Manage Credential Policies

- Credential Policy and Authentication, on page 1
- Configure a Credential Policy, on page 2
- Configure a Credential Policy Default, on page 2
- Monitor Authentication Activity, on page 3
- Configuring Credential Caching, on page 4
- Manage Session Termination, on page 4

Credential Policy and Authentication

The authentication function authenticates users, updates credential information, tracks and logs user events and errors, records credential change histories, and encrypts or decrypts user credentials for data storage.

The system always authenticates application user passwords and end user PINs against the Unified Communications Manager database. The system can authenticate end user passwords against the corporate directory or the database.

If your system is synchronized with the corporate directory, either the authentication function in Unified Communications Manager or lightweight directory access protocol (LDAP) can authenticate the password:

- With LDAP authentication enabled, user passwords and credential policies do not apply. These defaults are applied to users that are created with directory synchronization (DirSync service).
- When LDAP authentication is disabled, the system authenticates user credentials against the database. With this option, you can assign credential policies, manage authentication events, and administer passwords. End users can change passwords and PINs through the phone user interfaces.

Credential policies do not apply to operating system users or CLI users. These administrators use standard password verification procedures that the operating system supports.

After users are configured in the database, the system stores a history of user credentials in the database to prevent users from entering previous information when users are prompted to change their credentials.

JTAPI and TAPI Support for Credential Policies

Because the Cisco Unified Communications Manager Java telephony applications programming interface (JTAPI) and telephony applications programming interface (TAPI) support the credential policies that are

assigned to application users, developers must create applications that respond to the password expiration, PIN expiration, and lockout return codes for credential policy enforcement.

Applications use an API to authenticate with the database or corporate directory, regardless of the authentication model that an application uses.

For more information about JTAPI and TAPI for developers, see the developer guides at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html.

Configure a Credential Policy

Credential policies apply to application users and end users. You assign a password policy to end users and application users and a PIN policy to end users. The Credential Policy Default Configuration lists the policy assignments for these groups. When you add a new user to the database, the system assigns the default policy. You can change the assigned policy and manage user authentication events.

Note Ensure that the Inactive Days Allowed parameter under the Credential Policy Settings is set to 0 (unlimited) for CTI application users. Else, the application users unexpectedly become inactive and the CTI applications may fail to connect to Unified CM after restart.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy**.

Step 2 Perform one of the following steps:

- Click **Find** and select an existing credential policy.
- Click **Add New** to create a new credential policy.

Step 3 Complete the fields in the **Credential Policy Configuration** window. See the online help for more information about the fields and their configuration settings.

Step 4 Click **Save**.

Configure a Credential Policy Default

At installation, Cisco Unified Communications Manager assigns a static default credential policy to user groups. It does not provide default credentials. Your system provides options to assign new default policies and to configure new default credentials and credential requirements for users.

Procedure

Step 1 In Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy Default**.

Step 2 From the **Credential Policy** drop-down list box, choose the credential policy for this group.

Step 3 Enter the password in both the **Change Credential** and **Confirm Credential** configuration windows.

Step 4 Check the **User Cannot Change** check box if you do not want your users to be able to change this credential.

Step 5 Check the **User Must Change at Next Login** check box if you want to use this credential as a temporary credential that an end user must change the next time that they login.

Note Please note that, if you check this box, your users are unable to change PIN using Personal Directory service.

Step 6 If you do not want the credential to expire, check the **Does Not Expire** check box.

Step 7 Click **Save**.

Monitor Authentication Activity

The system shows the most current authentication results, such as last hack attempt time, and counts for failed logon attempts.

The system generates log file entries for the following credential policy events:

- Authentication success
- Authentication failure (bad password or unknown)
- Authentication failure because of
  - Administrative lock
  - Hack lock (failed logon lockouts)
  - Expired soft lock (expired credential)
  - Inactive lock (credential not used for some time)
  - User must change (credential set to user must change)
  - LDAP inactive (switching to LDAP authentication and LDAP not active)
- Successful user credential updates
- Failed user credential updates

Note If you use LDAP authentication for end user passwords, LDAP tracks only authentication successes and failures.

All event messages contain the string “ims-auth” and the user ID that is attempting authentication.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End Users**.

Step 2 Enter search criteria, click **Find**, and then choose a user from the resulting list.

Step 3 Click **Edit Credential** to view the user's authentication activity.

What to do next

You can view log files with the Cisco Unified Real-Time Monitoring Tool (Unified RTMT). You can also collect captured events into reports. For detailed steps about how to use Unified RTMT, see the *Cisco Unified Real-Time Monitoring Tool Administration Guide* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

Configuring Credential Caching

Enable credential caching to increase system efficiency. Your system does not have to perform a database lookup or invoke a stored procedure for every single login request. An associated credential policy is not enforced until the caching duration expires.

This setting applies to all Java applications that invoke user authentication.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Enterprise Parameters**.

Step 2 Perform the following tasks as needed:

- Set the **Enable Caching** enterprise parameter to **True**. With this parameter enabled, Cisco Unified Communications Manager uses cached credentials for up to 2 minutes.
- Set the **Enable Caching** enterprise parameter to **False** to disable caching, so that the system does not use cached credentials for authentication. The system ignores this setting for LDAP authentication. Credential caching requires a minimal amount of additional memory per user.

Step 3 Click **Save**.

Manage Session Termination

Administrators can use this procedure to terminate a user's active sign-in session specific to each node.

Note

- An administrator with privilege level 4 only can terminate the sessions.
- Session Management terminates the active sign-in sessions on a particular node. If the administrator wants to terminate all the user sessions across different nodes, then the administrator has to sign-in to each node and terminate the sessions.

This applies to the following interfaces:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified Communications Self Care Portal
- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting

Procedure

Step 1 From Cisco Unified OS Administration or Cisco Unified IM and Presence OS Administration, choose **Security** > **Session Management**.
The Session Management window is displayed.

Step 2 Enter the user ID of the active signed-in user in the **User ID** field.

Step 3 Click **Terminate Session**.

Step 4 Click **OK**.

If the terminated user refreshes the signed-in interface page, then the user is signed out. An entry is made in the audit log and it displays the terminated `userID`.