



Managing User Accounts

This chapter includes the following sections:

- [Configuring Local Users, page 1](#)
- [Configuring Active Directory, page 2](#)
- [Viewing User Sessions, page 5](#)
- [Terminating a User Session, page 5](#)

Configuring Local Users

Before You Begin

You must log in as a user with admin privileges to configure local users.

Procedure

	Command or Action	Purpose
Step 1	Server# scope user <i>usernumber</i>	Enters user command mode for user number <i>usernumber</i> .
Step 2	Server /user # set enabled { yes no }	Enables or disables the user account on the CIMC.
Step 3	Server /user # set name <i>username</i>	Specifies the username for the user.
Step 4	Server /user # set password	You are prompted to enter the password twice.
Step 5	Server /user # set role { readonly user admin }	Specifies the role assigned to the user. The roles are as follows: <ul style="list-style-type: none">• readonly—This user can view information but cannot make any changes.• user—This user can do the following:<ul style="list-style-type: none">• View all information

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

This example configures user 5 as an admin:

```

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

```

Configuring Active Directory

Active Directory

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 CIMC utilizes the Kerberos-based authentication service of Active Directory.

When Active Directory is enabled in the CIMC, all user authentication and role authorization is performed by Active Directory, and the CIMC ignores the local database. If the CIMC cannot connect to Active Directory, it reverts to the local database.

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

Configuring the Active Directory Server

The CIMC can be configured to use Active Directory for user authentication and authorization. To use Active Directory, configure users with an attribute that holds the user role and locale information for the CIMC. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can modify the Active Directory 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. For more information about altering the Active Directory schema, see the article at <http://technet.microsoft.com/en-us/library/bb727064.aspx>.

The following steps are to be performed on the Active Directory server.



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

Procedure

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

Step 2 Using the Active Directory 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 Active Directory snap-in:

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

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

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 CIMC to configure Active Directory.

Configuring Active Directory in the CIMC

Configure Active Directory in the CIMC when you want to use an Active Directory server for local user authentication and authorization.

Before You Begin

You must be logged in as admin to configure Active Directory.

Procedure

	Command or Action	Purpose
Step 1	Server# scope ldap	Enters the Active Directory command mode.
Step 2	Server /ldap # set enabled {yes no}	Enables or disables Active Directory. When Active Directory is enabled, user authentication and role authorization is performed by Active Directory for user accounts not found in the local user database.
Step 3	Server /ldap # set server-ip ip-address	Specifies the Active Directory server IP address.
Step 4	Server /ldap # set timeout seconds	Specifies the number of seconds the CIMC waits until it assumes the connection to Active Directory cannot be established.
Step 5	Server /ldap # set encrypted {yes no}	If encryption is enabled, the server encrypts all information sent to Active Directory.
Step 6	Server /ldap # set base-dn domain-name	Specifies the domain that all users must be in.
Step 7	Server /ldap # set attribute name	Specify an LDAP attribute that contains the role and locale information for the user. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. You can use an existing LDAP attribute that is mapped to the CIMC user roles and locales or you can create a custom attribute, such as the CiscoAVPair attribute, which has the following attribute ID: 1.3.6.1.4.1.9.287247.1 Note If you do not specify this property, user access is restricted to read-only.
Step 8	Server /ldap # commit	Commits the transaction to the system configuration.
Step 9	Server /ldap # show [detail]	(Optional) Displays the Active Directory configuration.

This example configures Active Directory using the CiscoAVPair attribute:

```
Server# scope ldap
Server /ldap # set enabled yes
```

```

Server /ldap *# set server-ip 10.10.10.123
Server /ldap *# set timeout 60
Server /ldap *# set encrypted on
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# commit
Server /ldap # show
Server IP          BaseDN          Encrypted Timeout  Enabled Attribute
-----
10.10.10.123      example.com    yes      60      yes     CiscoAvPair
Server /ldap #
    
```

Viewing User Sessions

Procedure

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

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

Name	Description
ID	The unique identifier for the session.
Name	The username for the user.
IP Address	The IP address from which the user accessed the server.
Type	The method by which the user accessed the server.
Killable	If your user account has admin privileges, this column displays yes if you can force the associated user session to end. Otherwise it displays N/A . Note You cannot terminate your current session.

This example displays information about current user sessions:

```

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

Terminating a User Session

Before You Begin

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

Procedure

	Command or Action	Purpose
Step 1	Server# show user-session	Displays information about current user sessions. The user session to be terminated must be eligible to be terminated (killable) and must not be your own session.
Step 2	Server /user-session # scope user-session <i>session-number</i>	Enters user session command mode for the numbered user session that you want to terminate.
Step 3	Server /user-session # terminate	Terminates the user session.

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

```

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

Server /user-session #

```