



Managing User Accounts

This chapter includes the following sections:

- [Configuring Local Users, on page 1](#)
- [Password Expiry, on page 3](#)
- [LDAP Servers, on page 4](#)
- [TACACS+ Server, on page 16](#)
- [Verify the TACACS+ Server Configuration for CIMC version 3.2.10 and 3.2.11, on page 18](#)
- [Verify the TACACS+ Server Configuration for CIMC with Accounting, on page 18](#)
- [Viewing User Sessions, on page 18](#)

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.

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 configure or 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** dialog box, update the following properties:

| 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: <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• 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. |
| Enabled check box | If checked, the user is enabled on the . |
| 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. 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 rules 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 Users 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 Enter password information.

Step 7 Click **Save Changes**.

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.

LDAP Servers

supports directory services that organize information in a directory, and manage access to this information. supports Lightweight Directory Access Protocol (LDAP), which stores and maintains directory information in a network. In addition, 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 utilizes the Kerberos-based authentication service of LDAP.

When LDAP is enabled in the , 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`.

you can require the server to encrypt data sent to the LDAP server.

Configuring the LDAP Server

The 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 . You can use an existing LDAP attribute that is mapped to the 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 user roles and locales.

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 |

| Properties | Value |
|------------|-----------------------|
| 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 :

| 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 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 Encryption check box | If checked, the server encrypts all information it sends to the LDAP server. |
| Enable Binding CA Certificate check box | If checked, allows you to bind the LDAP CA certificate. |
| Timeout (0 - 180) seconds | The number of seconds the waits until the LDAP search operation times out. If the search operation times out, 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. |
| User Search Precedence | Allows you to specify the order of search between the local user database and LDAP user database. This can be one of the following: <ul style="list-style-type: none"> • Local User Database (Default setting) • LDAP User Database |

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.

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 | |

| Name | Description |
|---|---|
| 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> |
| 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 user roles and locales, or can modify the schema such that a new LDAP attribute can be created. For example, CiscoAvPair.</p> <p>Note If you do not specify this property, the user cannot login. Although the object is located on the LDAP server, it should be an exact match of the attribute that is specified in this field.</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, enables the Configure Group button.</p> |
| 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. |

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

Step 9 Click **Save Changes**.

LDAP Certificates Overview

Cisco E-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** 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 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 | <p>Selecting this option allows you to choose the certificate from a remote location 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 to Local Desktop | <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 Certificate**.

Downloading 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** Click the **Download LDAP CA Certificate** link.
- The **Download LDAP CA Certificate** dialog box appears.

| Name | Description |
|---|--|
| Download from remote location radio button | <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 should use when downloading 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. |
| Download through browser client radio button | <p>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.</p> <p>When you select this option, Cisco IMC GUI displays a Browse button that lets you navigate to the file you want to import.</p> |
| Paste Certificate content radio button | <p>Selecting this option allows you to copy the entire content of the signed certificate and paste it in the Paste certificate content text field.</p> <p>Note Ensure the certificate is signed before uploading.</p> |
| Download Certificate button | Allows you to download 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** 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 **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**.

Deleting an LDAP CA Certificate

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** menu, click **User Management**.
- Step 3** In the **User Management** pane, click the **LDAP** tab.
- Step 4** Click the **Delete LDAP CA Certificate** link and click **OK** to confirm.

TACACS+ Server

TACACS+ is a security application that provides centralized validation of users attempting to gain access to a router or network access server. TACACS+ services are maintained in a database on a TACACS+ server running, typically, on a UNIX or Windows NT workstation. You must configure a TACACS+ server before you configure the TACACS+ features on your network access server and make them available.

On the TACACS+ server, ensure you configure Cisco attribute-value (AV) pair privilege level (priv-lvl) for Cisco Integrated Management Controller (CIMC) service for the minimum privilege level of administrators and operators.



Note

In CIMC 3.2.10 release or earlier, users with no privilege level or users with a privilege level less than the operator's privilege level were considered as auditors with read-only permissions.

From CIMC 3.2.10 release, users with privilege level zero do not have permissions to login to CIMC.

After the software is downgraded to a version that supports 15 characters, ensure to change the shared key to 15 characters.

Restrictions for TACACS+ Server

The following restrictions are applicable for CIMC 3.2.10 release:

- CIMC 3.2.10 release supports connection to a single TACACS+ server. From CIMC 3.2.12 release onwards, 3 TACACS+ server configuration is supported.
- Users must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.
- Accounting is not supported in CIMC 3.2.10 release. From CIMC 3.2.13 release onwards, TACACS accounting is supported. TACACS accounting will send all the configuration commands executed in CIMC GUI/CLI to TACACS server. Show commands executed in CIMC CLI/GUI will not be sent to TACACS server.
- TACACS+ and LDAP configurations are exclusive, only one configuration is enabled at a time
- Default time out is five seconds
- Default TCP port connection is 49
- Default login is PAP login where the username and password arrive at the network access server in a PAP protocol packet instead of details entered by the user.
- Supports only for IPv4
- Pre-shared key size is 15 characters. From CIMC 3.2.12 release onwards, shared key size is increased from 15 to 32.

Supported special characters in shared secret key are: ! @ % ^ * - _ & + =

Configure TACACS Server

Before you begin

Log in to CIMC as a user with admin privileges.

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** menu, click **TACACS** tab.
- Step 4** In the TACACS Settings area, update the following properties:

Table 1:

| | |
|--------------------------------|--|
| Enable TACACS check box | If checked, user authentication and role authorization is performed first by the TACACS server, followed by user accounts that are not found in the local user database. |
| Admin priv | Sets the privilege level to the administrator. The privilege level 14 is assigned to the administrator role, and privilege level 9 is assigned to the operator role - a user with privilege level 14 or higher has admin privileges when the user logs into the system. By default, admin privilege is 15. |
| Oper priv | A user with privilege level 9 or higher has all privileges of an operator at the time of login. By default, operator privilege is 11. |
| TACACS Server | Enter the TACACS server IP address. This option provides three slots for storing IP addresses (TACACS Server IP 1, 2, and 3). After you set the TACACS Server IP, set the corresponding Pre-Shared key. |
| Pre-Shared Key | <p>Sets the pre-shared key to initiate authentication with the server. This option provides three slots for Pre-Shared key (Shared Key 1,2, and 3).</p> <p>From CIMC 3.2.12 release onwards, the maximum length of the key is 32 characters.</p> |

| | |
|------------------------------------|--|
| TACACS Accounting check box | <p>If enabled, TACACS Accounting functionality will be enabled and all the configuration commands executed in CIMC GUI/CLI will be sent to TACACS server.</p> <p>Show commands executed in CIMC CLI/GUI will not be sent to TACACS server.</p> |
|------------------------------------|--|

Verify the TACACS+ Server Configuration for CIMC version 3.2.10 and 3.2.11

```

ENCS5406-FGL224331J8/tacacs#show detail
tacacs Settings:
Server domain name or IP address: 10.197.82.23
Enable tacacs: yes
shared-secret key: *****
admin-priv: 14
oper-priv: 10

```

Verify the TACACS+ Server Configuration for CIMC with Accounting

This example shows TACACS+ configuration with Accounting.

```

ENCS5406 # scope tacacs
ENCS5406 /tacacs # show detail
TACACS Settings:
Enable tacacs: yes
Enable tacacs cmd accounting: yes
Server1 domain name or IP addr: 192.168.1.1
Server2 domain name or IP addr: 192.168.1.2
Server3 domain name or IP addr: 192.168.1.3
Server1 Shared-secret key: *****
Server2 Shared-secret key: *****
Server3 Shared-secret key: *****
Admin-priv: 15
Oper-priv: 11

```

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 |
|--------------------------|---|
| 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 | <p>The type of session the user chose to access the server. This can be one of the following:</p> <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. |

