policy/password-expiration # show detail	Shows the password expiration details.
Step 9	(Optional) Server /user-policy/password-expiration # restore	At the confirmation prompt, enter yes to restore the password expiry settings to default values.

Example

This example sets the password expiration and restore the settings to default vales:

```
Server # scope user-policy
Server /user-policy # scope password-expiration
Server /user-policy/password-expiration # set password-expiry-duration 5
Server /user-policy/password-expiration * # set notification-period 2
Server /user-policy/password-expiration * # set grace-period 1
Server /user-policy/password-expiration * # set password-history 4
Server /user-policy/password-expiration * # commit
Server /user-policy/password-expiration # show detail
```

```

Password expiration parameters:
Valid password duration: 5
Number of stored old passwords: 4
Notification period: 2
Grace period: 1
Server /user-policy/password-expiration #
Restoring the password expiry parameters to default values:
Server /user-policy/password-expiration # restoreAre you sure you want to restore
User password expiration parameters to defaults?
Please enter 'yes' to confirm:yes
Server /user-policy/password-expiration #

```

LDAP Servers

Cisco IMC supports directory services that organize information in a directory, and manage access to this information. Cisco IMC supports Lightweight Directory Access Protocol (LDAP), which stores and maintains directory information in a network. In addition, Cisco IMC supports Microsoft Active Directory (AD). Active Directory is a technology that provides a variety of network services including LDAP-like directory services, Kerberos-based authentication, and DNS-based naming. The Cisco IMC utilizes the Kerberos-based authentication service of LDAP.

When LDAP is enabled in the Cisco IMC, user authentication and role authorization is performed by the LDAP server for user accounts not found in the local user database. The LDAP user authentication format is `username@domain.com`.

By enabling encryption in the configuration of Active Directory on the server, you can require the server to encrypt data sent to the LDAP server.

Configuring the LDAP Server

The Cisco IMC can be configured to use LDAP for user authentication and authorization. To use LDAP, configure users with an attribute that holds the user role and locale information for the Cisco IMC. You can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales or you can modify the LDAP schema to add a new custom attribute, such as the `CiscoAVPair` attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1.



Important

For more information about altering the schema, see the article at <http://technet.microsoft.com/en-us/library/bb727064.aspx>.



Note

This example creates a custom attribute named `CiscoAVPair`, but you can also use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales.

If you are using Group Authorization on the Cisco IMC LDAP configuration, then you can skip Steps 1-4 and perform the steps listed in the *Configuring LDAP Settings and Group Authorization in Cisco IMC* section.

The following steps must be performed on the LDAP server.

Procedure

Step 1 Ensure that the LDAP schema snap-in is installed.

Step 2 Using the schema snap-in, add a new attribute with the following properties:

Properties	Value
Common Name	<code>CiscoAVPair</code>
LDAP Display Name	<code>CiscoAVPair</code>
Unique X500 Object ID	<code>1.3.6.1.4.1.9.287247.1</code>
Description	<code>CiscoAVPair</code>
Syntax	<code>Case Sensitive String</code>

Step 3 Add the CiscoAVPair attribute to the user class using the snap-in:

- Expand the **Classes** node in the left pane and type **U** to select the user class.
- Click the **Attributes** tab and click **Add**.
- Type **C** to select the CiscoAVPair attribute.
- Click **OK**.

Step 4 Add the following user role values to the CiscoAVPair attribute, for the users that you want to have access to Cisco IMC:

Role	CiscoAVPair Attribute Value
admin	<code>shell:roles="admin"</code>
user	<code>shell:roles="user"</code>
read-only	<code>shell:roles="read-only"</code>

Note For more information about adding values to attributes, see the article at <http://technet.microsoft.com/en-us/library/bb727064.aspx>.

What to do next

Use the Cisco IMC to configure the LDAP server.

Configuring LDAP in Cisco IMC

Configure LDAP in Cisco IMC when you want to use an LDAP server for local user authentication and authorization.

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode.
Step 2	Server /ldap # set enabled {yes no}	Enables or disables LDAP security. When enabled, user authentication and role authorization is performed by LDAP for user accounts not found in the local user database.
Step 3	Server /ldap # set domain <i>LDAP domain name</i>	Specifies an LDAP domain name.
Step 4	Server /ldap # set timeout <i>seconds</i>	Specifies the number of seconds the Cisco IMC waits until the LDAP search operation times out. The value must be between 0 and 1800 seconds.
Step 5	Server /ldap # set encrypted {yes no}	If encryption is enabled, the server encrypts all information sent to AD.
Step 6	Server /ldap # set base-dn <i>domain-name</i>	Specifies the Base DN that is searched on the LDAP server.
Step 7	Server /ldap # set attribute <i>name</i>	<p>Specify an LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name.</p> <p>You can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales or you can create a custom attribute, such as the CiscoAVPair attribute, which has the following attribute ID:</p> <p>1.3.6.1.4.1.9.287247.1</p> <p>Note If you do not specify this property, user access is denied.</p>
Step 8	Server /ldap # set filter-attribute	Specifies the account name attribute. If Active Directory is used, then specify sAMAccountName for this field.
Step 9	Server /ldap # commit	Commits the transaction to the system configuration.
Step 10	Server /ldap # show [detail]	(Optional) Displays the LDAP configuration.

Example

This example configures LDAP using the CiscoAVPair attribute:

```

Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set encrypted yes
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# commit
Server /ldap # show detail
LDAP Settings:
  Enabled: yes
  Encrypted: yes
  Domain: sample-domain
  BaseDN: example.com
  Timeout: 60
  Filter-Attribute: sAMAccountName
  Attribute: CiscoAvPair
Server /ldap #

```

What to do next

If you want to use LDAP groups for group authorization, see *Configuring LDAP Groups in Cisco IMC*.

Configuring LDAP Groups in Cisco IMC



Note When Active Directory (AD) group authorization is enabled and configured, user authentication is also done on the group level for users that are not found in the local user database or who are not individually authorized to use Cisco IMC in the Active Directory.

Before you begin

- You must log in as a user with admin privileges to perform this task.
- Active Directory (or LDAP) must be enabled and configured.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode for AD configuration.
Step 2	Server /ldap# scope ldap-group-rule	Enters the LDAP group rules command mode for AD configuration.

	Command or Action	Purpose
Step 3	Server /ldap/ldap-group-rule # set group-auth {yes no}	Enables or disables LDAP group authorization.
Step 4	Server /ldap # scope role-group <i>index</i>	Selects one of the available group profiles for configuration, where <i>index</i> is a number between 1 and 28.
Step 5	Server /ldap/role-group # set name <i>group-name</i>	Specifies the name of the group in the AD database that is authorized to access the server.
Step 6	Server /ldap/role-group # set domain <i>domain-name</i>	Specifies the AD domain the group must reside in.
Step 7	Server /ldap/role-group # set role {admin user readonly}	Specifies the permission level (role) assigned to all users in this AD group. This can be one of the following: <ul style="list-style-type: none"> • admin—The user can perform all actions available. • user—The user can perform the following tasks: <ul style="list-style-type: none"> • View all information • Manage the power control options such as power on, power cycle, and power off • Launch the KVM console and virtual media • Clear all logs • Toggle the locator LED • readonly—The user can view information but cannot make any changes.
Step 8	Server /ldap/role-group # commit	Commits the transaction to the system configuration.

Example

This example shows how to configure LDAP group authorization:

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-auth yes
Server /ldap *# scope role-group 5
Server /ldap/role-group # set name Training
Server /ldap/role-group* # set domain example.com
Server /ldap/role-group* # set role readonly
Server /ldap/role-group* # commit
```

```
ucs-c250-M2 /ldap # show role-group
Group  Group Name      Domain Name      Assigned Role
-----
1      (n/a)             (n/a)           admin
2      (n/a)             (n/a)           user
3      (n/a)             (n/a)           readonly
4      (n/a)             (n/a)           (n/a)
5      Training          example.com     readonly

Server /ldap/role-group #
```

Configuring Nested Group Search Depth in LDAP Groups

You can search for an LDAP group nested within another defined group in an LDAP group map.

- You must log in as a user with admin privileges to perform this task.
- Active Directory (or LDAP) must be enabled and configured.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode for AD configuration.
Step 2	Server /ldap# scope ldap-group-rule	Enters the LDAP group rules command mode for AD configuration.
Step 3	Server /ldap/ldap-group-rule # set group-search-depth value	Enables search for a nested LDAP group.
Step 4	Server /ldap/role-group-rule # commit	Commits the transaction to the system configuration.

Example

This example shows how to search for run a search for an LDAP group nested within another defined group.

```
Server# scope ldap
Server /ldap # scope ldap-group-rule
Server /ldap/ldap-group-rule # set group-search-depth 10
Server /ldap/role-group-rule* # commit
Server /ldap/role-group-rule # show detail
Group rules for LDAP:
  Group search attribute: memberOf
  Enable Group Authorization: yes
  Nested group search depth: 10
Server/ldap/ldap-group-rule #
```

LDAP Certificates Overview

Cisco C-series servers allow an LDAP client to validate a directory server certificate against an installed CA certificate or chained CA certificate during an LDAP binding step. This feature is introduced in the event where anyone can duplicate a directory server for user authentication and cause a security breach due to the inability to enter a trusted point or chained certificate into the Cisco IMC for remote user authentication.

An LDAP client needs a new configuration option to validate the directory server certificate during the encrypted TLS/SSL communication.

Exporting LDAP CA Certificate

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode.
Step 2	Server# /ldap scope binding-certificate	Enters the LDAP CA certificate binding command mode.
Step 3	Server /ldap/binding-certificate # export-ca-certificate remote-protocol IP <i>Adderss LDAP CA Certificate file</i>	Specifies the protocol to connect to the remote server. It can be of the following types: <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP

	Command or Action	Purpose
		<p>Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.</p> <p>If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p> <p>Initiates the export of the certificate.</p>

Example

This example exports the LDAP certificate:

```

Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # export-ca-certificate tftp 172.22.141.66 test.csv
Initiating Export
  % Total    % Received % Xferd  Average Speed   Time    Time       Time  Current
   Dload  Upload   Total             Spent    Left     Speed
100 1262    0    0  100 1262      0  1244  0:00:01  0:00:01  ---:--:-- 1653
100 1262    0    0  100 1262      0  1237  0:00:01  0:00:01  ---:--:-- 1237
LDAP CA Certificate is exported successfully
Server /ldap/binding-certificate #
    
```

Downloading LDAP CA Certificate Content by Copying Content

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode.

	Command or Action	Purpose
Step 2	Server# /ldap scope binding-certificate	Enters the LDAP CA certificate binding command mode.
Step 3	Server# /ldap/binding-certificate set enabled {yes no}	Enables or disables LDAP CA certificate binding.
Step 4	Server /ldap/binding-certificate* # commit	Commits the transaction to the system configuration.
Step 5	Server /ldap/binding-certificate # paste-ca-certificate	Prompts you to paste the certificate content.
Step 6	Paste the certificate content and press CTRL+D.	Confirmation prompt appears.
Step 7	At the confirmation prompt, enter y.	This begins the download of the LDAP CA certificate.

Example

This example downloads the LDAP certificate:

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # set enabled yes
Server /ldap/binding-certificate *# commit
Server /ldap/binding-certificate # show detail
LDAP binding with Certificate:
  Enabled: yes
Server /ldap/binding-certificate # paste-ca-certificate
  Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIQV06yJcJPAYNO8Cp+FYQtTjANBgkqhkiG9w0BAQsFADBO
MRIwEAYKCZImiZPyLQGGRYCaW4xGzAZBgoJkiaJk/IsZAEZFgsOT0JKUkEySkhC
UTeBMBkGAlUEAxMSV01OLTRPQkpSQTJKSEJRLUNBMB4XDTE2MDIyNTE3MDczNl0X
DTIxDIyNTE3MTczM1owTjESMBAGCgmSJomT8ixkARkWAmluMRswGQYKCZImiZPy
LQGGRYLnE9CSlJBMkpIQ1ExGzAZBgnVBAMTEldJTi00T0JKUkEySkhCUS1DQTCC
ASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMM2cdgmrPTkZe4K2zI+EbeZ
mfQnjfiUz8Oiy97w81C/2S4qK46T+fnX13rXe8vvVHA05wgPDVQTGS4n1F46A6Ba
FK+krKcIgfRQB1gnF74qs/ln1YtKHNBjrvG5KyeWFrA7So6Mi2XEw8w/zMPL0d8T
b+LM1YnhnuXA9G8gVCJ/iUhXfMpB20L8sv30Mek7bw8x2cxJYTUJAviVIRjSwU5j
fO3WKttRuyFpeOIi00weklpF0+8D3Z9mBinoTbL2p10U32am6wTI+8WmtJ+8W68v
jH4Y8YBY/kzMHdpwjpdZkC5pe9Bcm0rL9xKoIu6X0ksNEssoGnepFyNaH3t8vnMC
AwEAAANRME8wCwYDVR0PBAQDAGGMA8GA1UdEWEB/wQFMAMBAF8wHQYDVR0OBBYE
FBAUu1HTAWBT1OBz8IgaEzXsfCcsMBAGCSsGAQQBgjcVAQQDAQEAMA0GCSqGSIB3
DQEBcwUAA4IBAQAzUMZr+0r1dWkVfFNbd7lu8tQbAEJf/A7PIKnJGNouq8moAGs4
pMndoxdpNGZhyCWDWX3GwdeFlHqZHhb38gGQ9yluOpIK7tgQufZmeCBH6T7Tzq/w
Dq+TMFGIjXF84xw3N665y4ePgUcUI7e/6aBgcGkGeUYodBptExe28tQyeuYwD4Zj
nLuZKkT+I4PAYyGcXqDGsvfRHDPgneb3R+GeonOf4ED/0tn5PLSL9kHb9qkHu/V
dO3/HmKVzUhl0TDBuAMq/wES2WZAWHGr3hBc4nWQNJZWEMOKDpYZVK/GhBmNF+xi
eRcFqgh64oEmH9qAp0caGS1e7UyYan+LtpRE
-----END CERTIFICATE-----
CTRL+D
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]
y
Server /ldap/binding-certificate #
```

Downloading LDAP CA Certificate Using Remote Server

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode.
Step 2	Server# /ldap scope binding-certificate	Enters the LDAP CA certificate binding command mode.
Step 3	Server# /ldap/binding-certificate set enabled {yes no}	Enables or disables LDAP CA certificate binding.
Step 4	Server /ldap/binding-certificate* # commit	Commits the transaction to the system configuration.
Step 5	Server /ldap/binding-certificate # download-ca-certificate <i>remote-protocol IP Address LDAP CA Certificate file</i>	<p>Specifies the protocol to connect to the remote server. It can be of the following types:</p> <ul style="list-style-type: none"> • TFTP • FTP • SFTP • SCP • HTTP <p>Note The Cisco UCS C-Series server now supports fingerprint confirmation of the server when you update firmware through a remote server. This option is available only if you choose SCP or SFTP as the remote server type.</p> <p>If you chose SCP or SFTP as the remote server type while performing this action, a prompt with the message Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue? Click y or n depending on the authenticity of the server fingerprint.</p> <p>The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to.</p>

	Command or Action	Purpose
Step 6	At the confirmation prompt, enter y .	This begins the download of the LDAP CA certificate.

Example

This example downloads the LDAP certificate:

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # set enabled yes
Server /ldap/binding-certificate *# commit
Server /ldap/binding-certificate # show detail
LDAP binding with Certificate:
  Enabled: yes
Server /ldap/binding-certificate # download-ca-certificate tftp 172.22.141.66
new_com_chain.cer
  % Total      % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left    Speed
100 1282 100 1282    0     0  1247      0  0:00:01  0:00:01  --:--:-- 1635
100 1282 100 1282    0     0  1239      0  0:00:01  0:00:01  --:--:-- 1239
  You are going to overwrite the LDAP CA Certificate.
  Are you sure you want to proceed and overwrite the LDAP CA Certificate? [y|N]y
LDAP CA Certificate is downloaded successfully
Server /ldap/binding-certificate #
```

Testing LDAP Binding

Before you begin

You must log in as a user with admin privileges to perform this task.



Note If you checked the **Enable Encryption** and the **Enable Binding CA Certificate** check boxes, enter the fully qualified domain name (FQDN) of the LDAP server in the LDAP Server field. To resolve the FQDN of the LDAP server, configure the preferred DNS of Cisco IMC network with the appropriate DNS IP address.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode.
Step 2	Server# /ldap scope binding-certificate	Enters the LDAP CA certificate binding command mode.
Step 3	Server /ldap/binding-certificate # test-ldap-binding <i>username</i>	Password prompt appears.
Step 4	Enter the corresponding password.	Authenticates the user.

Example

This example tests the LDAP user binding:

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # test-ldap-binding user
Password:
diagldapbinding: Authenticated by LDAP
User user authenticated successfully.
Server /ldap/binding-certificate #
```

Deleting LDAP CA Certificate

Before you begin

You must log in as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the LDAP command mode.
Step 2	Server# /ldap scope binding-certificate	Enters the LDAP CA certificate binding command mode.
Step 3	Server /ldap/binding-certificate # delete-ca-certificate	Confirmation prompt appears.
Step 4	At the confirmation prompt, enter y .	This deletes the LDAP CA certificate.

Example

This example deletes the LDAP certificate:

```
Server # scope ldap
Server /ldap # scope binding-certificate
Server /ldap/binding-certificate # delete-ca-certificate
You are going to delete the LDAP CA Certificate.
Are you sure you want to proceed and delete the LDAP CA Certificate? [y|N]y
LDAP CA Certificate is deleted successfully
Server /ldap/binding-certificate #
```

Setting User Search Precedence

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the BIOS command mode.
Step 2	Server# /ldap set userSearchPrecedence {localUserDB ldapUserDB}	Sets the user search precedence to the LDAP database or the local user database depending on the option you choose.
Step 3	Server# /ldap * commit	Commits the transaction.
Step 4	(Optional) Server# /ldap show detail	Shows the LDAP details.

Example

This example sets the user search precedence:

```
Server # scope ldap
Server /ldap # set userSearchPrecedence localUserDB
Server /ldap * # commit
Server /ldap # show detail
LDAP Settings:
Enabled: yes
Encrypted: no
Local User Search Precedence: localUserDB
Domain: new.com
Base DN: DC=new,DC=com
Timeout: 60
Filter Attribute: sAMAccountName
Attribute: CiscoAvPair
Server /ldap #
```

Viewing User Sessions

Procedure

	Command or Action	Purpose
Step 1	Server# show user-session	Displays information about current user sessions.

The command output displays the following information about current user sessions:

Name	Description
Terminate Session button	If your user account is assigned the admin user role, this option enables you to force the associated user session to end. Note You cannot terminate your current session from this tab.
Session ID column	The unique identifier for the session.
User name column	The username for the user.
IP Address column	The IP address from which the user accessed the server. If this is a serial connection, it displays N/A .
Type column	The type of session the user chose to access the server. This can be one of the following: <ul style="list-style-type: none"> • webgui— indicates the user is connected to the server using the web UI. • CLI— indicates the user is connected to the server using CLI. • serial— indicates the user is connected to the server using the serial port.

Example

This example displays information about current user sessions:

```
Server# show user-session
ID      Name      IP Address      Type      Killable
-----
15      admin     10.20.30.138   CLI       yes

Server /user #
```

Terminating a User Session

Before you begin

You must log in as a user with admin privileges to terminate a user session.

Procedure

	Command or Action	Purpose
Step 1	Server# show user-session	Displays information about current user sessions. The user session to be terminated must be eligible to be terminated (killable) and must not be your own session.

	Command or Action	Purpose
Step 2	Server /user-session # scope user-session <i>session-number</i>	Enters user session command mode for the numbered user session that you want to terminate.
Step 3	Server /user-session # terminate	Terminates the user session.

Example

This example shows how the admin at user session 10 terminates user session 15:

```

Server# show user-session
ID      Name           IP Address      Type      Killable
-----
10      admin          10.20.41.234   CLI      yes
15      admin          10.20.30.138   CLI      yes
Server# scope user-session 15
Server /user-session # terminate
User session 15 terminated.

Server /user-session #

```