Managing User Accounts

This chapter includes the following sections:

Modifying or Adding Local Users for Cisco UCS C-Series M6 and Earlier Servers

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 **Local User** tab displays a **Disable Strong Password** button 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 configure or modify local user accounts.

Procedure

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **Local User Management** tab.

Step 4 To add a local user account, click **Add User**.

To modify a local user account, click a row in the **Local User Management** pane and click **Modify User**.

Step 5 In the **Modify User Details** or **Local User Details** dialog box, update the following properties:

Name	Description
ID field	The unique identifier for the user.
Username field	The username for the user. Enter between 1 and 16 characters.

Role Played field	The role assigned to the user. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role can perform the following tasks:
	  • View all information
	  • Manage the power control options such as power on, power cycle, and power off
	  • Launch the vKVM console and virtual media
	  • Clear all logs
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.
	Note Any user with admin role will not have the option of **Change Password** from the right top corner in **Settings** drop-down menu.
	To change password as a non-admin user, select **read-only** or **user** role and not the **admin** role.

Enabled check box	If checked, the user is enabled on Cisco IMC.
Change Password check box	Enable this check box if you want to change the password.

Name	Description
New Password field	The password for this user name. Click the **Suggest** button to get a system generated password that you may want to use. When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed: • The password must have a minimum of 8 and a maximum of 20 characters. The password can have a maximum of 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 (!, @, #, $, %, ^, &, *, -, _,+ , =). These guidelines are meant to define a strong password for the user, for security reasons. However, if you want to set a password of your choice ignoring these guidelines, click the **Disable Strong Password** button on the **Local User Management** tab. While setting a password when the strong password option is disabled, you can use between 1- 20 characters.
Confirm Password field	The password repeated for confirmation.

Step 6 Enter password information.

Step 7 Click **Save Changes**.

Managing SSH Keys in User Accounts

Configuring SSH Keys

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

The Cisco IMC sessions authenticated using public SSH 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 does not apply to the accounts that use public key authentication.

Before you begin

- You must log in as a user with admin privileges to configure SSH keys for all the users.
- Ensure that you have created a pair of SSH RSA keys, public and private.
- Ensure that the SSH keys are in .pem or .pub format.

Procedure

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

Step 2 In the **Admin** menu, click the **User Management** tab.

Step 3 In the **User Management** pane, click the **Local User Management** tab.

Step 4 To view the number of SSH keys configured for an account, view the details in the **SSH Key Count** field.

Step 5 To view the details of the SSH keys for an account, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 6 In the **SSH Keys** window, view the following properties:

Name	Description
ID field	The unique identifier for the SSH key.
Comment	User name and remote server host name in the format *username@hostname*
Key	Details of the public SSH key configured for a specific user.

What to do next

Add or modify the SSH keys.

Adding SSH Keys

Before you begin

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

Procedure

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

Step 2 In the **Admin** menu, click the **User Management** tab.

Step 3 In the **User Management** pane, click the **Local User Management** tab.

Step 4 To add the SSH keys for an account, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 Click any of the radio buttons near the **ID** column.

Step 6 Click **Add Keys** icon in the **SSH Keys** window to add the SSH key.

Step 7 Select any of the following radio buttons to add the SSH key.

a) Select **Paste SSH key**.

Copy the public SSH key from the host and paste the key in the text field.

b) Select **Upload from local**.

Click **Browse** and navigate to the public SSH key file that you want to add.

c) Select **Upload from remote location**.

Enter the following details to upload the public key file from the remote location.

Name	Description
Upload SSH key from drop-down list	The remote server type. This can be one of the following: • TFTP • FTP • SCP • SFTP • HTTP **Note** If you choose FTP, SCP or SFTP, you will be prompted to enter your username and password.
Server IP/Hostname field	The IP address or hostname of the server on which the SSH key file is available
Path and Filename field	The path and filename of the public SSH key file on the remote server.

Step 8 Click **Upload SSH Key**.

What to do next

Modify or delete the SSH keys.

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 SSH keys only for your account.

Procedure

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

Step 2 In the **Admin** menu, click the **User Management** tab.

Step 3 In the **User Management** pane, click the **Local User Management** tab.

Step 4 To view and modify the SSH keys, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 To modify the SSH key, review the list of SSH keys and select the desired row in the **SSH Keys** window.

Step 6 Click the **Modify Key** icon.

Step 7 Select any of the following radio buttons to modify the SSH key.

a) Select **Paste SSH key**.

Copy the updated public SSH key from the host and paste the key in the text field.

b) Select **Upload from local**.

Click **Browse** and navigate to the updated public key file that you want to upload.

c) Select **Upload from remote location**.

Enter the following details to upload the updated public key file from the remote location.

Name	Description
Upload SSH key from drop-down list	The remote server type. This can be one of the following: • TFTP • FTP • SCP • SFTP • HTTP **Note** If you choose FTP, SCP or SFTP, you will be prompted to enter your username and password.
Server IP/Hostname field	The IP address or hostname of the server on which the updated SSH key file is available
Path and Filename field	The path and filename of the updated public SSH key file on the remote server.

Step 8 Click **Upload SSH Key**.

What to do next

Delete an 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 SSH keys only for your account.

Procedure

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

Step 2 In the **Admin** menu, click the **User Management** tab.

Step 3 In the **User Management** pane, click the **Local User Management** tab.

Step 4 To view and delete the SSH keys for a user account, click a row in the **Local User Management** pane and click **SSH Keys**.

The **SSH Keys** window is displayed.

Step 5 To delete the SSH key, review the list of SSH keys and select the desired row in the **SSH Keys** window.

Step 6 Click the **Delete Key** icon.

A pop-up window is displayed with the message *Do you want to delete the selected SSH key?*

Step 7 Click **Yes** to confirm the deletion.

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 between IPMI and Non-IPMI User Modes

Caution Performing this procedure restarts SSH, KVM, Webserver, XML API, and REST API services. It also removes the IPMI user support when you switch to Non-IPMI user mode.

Before you begin

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

Procedure

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

Step 2 In the **Admin** tab, click **User Management**.

Step 3 Click the **Disable IPMI User Mode** or **Enable IPMI User Mode** button and click **OK** to confirm.

Changing Password as a Non-Admin User

Note To perform this task, you must first login as admin and add a user with read-only or user privileges. Only then, you will be able to login as a non-admin user to change the password.

Procedure

Step 1 Login as an admin user.

Step 2 In the **Navigation** pane, click the **Admin** menu.

Step 3 In the **Admin** menu, click **User Management**.

Step 4 In the **User Management** pane, click the **Local User Management** tab.

Step 5 To configure or add a local user account, click a row in the **Local User Management** pane and click **Add User**.

Step 6 In the **Add User** dialog box, update the following properties by adding a user with read-only or user privileges:

Name	Description
ID field	The unique identifier for the user.

Name	Description
Username field	The username for the user. Enter between 1 and 16 characters.

Role Played field	The role assigned to the user. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role 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
	  • Set time zone
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.
	Note To change password select **read-only** or **user** role and not the **admin** role.

Enabled check box	If checked, the user is enabled on the Cisco IMC.
Change Password check box	If checked, the user is enabled to change the password.

Name	Description
New Password	Enter the new password for this username. Click the **Suggest** button to get a system generated password that you may want to use. When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed: • The password must have a minimum of 8 and a maximum of 14 characters. For Non IPMI users, the password can have maximum of 127 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 (!, @, #, $, %, ^, &, *, -, _, , =, "). These guidelines are meant to define a strong password for the user, for security reasons. However, if you want to set a password of your choice ignoring these guidelines, click the **Disable Strong Password** button on the **Local User Management** tab. While setting a password when the strong password option is disabled, you can use between 1- 20 characters.
Confirm Password field	The password repeated for confirmation.

Step 7 Click **Save Changes**.

Note On changing the password, you will be logged out of Cisco IMC.

Step 8 After creating a new user with read-only or user privileges, logout as admin.

Step 9 Now, login with the newly created read-only or user role. **Change Password** option is available in the right top corner in **Settings** drop-down menu.

When you click on the **Settings** icon, the drop-down lists the **Change Password** option. This option is visible only if you are logged in as a non-admin user.

If you do not see the **Change Password** option in the drop-down list, login as a non-admin user with read-only or user privileges.

You can now use the **Change Password** option to change your password. As soon as the password is changed, you will be logged out automatically and will be prompted to login with the new password.

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 Duration

Before you begin

- You must enable password expiry.

Procedure

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **Local User Management** pane (opens by default), click **Password Expiration Details**.

Step 4 In the **Password Expiration Details** dialog box, update the following fields:

Name	Description
Enable Password Expiry check box	Checking this box allows you to configure the **Password Expiry Duration**. Uncheck the check box to disable it.

Name	Description
Password Expiry Duration field	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 1 to 3650 days. **Note** Password expiry once set by the admin is applicable for all users that are subsequently created.
Password History field	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 field.
Notification Period field	Notifies the time by when the password expires. Enter a value between 0 to 15 days. Entering 0 disables this field. **Note** The notification period time must be lesser than the password expiry duration.
Grace Period field	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 field. **Note** The grace period time must be lesser than the password expiry duration.

Note The valid **Password Expiry Duration** must be greater than the **Notification Period** and the **Grace Period**. If otherwise, you will see an **User Password Expiry Policy configuration error**.

Step 5 Click **Save Changes**.

Step 6 Optionally, click **Reset Values** to clear the text fields and reset the values you entered. Click **Restore Defaults** to revert to the default settings.

Enabling Password Expiry

Before you begin

Procedure

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **Local User Management** pane (opens by default), click **Password Expiration Details**.

Step 4 In the **Password Expiration Details** dialog box, check the **Enable Password Expiry** check box.

The **Password Expiry Duration** text field becomes editable and you can configure the duration by entering a number in days.

What to do next

Configure password expiry duration.

Configuring Account Lockout Details

Procedure

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **Local User Management** tab.

Step 4 In the **Local User Management** pane, click **Account Lockout Details**.

Step 5 In the **Account Lockout Details** dialog box, complete the following:

Name	Description
Allowed Attempts (0-20) field	Number of unsuccessful log in attempts allowed for a user before which it is locked out for the duration defined in **Lockout Period**.
Lockout Period (0-60 Minutes) field	The time duration, in minutes, for which the user account is locked out after the allowed attempts.
Disable User on Lockout check box	Disables the user ID up on lockout.

Configuring User Authentication Precedence

Procedure

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **Local User Management** tab.

Step 4 In the **Local User Management** pane, click **Configure User Authentication Precedence**.

Step 5 In the **Configure User Authentication Precedence** dialog box, select the database for which you wish to update the priority.

Step 6 Use the Up or the Down arrow to change the priority of the database.

Resetting User Credentials to Factory Default Values

Caution You may lose current IP address settings, NIC port settings, NIC redundancy after performing this procedure. Cisco recommends that you make a note of your current server settings before performing this procedure.

Before you begin

Ensure that your management Ethernet cable is plugged into the dedicated management port.

Procedure

Step 1 Login as an admin user.

Step 2 In the **Navigation** pane, click the **Chassis** menu.

Step 3 In the **Chassis** menu, click **Summary**.

Step 4 From the tool bar, click **Launch KVM**.

Step 5 Alternatively, in the **Navigation** pane, click the **Compute** menu.

- **a.** In the **Compute** menu, select a server.
- **b.** In the work pane, click the **Remote Management** tab.
- **c.** In the **Remote Management** pane, click the **Virtual KVM** tab.
- **d.** In the **Virtual KVM** tab, click **Launch HTML based KVM console**.

Step 6 From the **Power** menu, select **Reset System**.

Step 7 When prompted, press **F8** to enter the Cisco IMC Configuration Utility. This utility opens in the KVM console window.

Step 8 Check the **Factory Default** check box, the server reverts to the factory defaults.

Step 9 Press **F5** to refresh the settings that you made. You might have to wait about 45 seconds until the new settings appear and the message **Network settings configured** is displayed before you reboot the server in the next step.

Step 10 Press **F10** to save your settings and reboot the server.

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 checking the Enable Encryption check box in the **LDAP Settings** area, 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 In the **Navigation** pane, click the **Admin** menu.

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click **LDAP**.

Step 4 Ensure that the LDAP schema snap-in is installed.

Step 5 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`

Properties	Value
Syntax	`Case Sensitive String`

Step 6 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 7 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 Settings and Group Authorization in Cisco IMC

Before you begin

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

Procedure

Step 1 In the **Navigation** pane, click the **Admin** menu.
Step 2 In the **Admin** menu, click **User Management**.
Step 3 In the **User Management** pane, click **LDAP**.
Step 4 In the **LDAP Settings** area, update the following properties:

Name	Description
Enable LDAP check box	If checked, user authentication and role authorization is performed first by the LDAP server, followed by user accounts that are not found in the local user database.

Name	Description
Base DN field	Base Distinguished Name. This field describes where to load users and groups from. It must be in the **dc=domain,dc=com** format for Active Directory servers.
Domain field	The IPv4 domain that all users must be in. This field is required unless you specify at least one Global Catalog server address.
Enable Secure LDAP check box	If checked, the server enables secure LDAP and prompts you to download LDAP CA certificate. Refer Downloading an LDAP CA Certificate, on page 24 to download LDAP CA certificate. To delete an existing secure LDAP certificate, un-check this option. Follow the system prompts to confirm deletion.
Timeout (0 - 180) seconds	The number of seconds the Cisco IMC waits until the LDAP search operation times out. If the search operation times out, Cisco IMC tries to connect to the next server listed on this tab, if one is available. **Note** The value you specify for this field could impact the overall time.

Note If you check the **Enable Secure LDAP**check box, 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.

Step 5 In the **Configure LDAP Servers** area, update the following properties:

Name	Description
Pre-Configure LDAP Servers radio button	If checked, the Active Directory uses the pre-configured LDAP servers.
LDAP Servers fields	
Server	The IP address of the 6 LDAP servers. If you are using Active Directory for LDAP, then servers 1, 2 and 3 are domain controllers, while servers 4, 5 and 6 are Global Catalogs. If you are not Active Directory for LDAP, then you can configure a maximum of 6 LDAP servers. **Note** You can provide the IP address of the host name as well.

Name	Description
Port	The port numbers for the servers. If you are using Active Directory for LDAP, then for servers 1, 2 and 3, which are domain controllers, the default port number is 389. For servers 4, 5 and 6, which are Global Catalogs, the default port number is 3268. LDAPS communication occurs over the TCP 636 port. LDAPS communication to a global catalog server occurs over TCP 3269 port.
Use DNS to Configure LDAP Servers radio button	If checked, you can use DNS to configure access to the LDAP servers.
DNS Parameters fields	
Source drop-down list	Specifies how to obtain the domain name used for the DNS SRV request. It can be one of the following: • **Extracted**—specifies using domain name extracted-domain from the login ID • **Configured**—specifies using the configured-search domain. • **Configured-Extracted**—specifies using the domain name extracted from the login ID than the configured-search domain.
Domain to Search	A configured domain name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.
Forest to Search	A configured forest name that acts as a source for a DNS query. This field is disabled if the source is specified as **Extracted**.

Step 6 In the **Binding Parameters** area, update the following properties:

Name	Description
Method drop-down list	It can be one of the following: • **Anonymous**—requires NULL username and password. If this option is selected and the LDAP server is configured for Anonymous logins, then the user can gain access. • **Configured Credentials**—requires a known set of credentials to be specified for the initial bind process. If the initial bind process succeeds, then the distinguished name (DN) of the user name is queried and re-used for the re-binding process. If the re-binding process fails, then the user is denied access. • **Login Credentials**—requires the user credentials. If the bind process fails, the user is denied access. By default, the **Login Credentials** option is selected.
Binding DN	The distinguished name (DN) of the user. This field is editable only if you have selected **Configured Credentials** option as the binding method.
Password	The password of the user. This field is editable only if you have selected **Configured Credentials** option as the binding method.

Step 7 In the **Search Parameters** area, update the following fields:

Name	Description
Filter Attribute	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **sAMAccountName**.
Group Attribute	This field must match the configured attribute in the schema on the LDAP server. By default, this field displays **memberOf**.

Name	Description
Attribute	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. The LDAP attribute can use an existing LDAP attribute that is mapped to the Cisco IMC user roles and locales, or can modify the schema such that a new LDAP attribute can be created. For example, **CiscoAvPair**.
Nested Group Search Depth (1-128)	Parameter to search for an LDAP group nested within another defined group in an LDAP group map. The parameter defines the depth of a nested group search.

Step 8 (Optional) In the **Group Authorization** area, update the following properties:

Name	Description
LDAP Group Authorization check box	If checked, user authentication is also done on the group level for LDAP users that are not found in the local user database. If you check this box, Cisco IMC enables the **Configure Group** button.
Group Name column	The name of the group in the LDAP server database that is authorized to access the server.
Group Domain column	The LDAP server domain the group must reside in.

Role column	The role assigned to all users in this LDAP server group. This can be one of the following:
	• **read-only**—A user with this role can view information but cannot make any changes.
	• **user**—A user with this role 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
	  • Ping
	• **admin**—A user with this role can perform all actions available through the GUI, CLI, and IPMI.

Name	Description
Configure button	Opens the **Configure LDAP Group** window for an active directory group with the same **Group Name**, **Group Domain**, and **Role** options listed above. Once configured, click **Save Changes**.
Delete button	Deletes an existing LDAP group.

Step 9 Click **Save Changes**.

LDAP Certificates Overview

Cisco S3260 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.

Viewing LDAP CA Certificate Status

Procedure

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 In the **Certificate Status** area, view the following fields:

Name	Description
Download Status	This field displays the status of the LDAP CA certificate download.
Export Status	This field displays the status of the LDAP CA certificate export.

Exporting an LDAP CA Certificate

Before you begin

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

You should have downloaded a signed LDAP CA Certificate before you can export it.

Procedure

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 Click the **Export LDAP CA Certificate** link.

The **Export LDAP CA Certificate** dialog box appears.

Name	Description
Export to Remote Location	Selecting this option allows you to choose the certificate from a remote location and export it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?*. Click Yes or No 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. • **Server IP/Hostname** field — The IP address or hostname of the server on which the LDAP CA certificate file should be exported. Depending on the setting in the **Download Certificate from** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename Cisco IMC should use when downloading the certificate from the remote server. • **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • **Password** field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.

Name	Description
Export to Local Desktop	Selecting this option allows you to choose the certificate stored on a drive that is local to the computer and export it.

Step 5 Click **Export Certificate**.

Downloading an LDAP CA Certificate

Note Only CA certificates or chained CA certificates must be used in Cisco IMC. By default, CA certificate is in .cer format. If it is a chained CA certificate, then it needs to be converted to .cer format before downloading it to Cisco IMC.

Steps

1. In the **Navigation** pane, click the **Admin** tab.
2. In the **Admin** menu, click **User Management**.
3. In the **User Management** pane, click the **LDAP** tab.
4. Click the **Download LDAP CA Certificate** link.

   The **Download LDAP CA Certificate** dialog box appears.
5. Fill the required information in the **Download LDAP CA Certificate** dialog box.

Name	Description
Upload **from remote location** radio button	Selecting this option allows you to choose the certificate from a remote location and Upload it. Enter the following details: • • **TFTP Server** • **FTP Server** • **SFTP Server** • **SCP Server** • **HTTP Server** **Note** If you chose SCP or SFTP as the remote server type while performing this action, a pop-up window is displayed with the message *Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*. Click Yes or No 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. • **Server IP/Hostname** field — The IP address or hostname of the server on which the LDAP CA certificate file should be stored. Depending on the setting in the Upload **Certificate from** drop-down list, the name of the field may vary. • **Path and Filename** field — The path and filename Cisco IMC should use when uploading the file to the remote server. • **Username** field — The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP or HTTP. • **Password** field — The password for the remote server username. This field does not apply if the protocol is TFTP or HTTP.
Upload **through browser client** radio button	Selecting this option allows you to navigate to the certificate stored on a drive that is local to the computer running the Cisco IMC GUI. When you select this option, Cisco IMC GUI displays a **Browse** button that lets you navigate to the file you want to import.
Paste Certificate content radio button	Selecting this option allows you to copy the entire content of the signed certificate and paste it in the **Paste certificate content** text field. **Note** Ensure the certificate is signed before uploading.
Upload **Certificate** button	Allows you to Upload the certificate to the server.

Testing LDAP Binding

Before you begin

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

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

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **LDAP** tab.

Step 4 Click the **Test LDAP Binding** link.

The **Test LDAP CA Certificate Binding** dialog box appears.

Name	Description
Username field	Enter the user name.
Password field	Enter the corresponding password.

Step 5 Click **Test**.

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 27 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

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **TACACS+** tab.

Step 4 Under the **TACACS+ Properties** area perform the following:

Name	Description
Enabled check box	Check this box to enable TACACS+ based user authentication.
Fallback only on no connectivity check box	If checked, the authentication falls back to the next precedence database only in-case Cisco IMC is not able to connect to any of the configured TACACS+ servers. Ensure to configure user authentication precedence. Refer Configuring User Authentication Precedence, on page 13.
Timeout (for each server): (5 - 30) seconds field	Time duration, in seconds, for which Cisco IMC waits for a response from each of the TACACS+ servers

Configuring TACACS+ Remote Server Settings

You can configure up to six TACACS+ remote servers.

Procedure

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click the **TACACS+** tab.

Step 4 Under the **Server List** area, click the radio button for the server ID which you wish to configure and click the **Edit** button.

Step 5 Update the following fields:

Name	Description
ID	This is unique identifier of the server and is not user editable.
IP Address or Host Name	The IP address at which the TACACS+ server is running.
Port	The port on which TACACS+ server is running.
Server key	The same key that is configured on the TACACS+ server. Repeat the same key for **Confirm Server Key**.

Viewing User Sessions

Procedure

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

Step 2 In the **Admin** menu, click **User Management**.

Step 3 In the **User Management** pane, click **Session Management**.

Step 4 In the **Sessions** pane, view 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.
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. • — indicates the user is connected to the server using XML API. • — indicates the user is connected to the server using Redfish API.