Managing User Accounts

This chapter includes the following sections:

Configuring Local Users for Cisco UCS C-Series M7 and Later Servers

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** *usernumber*	Enters user command mode for user number *usernumber*.

	Command or Action	Purpose
Step 2	Server /user # **set enabled** {**yes** | **no**}	Enables or disables the user account on the Cisco IMC.
Step 3	Server /user # **set name** *username*	Specifies the username for the user.

Step 4	Server /user # **set role** {**readonly** | **user** | **admin**}	Specifies the role assigned to the user. The roles are as follows:
		• readonly—This user can view information but cannot make any changes.
		• user—This user can do the following:
		  • 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
		  • Set the time zone
		  • Ping an IP address
		• admin—This user can perform all actions available through the GUI, CLI, and IPMI.

Step 5	Server /user # **set user-typeCIMC|SNMP|IPMI**	Specifies the user type assigned to the user. You may select one or multiple user-type for a single user.
Step 6	Server /user # **set password**	You are prompted to enter the password twice.

	Command or Action	Purpose

		Note When strong password is enabled, you must follow these guidelines while setting a password:
		• 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)
		  • Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
		
		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.

Step 7	Server /user # **set ipmi-password** *password*	Set the password for IPMI user type.
Step 8	Server /user # **set v3priv-proto***None*|*CFB128_AES128*	Set this value for SNMP user type.
Step 9	Server /user # **set v3proto***HMAC128_SHA224*| *HMAC192_SHA256*| *HMAC256_SHA384* |*HMAC384_SHA512* |*HMAC_SHA96* |*None*	Set this value for SNMP user type.
Step 10	Server /user # **set v3priv-auth-key***Priv_Auth_key*	Set the key, if required.
Step 11	Server /user # **set v3auth-key***Auth_key*	Set the key, if required.

	Command or Action	Purpose
Step 12	Server /user # **commit**	Commits the transaction to the system configuration.

Example

This example configures user 5 as an admin and all three user type:

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name UserName
Server /user *# set role readonly
Server /user *# set user-type CIMC,SNMP,IPMI
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 ipmi-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 20 characters for IPMI users
 and
maximum 127 characters for Non IPMI users.
        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)
            Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
Please enter ipmi-password:
Server /user *# set v3proto None
Server /user *# set v3priv-proto None
Server /user *# commit
```

Managing SSH Keys for User Accounts

Configuring SSH Keys

In the release 4.1.2, Cisco IMC provides SSH RSA key-based authentication in addition to password authentication. SSH keys are a set of public and private RSA key pair, which you can use for authentication. Public key-based authentication provides enhanced security over password-based authentication.

You must log in as a user with admin privileges to configure the SSH keys for all the users. If you are a non-admin user, you can configure the SSH keys to authenticate and login only to your account. You can configure only one SSH RSA key pair, public and private, for your account. The SSH keys must be in .pem or .pub format.

The Cisco IMC sessions authenticated using public keys will be active even if the password has expired. You can also start new sessions using the public SSH key even after the password has expired. **Account lockout** option, available on some C-series servers, does not apply to the accounts that use public key authentication.

Adding SSH Keys

Before you begin

- You must log in as a user with admin privileges to add the SSH keys for all the users.
- If you are a non-admin user, you can add the public key only for your account.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope user** *user-number*	Enters the user command mode for a user.
Step 2	Server /user # **show-detail**	Displays the details of the user account. You can view the number of SSH keys configured for a user in the `SSH Key Count` field.
Step 3	Server /user # **scope ssh-keys**	Enters the SSH keys command mode.
Step 4	Server /user/ssh-keys # **add-key 1 remote**	Use this option to add the SSH key from a remote server. Enter the following details: **a.** Specify the protocol to connect to the remote server. It can be of the following types: • TFTP FTP SFTP SCP HTTP **Note** If you choose FTP, SCP or SFTP, you will be prompted to enter your username and password. **b.** Specify the remote server address. **c.** Specify the remote file path.

	Command or Action	Purpose
		d. Specify your username and password.
Step 5	(Optional) Server /user/ssh-keys # **add-key 2 paste**	Use this option to add the SSH key by paste method. Launches a dialog for entering the public SSH key. Copy the SSH key text, paste it into the console when prompted, and type CTRL+D.
Step 6	(Optional) Server /user/ssh-keys # **show-detail**	Displays the public SSH key that you have added to the account.

Example

1. This example adds the SSH key from a remote server.

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # add-key 1 remote
Enter the remote Protocol [tftp | ftp | sftp | scp | http]: scp
Enter the remote Server: 10.10.10.10
Enter the remote file Path: /home/xyz/publickey.pem
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: xyz
Password:
SSH Public key added successfully
Server /user/ssh-keys #
```

2. This example adds the SSH key by paste method.

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # add-key 2 paste
Please paste your ssh key here, when finished, press CTRL+D.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFOK17ZYbMMfGcxGrfxlupMqFyl1ZNIJohPxAStu41
OkItF9VrrhrfF1ZKOpogJinx3s0OcPfGLMSWEQkUq1zGlL8rAESZbi6z36WGFeZ93amJ3nfxDU7JWD9K
HmINixpX5XbbZeKQJvfSTptanmkjTQ8sq2iSMK0HL+G35i8BXmwIBLuEM+SWIEYjLaDAZ6aLKPxxddTr
FxWTP9QpzJAfQGlXXZSYauYb6OMNUxjgqFtB2XCiROZTzcj4n1XQRbzU+56HvHmowcOPhO81Btbun+xv
ksTeXbV3e9DVymjQK1qD2yY5h/EJdC0+9wGPyVmaT2bAOu4HbTsz8u4HFkTf
SSH Public key added successfully
Server /user/ssh-keys #
```

What to do next

Modify or delete the SSH key.

Modifying SSH Keys

Before you begin

- You must log in as a user with admin privileges to modify the SSH keys for all the users.

- If you are a non-admin user, you can modify the public key only for your account.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope user** *user-number*	Enters the user command mode for a user.
Step 2	Server /user # **show-detail**	Displays the details of the user account. You can view the number of SSH keys configured for a user in the `SSH Key Count` field.
Step 3	Server /user # **scope ssh-keys**	Enters the SSH keys command mode.
Step 4	Server /user/ssh-keys # **modify-key 1 remote**	Use this option to add the modified key from a remote server. Enter the following details: **a.** Specify the protocol to connect to the remote server. It can be of the following types: • TFTP FTP SFTP SCP HTTP **Note** If you choose FTP, SCP or SFTP, you will be prompted to enter your username and password. **b.** Specify the remote server address. **c.** Specify the remote file path. **d.** Specify your username and password.
Step 5	(Optional) Server /user/ssh-keys # **modify-key 2 paste**	Use this option to add the modified SSH key by paste method. Launches a dialog for entering the updated public SSH key. Copy the SSH key text, paste it into the console when prompted, and type CTRL+D.
Step 6	(Optional) Server /user/ssh-keys # **show-detail**	Displays the updated public SSH key that you modified in the account.

Example

1. This example adds the modified SSH key from a remote server.

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # modify-key 1 remote
Enter the remote Protocol [tftp | ftp | sftp | scp | http]: scp
Enter the remote Server: 10.10.10.10
Enter the remote file Path: /home/xyz/publickey.pem
Server (RSA) key fingerprint is dd:b5:2b:07:ad:c0:30:b2:d5:6a:6a:78:80:85:93:b0
Do you wish to continue? [y/N]y
Username: xyz
Password:
SSH Public key modified successfully
Server /user/ssh-keys #
```

2. This example adds the modified SSH key by paste method.

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # modify-key 2 paste
Please paste your ssh key here, when finished, press CTRL+D.
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFOK17ZYbMMfGcxGrfxlupMqFyl1ZNIJohPxAStu41
OkItF9VrrhrfF1ZKOpogJinx3s0OcPfGLMSWEQkUq1zGlL8rAESZbi6z36WGFeZ93amJ3nfxDU7JWD9K
HmINixpX5XbbZeKQJvfSTptanmkjTQ8sq2iSMK0HL+G35i8BXmwIBLuEM+SWIEYjLaDAZ6aLKPxxddTr
FxWTP9QpzJAfQGlXXZSYauYb6OMNUxjgqFtB2XCiROZTzcj4n1XQRbzU+56HvHmowcOPhO81Btbun+xv
ksTeXbV3e9DVymjQK1qD2yY5h/EJdC0+9wGPyVmaT2bAOu4HbTsz8u4HFkTf
SSH Public key modified successfully
Server /user/ssh-keys #
```

What to do next

Delete the SSH key.

Deleting SSH Keys

Before you begin

- You must log in as a user with admin privileges to delete the SSH keys for all the users.
- If you are a non-admin user, you can delete the public key only for your account.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope user** *user-number*	Enters the user command mode for a user.
Step 2	Server /user # **show-detail**	Displays the details of the user account. The field `SSH Key Count`displays the number of SSH keys that are configured for the user.
Step 3	Server /user # **scope ssh-keys**	Enters the SSH keys command mode.

	Command or Action	Purpose
Step 4	Server /user/ssh-keys # **delete-key 1**	A prompt with the message `Do you wish to continue? [y/N]` is displayed.
Step 5	Enter `y` to confirm the deletion.	
Step 6	(Optional) Server /user/ssh-keys # **show-detail**	Displays the updated user details and SSH key count.

Example

This example deletes the SSH key.

```
Server# scope user 1
Server /user # scope ssh-keys
Server /user/ssh-keys # delete-key 1
This operation will delete the SSH key -
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFOK17ZYbMMfGcxGrfxlupMqFyl1ZNIJohPxAStu41
OkItF9VrrhrfF1ZKOpogJinx3s0OcPfGLMSWEQkUq1zGlL8rAESZbi6z36WGFeZ93amJ3nfxDU7JWD9K
HmINixpX5XbbZeKQJvfSTptanmkjTQ8sq2iSMK0HL+G35i8BXmwIBLuEM+SWIEYjLaDAZ6aLKPxxddTr
FxWTP9QpzJAfQGlXXZSYauYb6OMNUxjgqFtB2XCiROZTzcj4n1XQRbzU+56HvHmowcOPhO81Btbun+xv
ksTeXbV3e9DVymjQK1qD2yY5h/EJdC0+9wGPyVmaT2bAOu4HbTsz8u4HFkTf
Do you wish to continue? [y/N]y
SSH Public key deleted successfully
Server /user/ssh-keys #
```

Non-IPMI User Mode

Release 4.1 introduces a new user configuration option called **User Mode** that allows you to switch between IPMI and non-IPMI user modes. Introduction of the non-IPMI user mode provides enhanced password security for users and security enhancements to the BMC database that were restricted in earlier releases due to the constraints posed by the IPMI 2.0 standards. Non-IPMI user mode allows you to use 127 characters to set user passwords whereas users in IPMI mode are restricted to a password length of 20 characters. Non-IPMI user mode enables you to set stronger passwords for users configured in this mode.

You must consider the following configuration changes that occur while switching between user modes, when you:

- Switch to the non-IPMI mode, IPMI over LAN will not be supported.
- Switch from the non-IPMI to IPMI mode, deletes all the local users and reverts user credentials to default username and password. On subsequent login, you will be prompted to change the password.

  User data is not affected when you switch from IPMI to non-IPMI mode.
- Downgrade the firmware to a versions lower than 4.1 and if the user mode is non-IPMI, deletes all the local users and reverts user credentials to default username and password. On subsequent login, you will be prompted to change the default password.

Note When you reset to factory defaults, the user mode reverts to IPMI mode.

Switching User Mode from IPMI to Non-IPMI

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 # **scope user-mode**	Enters user mode command mode.
Step 3	Server /user-policy/user-mode # **set user-mode non-ipmi**	Enter y at the confirmation prompt to switch to Non-IPMI user mode.
Step 4	Server /user-policy/user-mode * # **commit**	Commits the transaction to the system configuration.
Step 5	Server /user-policy/user-mode # **show detail**	Displays the user mode.

Example

This example shows how to disable strong password:

```
Server# scope user-policy
Server /user-policy # scope user-mode
Server /user-policy/user-mode # set user-mode non-ipmi
Server /user-policy/user-mode *# commit
Warning: This will enable NON-IPMI based user mode.
         Converting to Non-IPMI User Mode disables IPMI Services and removes IPMI user
support.
         SSH, KVM, Webserver, XMAPI and Redfish sessions will be disconnected.
Do you wish to continue? [y/N] y
Connection to 10.10.10.10 closed by remote host.
Connection to 10.10.10.10 closed.
Server /user-policy/user-mode # show detail
User Mode:
    User mode for IPMI accessibility: non-ipmi
Server /user-policy/user-mode #
```

Switching User Mode from Non-IPMI to IPMI

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.

	Command or Action	Purpose
Step 2	Server /user-policy # **scope user-mode**	Enters user mode command mode.
Step 3	Server /user-policy/user-mode # **set user-mode ipmi**	Enter y at the confirmation prompt to switch to IPMI user mode. **Note** Switching to IPMI user mode deletes all the UCS users and reverts to default username and password.
Step 4	Server /user-policy/user-mode * # **commit**	Commits the transaction to the system configuration.
Step 5	Server /user-policy/user-mode # **show detail**	Displays the user mode.

Example

This example shows how to disable strong password:

```
Server# scope user-policy
Server /user-policy # scope user-mode
Server /user-policy/user-mode # set user-mode ipmi
Server /user-policy/user-mode *# commit
Warning: This will enable IPMI based user mode.
         Converting to IPMI User Mode deletes all UCS users and reverts to default
userid/password.
         SSH, KVM, Webserver, XMAPI and Redfish sessions will be disconnected.
Do you wish to continue? [y/N] y
Connection to 10.10.10.10 closed by remote host.
Connection to 10.10.10.10 closed.
Server /user-policy/user-mode # show detail
User Mode:
    User mode for IPMI accessibility: ipmi
Server /user-policy/user-mode #
```

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 User Authentication Precedence

Procedure

	Command or Action	Purpose
Step 1	Server # **scope user-policy**	Enters the TACACS+ command mode.
Step 2	Server/user-policy # **set authentication-precedence** *User Database name*	Enter comma delimited list of user database.
Step 3	Server/user-policy # **commit**	

Example

```
Server # scope user-policy
Server /user-policy # set authentication-precedence DB1,DB2
Server /user-policy* # commit
```

Resetting the User Password

You can use the change password option to change your password.

Note

- This option is not available when you login as an admin, you can only change the password of the configured users with read-only user privileges.
- When you change your password you will be logged out of Cisco IMC.

Procedure

	Command or Action	Purpose
Step 1	Server # **scope user** *user ID*	Enters the chosen user command mode.
Step 2	Server /chassis/user # **set password**	Read the password requirements instructions and enter the current password, new password and confirm the password at the respective prompts.
Step 3	Server /chassis/user * # **commit**	Commits the transaction to the system configuration.

Example

This example shows how to change the password of a configured user:

```
Server # scope user 2
Server /chassis/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 20 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)
            Non-alphabetic characters (!, @, #, $, %, ^, &, *, -, _, +, =)
Please enter current password:Testabcd1
Please enter password: Testabcd2
Please confirm password: Testabcd2
Server /chassis/user * # commit
Server /chassis/user #
```

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** *integer in the range 0-3650*	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** *integer in the range 0-15*	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** *integer in the range 0-5*	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** *integer in the range 0-5*	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.

	Command or Action	Purpose
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	`CiscoAVPair`
LDAP Display Name	`CiscoAVPair`
Unique X500 Object ID	`1.3.6.1.4.1.9.287247.1`
Description	`CiscoAVPair`
Syntax	`Case Sensitive String`

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

a) Expand the **Classes** node in the left pane and type `U` to select the user class.

b) Click the **Attributes** tab and click **Add**.

c) Type `C` to select the CiscoAVPair attribute.

d) 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	`shell:roles="admin"`
user	`shell:roles="user"`
read-only	`shell:roles="read-only"`

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***LDAP domain name*	Specifies an LDAP domain name.
Step 4	Server /ldap # **set timeout** *seconds*	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 base-dn** *domain-name*	Specifies the Base DN that is searched on the LDAP server.
Step 6	Server /ldap # **set attribute** *name*	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.

	Command or Action	Purpose
		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: `1.3.6.1.4.1.9.287247.1` **Note** If you do not specify this property, user access is denied.
Step 7	Server /ldap # **set filter-attribute**	Specifies the account name attribute. If Active Directory is used, then specify **sAMAccountName** for this field.
Step 8	Server /ldap # **scope secure**	Enters the secure LDAP mode.
Step 9	Enable secure LDAP and either download the certificate remotely or paste the certificate.	Perform one of the following: **a.** Server /ldap # **secure-ldap** *disabled|enabled paste tftp | ftp | sftp | scp | http* Prompts you to paste the certificate content. **b.** Paste the certificate content and press **CTRL+D**. Confirmation prompt appears. **c.** At the confirmation prompt, enter **y**. This begins the download of the LDAP CA certificate. **OR** **a.** Server /ldap # **secure-ldap** *disabled|enabled remote tftp | ftp | sftp | scp | http IP Address LDAP CA Certificate file*

	Command or Action	Purpose
		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. 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. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. **b.** At the confirmation prompt, enter **y**. This begins the download of the LDAP CA certificate.
Step 10	Server /ldap # **commit**	Commits the transaction to the system configuration.
Step 11	Server /ldap # **show** [**detail**]	(Optional) Displays the LDAP configuration.

Example

This example configures LDAP using remote download option:

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# scope secure
Server /ldap/secure *# secure-ldap enabled remote ftp xx.xx.xx.xx filename
% 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/secure *# commit
Server /ldap # exit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout: 60
    Filter-Attribute: sAMAccountName
Server /ldap #
```

This example configures secure LDAP using paste certificate option:

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set domain sample-domain
Server /ldap *# set timeout 60
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# set filter-attribute sAMAccountName
Server /ldap *# scope secure
Server /ldap/secure *# secure-ldap enabled ftp paste

 Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIQV06yJcJPAYNO8Cp+FYQttjANBgkqhkiG9w0BAQsFADBO
MRIwEAYKCZImiZPyLGQBGRYCaW4xGzAZBgoJkiaJk/IsZAEZFgs0T0JKUkEySkhC
UTEbMBkGA1UEAxMSV0lOLTRPQkpSQTJKSEJRLUNBMB4XDTE2MDIyNTE3MDczNloX
DTIxMDIyNTE3MTczM1owTjESMBAGCgmSJomT8ixkARkWAmluMRswGQYKCZImiZPy
LGQBGRYLNE9CSlJBMkpIQlExGzAZBgNVBAMTEldJTi00T0JKUkEySkhCUS1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMM2cdgmrPTkZe4K2zI+EbeZ
mfQnjfiUz8OIY97w8lC/2S4qK46T+fnX13rXe8vvVHAO5wgPDVQTGS4nlF46A6Ba
FK+krKcIgFrQB1gnF74qs/ln1YtKHNBjrvg5KyeWFrA7So6Mi2XEw8w/zMPL0d8T
b+LM1YnhnuXA9G8gVCJ/iUhXfMpB20L8sv30Mek7bw8x2cxJYTuJAviVIrjSwU5j
fO3WKttRuyFpeOIi00weklpF0+8D3Z9mBinoTbL2pl0U32am6wTI+8WmtJ+8W68v
jH4Y8YBY/kzMHdpwjpdZkC5pE9BcM0rL9xKoIu6X0kSNEssoGnepFyNaH3t8vnMC
AwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
FBAUulHTAWBT1OBz8IgAEzXsfcCsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3
DQEBCwUAA4IBAQAzUMZr+0r1dWkVfFNBd7lu8tQbAEJf/A7PIKnJGNoUq8moAGs4
pMndoxdpNGZhYCWDWX3GWdeF1HqZHhb38gGQ9ylu0pIK7tgQufZmeCBH6T7Tzq/w
Dq+TMFGIjXF84xW3N665y4ePgUcUI7e/6aBGcGkGeUYodBPtExe28tQyeuYwD4Zj
nLuZKkT+I4PAYygVCqxDGsvfRHDpGneb3R+GeonOf4ED/0tn5PLSL9khb9qkHu/V
dO3/HmKVzUhloTDBuAMq/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/secure *# commit
Server /ldap # exit
Server /ldap # show detail
LDAP Settings:
    Enabled: yes
    Domain: sample-domain
    BaseDN: example.com
    Timeout: 60
```

```
    Filter-Attribute: sAMAccountName
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.
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** *index*	Selects one of the available group profiles for configuration, where *index* is a number between 1 and 28.
Step 5	Server /ldap/role-group # **set name** *group-name*	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** *domain-name*	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: • **admin**—The user can perform all actions available.

	Command or Action	Purpose
		• **user**—The user can perform the following tasks: • 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 #
```

TACACS+ Authentication

Beginning with 4.1(3b) release, Cisco IMC supports Terminal Access Controller Access-Control System Plus (TACACS+) user authentication. Cisco IMC supports up to six TACACS+ remote servers. Once a user is successfully authenticated, the username is appended with **(TACACS+)**. This is also displayed in the Cisco IMC interfaces.

Refer Enabling TACACS+ Authentication, on page 24 to enable TACACS+ Authentication. Cisco IMC also supports user authentication precedence in case TACACS+ remote servers are inaccessible. User authentication precedence can be configured using Configuring User Authentication Precedence, on page 13.

TACACS+ Server Configuration

Privilege level of a user is calculated based on the **cisco-av-pair** value configured for that user. A **cisco-av-pair** should be created on the TACACS+ server. Users cannot use any existing TACACS+ attributes.

Following three syntax are supported for the **cisco-av-pair** attribute:

- For **`admin`** privilege: **cisco-av-pair=shell:roles="admin"**
- For **`user`** privilege: **cisco-av-pair=shell:roles="user"**

- For **`read-only`** privilege: **cisco-av-pair=shell:roles="read-only"**

More roles, if required, can be added by using **comma** as a separator.

Note If **cisco-av-pair** is not configured on the TACACS+ server, then a user with that server has **read-only** privilege.

Enabling TACACS+ Authentication

Before you begin

Before configuring Terminal Access Controller Access-Control System (TACACS+) based user authentication, ensure that privilege level of a user is configured on TACACS+ server based on the **cisco-av-pair** value.

Procedure

	Command or Action	Purpose
Step 1	Server# **scope tacacs+**	Enters the TACACS+ command mode.
Step 2	Server/tacacs+ # **set enabled** *yes|no*	
Step 3	Server/tacacs+ # **set fallback-only-on-no-connectivity** *yes|no*	If you are enabling **`fallback-only-on-no-connectivity`**, enter **`Y`** to confirm.
Step 4	Server/tacacs+ # **set timeout** *timeout duration in seconds*	Enter a value between 5 to 30.
Step 5	Server/tacacs+ # **restore**	If you wish to restore TACACS+ configuration to default in case of time out, enter **`yes`** to confirm.
Step 6	Server/tacacs+ # **commit**	Saves the changes in the system.

Example

```
Server # scope tacacs+
Server /tacacs+ # set enabled yes
Server /tacacs+ # set fallback-only-on-no-connectivity yes

Warning: If TACACS+ and fallback option is enabled, then the fallback to the next
         precedence database happens only when CIMC is not able to connect to any
         of the configured TACACS+ servers.
Do you wish to continue? [y/N] y
Server /tacacs+ # set timeout 5
Server /tacacs+ # restore
Are you sure you want to restore TACACS+ configuration to defaults?
Please enter 'yes' to confirm: yes
Restored TACSCS+ default configuration.

Server /tacacs+ # commit
```

Configuring TACACS+ Remote Server Settings

Procedure

	Command or Action	Purpose
Step 1	Server# **scope tacacs+**	Enters the TACACS+ command mode.
Step 2	Server# **scope tacacs-server***Server Number*	Enters the TACACS server command mode.
Step 3	Server/tacacs+/tacacs-server # **set tacacs-port** *Port Number*	Enter a value between 1 and 65535.
Step 4	Server/tacacs+/tacacs-server # **set tacacs-key** *Server Key*	Enter the same key configured on the remote TACACS+ server.
Step 5	Server/tacacs+/tacacs-server # **set tacacs-server** *Server IP Address*	Enter remote TACACS+ server IP address.
Step 6	Server/tacacs+/tacacs-server # **restore**	If you wish to restore TACACS+ configuration to default in case of time out, enter **`yes`** to confirm.

Example

```
Server # scope tacacs+
Server # scope tacacs-server 1
Server /tacacs+/tacacs-server # set tacacs-port 6
Server /tacacs+/tacacs-server # set tacacs-key xxx
Server /tacacs+/tacacs-server # set tacacs-server xx.xx.xx.xx
Server /tacacs+/tacacs-server # restore
Are you sure you want to restore TACACS+ configuration to defaults?
Please enter 'yes' to confirm: yes
Restored TACSCS+ default configuration.

Server /tacacs+/tacacs-server # commit
```

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 Adderss LDAP CA Certificate file*	Specifies the protocol to connect to the remote server. It can be of the following types: • TFTP • FTP • SFTP • SCP • HTTP **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. 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. The fingerprint is based on the host's public key and helps you to identify or verify the host you are connecting to. Initiates the export of the certificate.

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 #
```

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** *username*	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 #
```

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
Session ID column	The unique identifier for the session.
BMC Session ID	The identifier for the BMC session.
User Name column	The username for the user.

Name	Description
IP Address column	The IP address from which the user accessed the server. If this is a serial connection, it displays **N/A**.
Session Type column	The type of session the user chose to access the server. This can be one of the following: • **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. • **XML API**— indicates the user is connected to the server using XML API. • **Redfish**— indicates the user is connected to the server using Redfish API.
Action column	This column displays **N/A** when the SOL is enabled and **Terminate** when the SOL is disabled. You can terminate a session by clicking **Terminate** on the web UI.

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** *session-number*	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 #
```