Credential Policy Setup

This chapter provides information to configure credential policies.

About Credential Policy Setup

In Cisco Unified Communications Manager Administration, use the **User Management** > **Credential Policy** menu path to configure credential policies.

The Credential Policy Configuration window in Cisco Unified Communications Manager Administration allows you to configure credential policies to secure user accounts.

A policy comprises a set of rules that controls access to a system or network resource. A credential policy defines password requirements and account lockouts for user accounts. Credential policies that are assigned to user accounts control the authentication process in Cisco Unified Communications Manager. After you add a credential policy, you can assign the new policy as the default policy for a credential type or to an individual application or end user.

At installation, Cisco Unified Communications Manager assigns a static credential policy to end user PINs and to application and end user passwords. The policy contains settings for failed login resets, lockout durations, expiration periods, and credential requirements. The Credential Policy Configuration window allows you to configure new credential policies for your system or site. You cannot change the static policy.

Credential Policies Configuration Tips

The system provides trivial credential checks to disallow credentials that are easily hacked. You enable trivial credential checks by checking the Check for Trivial Passwords check box in the Credential Policy Configuration window.

Passwords can contain any alphanumeric ASCII character and all ASCII special characters. A non-trivial password meets the following criteria:

- Must contain three of the four allowable characteristics: uppercase character, lowercase character, number, 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)

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 or 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.

Tip You cannot modify the system Default Credential Policy.

Next Steps

You can assign the new credential policy as a default policy for a credential type, or to individual users.

Credential Policy Deletion

Note You cannot delete a credential policy if it is assigned as the default policy for end user passwords, end user PINS, or application user passwords.

To find out which default policies use the credential policy, choose Dependency Records from the Related Links drop-down list box in the Credential Policy Configuration window and click Go.

If the dependency records feature is not enabled for the system, the dependency records summary window displays a message that shows the action that you can take to enable the dependency records. The message also displays information about high CPU consumption that is related to the dependency records feature.

If you attempt to delete a credential policy that is in use, a message displays. To delete a credential policy that is currently in use, you must either choose a different credential policy for the user or create and assign a new policy.

Credential Policy Settings

Field	Description
Display Name	Specify the credential policy name. Enter up to 64 characters, except for quotation marks. Do not enter tab.

Field	Description
Failed Logon / No Limit for Failed Logons	Specify the number of allowed failed login attempts. When this threshold is reached, the system locks the account. Enter a number in the range 1-100. To allow unlimited failed logins, enter 0 or check the No Limit for Failed Logons check box. Uncheck the check box to enter a value greater than 0. The default setting specifies 3.
Reset Failed Logon Attempts Every	Specify the number of minutes before the counter is reset for failed login attempts. After the counter resets, the user can try logging in again. Enter a number in the range 1-120. The default setting specifies 30.
Lockout Duration / Administrator Must Unlock	Specify the number of minutes an account remains locked when the number of failed login attempts exceeds the specified threshold. Enter a number in the range 1-1440. Enter 0 or check the Administrator Must Unlock check box, so accounts will remain locked until an administrator manually unlocks them. Uncheck the check box to enter a value greater than 0. The default setting specifies 30.
Minimum Duration Between Credential Changes	Specify the number of minutes that are required before a user can change credentials again. Enter 0 to allow a user to change credentials at any time. Uncheck the check box to enter a value greater than 0. The default setting specifies 0.
Credential Expires After / Never Expires	Specify the number of days before a credential will expire. Enter a number in the range 1-365.To allow credentials to never expire, enter 0 or check the Never Expires check box. Uncheck the check box to enter a value greater than 0. Use the 0 option for low-security accounts or multiple user accounts, for example. The default setting specifies 180.
Minimum Credential Length	Specify the minimum length for user credentials (password or PIN). Do not enter 0 because blank passwords are not allowed. The default setting specifies 8. The minimum setting must equal at least 1.

Field	Description
Stored Number of Previous Credentials	Specify the number of previous user credentials to store. This setting prevents a user from configuring a recently used credential that is saved in the user list. Enter a number in the range 0-25. If no previous credentials should be stored, enter 0. The default setting specifies 12.
Inactive Days Allowed	Specify the number of days that a password can remain inactive before the account gets locked. Enter a number in the range 0-5000. The default setting specifies 0.
Expiry Warning Days	Enter a number in the range 0-90 to specify the number of days before a user password expires to start warning notifications. The default setting specifies 0.
Check for Trivial Passwords	Check this check box to require the system to disallow credentials that are easily hacked, such as common words and repeated character patterns. The default setting is checked.