Managing User Accounts

This chapter includes the following sections:

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 checking the Enable Encryption check box in the **Active Directory Properties** area, you can require the server to encrypt data sent to Active Directory.

Configuring Active Directory in CIMC

Before You Begin

You must log in as a user with admin privileges to configure active directory.

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 **Active Directory** tab.

Step 4 In the **Active Directory Properties** area, update the following properties:

Name	Description
Enabled check box	If checked, all user authentication and role authorization is performed by Active Directory and CIMC ignores the local user database. **Note** If the CIMC cannot establish a connection to Active Directory, it automatically reverts back to using the local user database.
Server IP Address field	The Active Directory server IP address.
Timeout field	The number of seconds the CIMC waits until it assumes the connection to Active Directory cannot be established.
Enable Encryption check box	If checked, the server encrypts all information it sends to Active Directory.
Domain field	The domain that all users must be in.
Attributes field	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 must have 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 5 Click **Save Changes**.

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 Local Users

Before You Begin

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

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** tab.

Step 4 To configure a local user, click in a row.

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

Name	Description
ID column	The unique identifier for the user.
Enabled check box	If checked, the user is enabled on the CIMC.
User Name column	The user name for the user.
Role column	The role assigned to the user. This can be: • **read-only**—This user can view information but cannot make any changes. • **user**—This user can: ◦ 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 • **admin**—This user can perform all actions available through the GUI, CLI, and IPMI.

Step 6 Enter password information.

Step 7 Click **Save Changes**.

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.
Username column	The user name for the user.
IP Address column	The IP address from which the user accessed the server.
Type column	The method by which the user accessed the server.
Action column	If your user account has admin privileges, this column displays **Terminate** if you can force the associated user session to end. Otherwise it displays **N/A**. **Note** You cannot terminate your current session from this tab.