



Managing User Accounts

This chapter includes the following sections:

- [Configuring Local Users, on page 1](#)
- [LDAP Servers, on page 3](#)
- [Viewing User Sessions, on page 16](#)
- [Password Expiry, on page 17](#)

Configuring Local Users

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.

Effective with Release 2.0(9f), you can choose to disable all local users and authenticate only using remote authentication including LDAP or Active Directory. To enable this, local user management supports the disabling of all Cisco IMC users including default admin user.



Warning

If you choose to disable all Cisco IMC users and do not have an alternative method to log on to Cisco IMC, you may not be able access Cisco IMC. As a workaround, the Cisco IMC factory default is required, which then enables the default admin user credentials.

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** tab.
- Step 2** On the **Admin** tab, click **User Management**.
- Step 3** In the **User Management** pane, click the **Local User Management** tab.
- Step 4** To configure or modify a local user account, click a row.

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

Name	Description
ID field	The unique identifier for the user.
Enabled check box	If checked, the user is enabled on the Cisco IMC.
Username field	The username for the user. Enter between 1 and 16 characters.
Role field	<p>The role assigned to the user. This can be one of the following:</p> <ul style="list-style-type: none"> • 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: <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 • Ping • admin—A user with this role can perform all actions available through the GUI, CLI, and IPMI.
Change Password check box	If checked, when you save the changes the password for this user will be changed. You must check this box if this is a new user name.

Name	Description
New Password field	<p>The password for this user name.</p> <p>Click the Suggest button to get a system generated password that you may want to use.</p> <p>When you move the mouse over the help icon beside the field, the following guidelines to set the password are displayed:</p> <ul style="list-style-type: none"> • 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: <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>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.</p>
Confirm New Password field	The password repeated for confirmation purposes.

Step 6 Click **Save Changes**.

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

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:

- 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 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** tab.
- Step 2** On the **Admin** tab, click **User Management**.
- Step 3** In the **User Management** pane, click the **LDAP** tab.
- 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.
Base DN field	Base Distinguished Name. This field describes where to load users and groups from. It must be in the <code>dc=domain,dc=com</code> 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 Encryption check box	If checked, the server encrypts all information it sends to the LDAP server.

Name	Description
Enable Binding CA Certificate check box	If checked, allows you to bind the LDAP CA certificate.
Timeout (0 - 180) seconds	<p>The number of seconds the Cisco IMC waits until the LDAP search operation times out.</p> <p>If the search operation times out, Cisco IMC tries to connect to the next server listed on this tab, if one is available.</p> <p>Note The value you specify for this field could impact the overall time.</p>
User Search Precedence	<p>Allows you to specify the order of search between the local user database and LDAP user database. This can be one of the following:</p> <ul style="list-style-type: none"> • Local User Database (Default setting) • LDAP User Database

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	<p>The IP address of the 6 LDAP servers.</p> <p>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.</p> <p>Note You can provide the IP address of the host name as well.</p>
Port	<p>The port numbers for the servers.</p> <p>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.</p> <p>LDAPS communication occurs over the TCP 636 port. LDAPS communication to a global catalog server occurs over TCP 3269 port.</p>

Name	Description
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	<p>Specifies how to obtain the domain name used for the DNS SRV request. It can be one of the following:</p> <ul style="list-style-type: none"> • 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	<p>A configured domain name that acts as a source for a DNS query.</p> <p>This field is disabled if the source is specified as Extracted.</p>
Forest to Search	<p>A configured forest name that acts as a source for a DNS query.</p> <p>This field is disabled if the source is specified as Extracted.</p>

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

Name	Description
Method	<p>It can be one of the following:</p> <ul style="list-style-type: none"> • 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. <p>By default, the Login Credentials option is selected.</p>
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	<p>This field must match the configured attribute in the schema on the LDAP server.</p> <p>By default, this field displays sAMAccountName.</p>
Group Attribute	<p>This field must match the configured attribute in the schema on the LDAP server.</p> <p>By default, this field displays memberOf.</p>

Name	Description
Attribute	<p>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>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.</p>
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	<p>If checked, user authentication is also done on the group level for LDAP users that are not found in the local user database.</p> <p>If you check this box, Cisco IMC enables the Configure Group button.</p>
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.
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	<p>The role assigned to all users in this LDAP server group. This can be one of the following:</p> <ul style="list-style-type: none"> • 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: <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 • Ping • admin—A user with this role can perform all actions available through the GUI, CLI, and IPMI.

Name	Description
Configure button	Configures an active directory group.
Delete button	Deletes an existing LDAP group.

Step 9 Click **Save Changes**.

Setting User Search Precedence

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** tab.

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

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

Step 4 In the **LDAP Settings** area's **User Search Precedence** field, select **Local User Database** or **LDAP User Database**.

This field allows you to specify the order of search between the above options. **Local User Database** is the default option.

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.

Downloading an LDAP CA Certificate from Local Browser

Before you begin

- You must log in as a user with admin privileges to perform this action.
- You must enable Binding CA Certificate to perform this action.



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.

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** In the **Certificate** area, click the **Download LDAP CA Certificate from Local Browser** link.

The **Download LDAP CA Certificate from Local Browser** dialog box appears.

Name	Description
File field	Using the Browse button, select an LDAP CA certificate stored on a drive that is local to the computer running the Cisco IMC GUI.
Download Certificate button	Allows you to download the certificate to the server.

Downloading an LDAP CA Certificate from Remote Server

Before you begin

- You must log in as a user with admin privileges to perform this action.
- You must enable Binding CA Certificate to perform this action.



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.

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** In the **Certificate** area, click the **Download LDAP CA Certificate from Remote Server** link.

The **Download LDAP CA Certificate from Remote Server** dialog box appears.

Name	Description
Download LDAP CA Certificate from drop-down list	<p>Selecting this option allows you to choose the certificate from a remote location and download it. Enter the following details:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>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 <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?.</i> Click Yes or No 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> <ul style="list-style-type: none"> • 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 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.
Download Certificate button	Allows you to download the certificate to the server.

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** In the **Certificate** area, click the **Export LDAP CA Certificate** link.
- The **Export LDAP CA Certificate** dialog box appears.

Name	Description
Export LDAP CA Certificate to Remote Server	<p>Selecting this option allows you to choose the certificate from a remote server and export it. Enter the following details:</p> <ul style="list-style-type: none"> • TFTP Server • FTP Server • SFTP Server • SCP Server • HTTP Server <p>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 <i>Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?</i>. Click Yes or No 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> <ul style="list-style-type: none"> • 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.
Export LDAP CA Certificate to Local File	<p>Selecting this option allows you to choose the certificate stored on a drive that is local to the computer and export it.</p>

Step 5 Click **Export**.

Pasting an LDAP CA Certificate

Before you begin

- You must log in as a user with admin privileges to perform this action.
- You must enable Binding CA Certificate to perform this action.



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.

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** In the **Certificate** area, click the **Paste LDAP CA Certificate** link.

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

Name	Description
Certificate text field	Copy the entire content of the signed certificate and paste it here.
	Note Ensure the certificate is signed before downloading.

Step 5 Click **Save Certificate**.

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** tab.
- 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** area, 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**.
-

Viewing User Sessions

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** tab.
- Step 2** On the **Admin** tab, click **User Management**.
- Step 3** In the **User Management** pane, click the **Sessions** tab.
- Step 4** View the following information about current user sessions:

Tip Click a column header to sort the table rows, according to the entries in that column.

Name	Description
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.

Name	Description
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.

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** tab.
- Step 2** On the **Admin** tab, click **User Management**.
- Step 3** In the **Local Users** 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.
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.

Step 5 Click **Save Changes**.

Enabling Password Expiry

Before you begin

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** tab.
- Step 2** On the **Admin** tab, click **User Management**.
- Step 3** In the **Local Users** area (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.