Configure Credential Policy

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.

Secure End Users Login Credentials

From Unified Communications Manager Release 12.5(1), all end users login credentials are hashed with SHA2 to provide enhanced security. Earlier than Unified Communications Manager Release 12.5(1), all end users login credentials were hashed with SHA1 only. Unified Communications Manager Release 12.5(1) also includes the “UCM Users with the Out-Of-Date Credential Algorithm” report. This report is available in the Cisco Unified Reporting page. This report helps the administrator to list all the end users whose passwords or PINs are hashed with SHA1.

All end users passwords or PINs that are hashed with SHA1 are migrated to SHA2 automatically upon their first successful login. The end users with SHA1 hashed (out of date) credentials can update their PINs or passwords using one of the following ways:

- Update the PIN by logging into Extension Mobility or Directory access on the phone.
- Update the password by logging into Cisco Jabber, Cisco Unified Communications Self Care Portal, or Cisco Unified CM Administration.

For more information on how to generate the report, see the *Cisco Unified CM Administration Online Help*.

Credential Policy Configuration Task Flow

Procedure

	Command or Action	Purpose
Step 1	Configure a Credential Policy, on page 3	Configure credential policies for end users and application users.
Step 2	Configure Default Credentials for a Credential Policy, on page 4	Apply the configured credential policy as the default credential policy for any of three credential types: end user passwords, and application users. The default credential policy will be applied by default to that credential type for newly provisioned users.

Related Topics

Apply Credential Policy to End User

Configure a Credential Policy

Configure a credential policy that you can apply as the default credential policy for all credentials that match a specific credential type such as end user PINs or end user passwords.

Note Ensure that the **Inactive Days Allowed** parameter under the Credential Policy Settings is set to 0 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**.

What to do next

Configure Default Credentials for a Credential Policy, on page 4

Configure Default Credentials for a Credential Policy

Perform these steps to configure the default credentials for your credential policy. You can assign default credentials to assign a temporary password that a user must change upon their next login.

Before you begin

Configure a Credential Policy, on page 3

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**.

What to do next

If you want to apply a credential policy to a specific end user or PIN:

- Apply Credential Policy to End User