Credential Policies

Credential Policy Overview

Credential policies control the authentication process for resources in Cisco Unified Communications Manager. A credential policy defines password requirements and account lockout details such as failed login attempts, expiration periods and lockout durations for end user passwords, end user PINs, and application user passwords. Credential policies can be assigned broadly to all accounts of a specific credential types, such as all end user PINs, or they can be customized for a specific application user, or end user.

Credential Types

In Credential Policy Configuration you can configure a new credential policy and then apply that new policy as the default credential policy for each of the following three credential types:

- End User PINs
- End User Passwords
- Application User Passwords

You can also apply the credential policy to a specific end user PIN, end user password, or application user password.

Credential Policies with LDAP Authentication Enabled

If your system is configured for LDAP Authentications with the corporate directory:

- With LDAP Autthentication enabled, credential policies do not apply to end user passwords.
- Credential policies do apply to end user PINs and application user passwords, irrespective of whether LDAP Authentication is enabled. These password types use local authentication.

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

Trivial Passwords

The system can be configured to check for trivial passwords and PINs. A trivial password is a credential that can be easily hacked, such as a password that be guessed easily such as using ABCD as your password or 123456 as your PIN.

Non-trivial passwords meet the following requirements:

- Must contain three of the following four characteristics: uppercase character, lowercase character, number, or symbol.
- Must not use a character or number more than three times consecutively.
- Must not repeat or include the alias, username, or extension.
- Cannot consist of consecutive characters or numbers. For example, passwords such as 654321 or ABCDEFG are not allowed.

PINs can contain digits (0-9) only. A non-trivial PIN meets the following criteria:

- Must not use the same number more than two times consecutively.
- Must not repeat or include the user extension, mailbox, or the reverse of the user extension or mailbox.
- Must contain three different numbers. For example, a PIN such as 121212 is trivial.
- Must not match the numeric representation (that is, dial by name) for the first or last name of the user.
- Must not contain groups of repeated digits, such as 408408, or patterns that are dialed in a straight line on a keypad, such as 2580, 159, or 753.

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 Default Credential Policy

Use this procedure to configure clusterwide default credential policies that get applied to newly provisioned users. You can apply a separate credential policy for each of the following credential types:

- Application User Passwords
- End User Passwords
- End User PINs

Step 1 Configure settings for a credential policy:

a) From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy**.
b) Do either of the following:
   - Click **Find** and select an existing credential policy.
   - Click **Add New** to create a new credential policy.
c) If you want the system to check for easily hacked passwords such as ABCD or 123456, check the **Check for Trivial Passwords** check box.
d) Complete the fields in the **Credential Policy Configuration** window. For help with the fields and their settings, see the online help.
e) Click **Save**.
f) If you want to create a different credential policy for one of the other credential types, repeat these steps.

Step 2 Apply the credential policy to one of the credential types:

a) From Cisco Unified CM Administration, choose **User Management** > **User Settings** > **Credential Policy Default**.
b) Select the credential type to which you want to apply your credential policy.
c) From the **Credential Policy** drop-down, select the credential policy that you want to apply for this credential type. For example, you might select the credential policy that you created.
d) Enter the default passwords in both the **Change Credential** and **Confirm Credential** fields. Users have to enter these passwords at next login.
e) Configure the remaining fields in the **Credential Policy Default Configuration** window. For help with the fields and their settings, see the online help.
f) Click **Save**.
g) If you want to assign a credential policy for one of the other credential types, repeat these steps.

Note For individual users, you can also assign a policy to a specific user credential from the **End User Configuration** window or **Application User Configuration** window for that user. Click the **Edit Credential** button that is adjacent to the credential type (password or PIN) to open the **Credential Configuration** settings for that user credential.

Edit User Credentials or Credential Policy

Use this procedure if you want to edit an existing user credential or to edit the policy that is assigned to a user credential. After resetting the credential, you can apply a rule such as mandating that the user update credentials at next login. You may want to do this if:

- You have local DB authentication configured, and you want to reset an end user password
- You want to reset an end user PIN or application user password
- You want to change the credential policy that is assigned to a specific user credential

Step 1 From Cisco Unified CM Administration, choose one of the following:

- For end user passwords and PINs, choose **User Management** > **End Users**.
- For application user passwords, choose **User Management** > **Application Users**.

Step 2 Click **Find** and select the appropriate user.

Step 3 If you want to change an existing password or PIN, enter the new credential in the **Password**/**Confirm Password** or **PIN**/**Confirm PIN** fields and click **Save**.

Step 4 If you want to change the credential policy that is assigned to a user credential, or if you want to apply rules such as requiring that the user enter a new password or PIN at next login:

a) Click the **Edit Credential** button that is adjacent to the **Password** or **PIN**. The **Credential Configuration** window opens for that user credential.
b) Optional. To assign a new credential policy, select the policy from the **Authentication Rule** drop-down.
c) Optional. Check the **User Must Change at Next Login** check box if you want the user to update the password or PIN at the next login.
d) Complete the remaining fields. Refer to the online help for field descriptions.
e) Click **Save**.

Enable PIN Synchronization

Use this procedure to enable PIN synchronization so that the end users can log in to Extension Mobility, Conference Now, Mobile Connect, and the Cisco Unity Connection Voicemail using the same PIN.

Note The pin synchronization between Cisco Unity Connection and Cisco Unified Communications Manager is successful, only when Cisco Unified Communications Manager publisher database server is running and completes its database replication. Following error message is displayed when the pin synchronization fails on Cisco Unity Connection: `Failed to update PIN on CUCM. Reason: Error getting the pin.`

If the PIN Synchronization is enabled and the end user changes the pin, then pin is updated in Cisco Unified Communications Manager. This happens only when the pin update is successful in at least one of the configured Unity Connection Application servers.

Note For PIN Synchronization to take effect, administrators must force the users to change their PIN after successfully enabling the feature.

Before you begin

This procedure assumes that you already have your application server connection to Cisco Unity Connection setup. If not, for more information on how to add a new application server, see the Related Topics section.

To enable PIN Synchronization feature, you need to first upload a valid certificate for the Cisco Unity Server connection from the Cisco Unified OS Administration page to the Cisco Unified Communications Manager tomcat-trust. For more information on how to upload the certificate, see the "Manage Security Certificates" chapter in the *Administration Guide for Cisco Unified Communications Manager* at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

The user ID in the Cisco Unity Connection Server must match the user ID in Cisco Unified Communications Manager.

Step 1 From Cisco Unified CM Administration, choose **System** > **Application Servers**.

Step 2 Select the application server that you set up for Cisco Unity Connection.

Step 3 Check the **Enable End User PIN Synchronization** check box.

Step 4 Click **Save**.

Related Topics

Configure Application Servers

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.

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.

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

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`.