Credential Policy Default Setup

This chapter provides information to configure credential policies.

About Credential Policy Default Setup

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

The Credential Policy Default window provides options to change the default credential policy assignment for a user and credential type (for example, end user PINs). At installation, Cisco Unified Communications Manager assigns the system Default Credential Policy to end user passwords, end user PINs, and application user passwords. The system applies the application password that you configured at installation to all application users. You can assign a new default credential policy and configure new default credentials after installation.

Credential Policy Defaults Configuration Tips

The system provides the default credential policy to facilitate installs and upgrades. The default credential policy settings differ from the credential policy defaults settings that are used to add a new credential policy.

Note The system does not support empty (null) credentials. If your system uses LDAP authentication, you must configure end user default credentials immediately after installation, or logins will fail.

You can also assign a new user credential policy, manage user authentication events, or view credential information for a user in the user configuration windows.

Credential Policy Default Settings

Field	Description
Credential User	This field displays the user type for the policy that you selected in the Find and List Credential Policy Defaults window. You cannot change this field.
Credential Type	This field displays the credential type for the policy that you selected in the Find and List Credential Policy Defaults window. You cannot change this field.
Credential Policy	Choose a credential policy default for this credential group. The list box displays the predefined Default Credential Policy and any credential policies that you created.
Change Credential	Enter up to 127 characters to configure a new default credential for this group.
Confirm Credential	For verification, reenter the login credential that you entered in the Change Credential field.
User Cannot Change	Check this check box to block users that are assigned this policy from changing this credential. You cannot check this check box when User Must Change at Next Login is checked. The default setting for this check box specifies unchecked.
User Must Change at Next Login	Check this check box to require users that are assigned this policy to change this credential at next login. Use this option after you assign a temporary credential. You cannot check this check box when the User Cannot Change check box is checked. The default setting for this check box specifies checked.
Does Not Expire	Check this check box to block the system from prompting the user to change this credential. You can use this option for low-security users or group accounts. If this check box is checked, the user can still change this credential at any time. When this check box is unchecked, the expiration setting in the associated credential policy applies. The default setting for this check box specifies unchecked.

Assign and Set Up Credential Policy Defaults

This section describes how to assign a new credential policy and new default credentials to a credential group. At installation, the system assigns a default credential policy to the credential groups.

Note Upgrades from 5.x releases automatically migrate application and end user passwords and PINs.

Before you begin

To assign a default credential policy other than the predefined Default Credentials Policy, you must first create the policy.

Procedure

Step 1 Choose **User Management** > **Credential Policy Default**.

The Find and List Find and List Credential Policy Defaults window displays.

Step 2 Click the list item to change.

The Credential Policy Default Configuration window displays with the current settings.

Step 3 Enter the appropriate settings, as described in #unique_603 unique_603_Connect_42_table34, on page 2, using these guidelines:

a) To change the applied credential policy, select the policy from the drop-down list box.
b) To change the default credential, enter and confirm the new credential in the appropriate fields.
c) To change credential requirements, check or uncheck the appropriate check boxes.

Step 4 Click the Save button or the Save icon.

What to do next

You can assign a new user credential policy, manage user authentication events, view credential information for a user, or configure a unique password for the user.

The Bulk Administration Tool (BAT) allows administrators to define common credential parameters, such as passwords and PINs, for a group of users in the BAT User Template. See the Cisco Unified Communications Manager Bulk Administration Guide for more information.

End users can change PINs at the phone user pages; end users can change passwords at the phone user pages when LDAP authentication is not enabled. See the documentation for your Cisco Unified IP Phone for more information.