CHAPTER 18

Specifying Password, PIN, Sign-In, and Lockout Policies in Unity Connection 8.x

See the applicable sections, depending on your configuration:

- Cisco Unified Communications Manager Business Edition (CMBE) Only, page 18-1
- Unity Connection Only, page 18-1

Cisco Unified Communications Manager Business Edition (CMBE) Only

In Cisco Unified Communications Manager Business Edition (CMBE), you use Cisco Unified Communications Manager Administration to specify password, PIN, and account lockout policies for phone and web-tool access, and to specify the sign-in policy for web-tool access for all users who access Unity Connection voice messages.

The policies are specified on the User Management > Credential pages in Cisco Unified CM Administration. See the online Help, or the *Cisco Unified Communications Manager Administration Guide* for details and related topics. (Administration documentation for Cisco Unified Communications Manager is available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.)

Note that although you cannot set password, PIN, sign-in, and lockout policies in Cisco Unity Connection Administration, you can change a Unity Connection user password or PIN on the user account page. See the "Passwords and PINs" section in the "Setting Up Features and Functionality Controlled By User Account Settings in Unity Connection 8.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 8.x*, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx/8xcucmac040.html. Alternatively, users can change their own passwords and PINs in the Unity Connection Messaging Assistant.

Unity Connection Only

In Unity Connection, you use authentication rules to determine the password, PIN, and account lockout policies for phone and web-tool access, and to specify the sign-in policy for web-tool access for all users who access Unity Connection voice messages.

See the following sections:

- Specifying Password, PIN, Sign-In, and Lockout Policies Using Authentication Rules, page 18-2
- Creating and Modifying Authentication Rules, and Assigning Rules to Users, page 18-2

Specifying Password, PIN, Sign-In, and Lockout Policies Using Authentication Rules

In Unity Connection, authentication rules govern user passwords, PINs, and account lockouts for all user accounts. You use authentication rules to secure how users access Unity Connection by phone, and how users access Cisco Unity Connection Administration and the Cisco Personal Communications Assistant (PCA).

For example, an authentication rule determines:

- The number of failed sign-in attempts that are allowed before an account is locked
- The number of minutes an account remains locked before it is reset
- Whether a locked account must be unlocked manually by an administrator
- The minimum length allowed for passwords and PINs
- The number of days before a password or PIN expires

Creating and Modifying Authentication Rules, and Assigning Rules to Users

Authentication rules are specified on the System Settings > Authentication Rules page in Cisco Unity Connection Administration. Unity Connection includes the following predefined authentication rules:

Recommended Voicemail Authentication Rule	By default, Unity Connection applies this rule to the voicemail PIN on the Password Settings page of each user account and user template for which you set up user access to Unity Connection by phone.
Recommended Web Application Authentication Rule	By default, Unity Connection applies this rule to the Web Application password on the Password Settings page of each user account and user template for which you set up user access to Cisco Unity Connection Administration, or to the Cisco Personal Communications Assistant.

You can change these defaults, and can create an unlimited number of additional authentication rules.

For user accounts and templates, you specify the authentication rule that governs user access to Unity Connection. For information on specifying an authentication rule for a user account or template, see the "Passwords and PINs in Cisco Unity Connection 8.x" section in the "Setting Up Features and Functionality Controlled By User Account Settings in Unity Connection 8.x" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 8.x*, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx/8xcucmac040.html.