CHAPTER 18

Specifying Password, Logon, and Lockout Policies

See the applicable sections, depending on your configuration:

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 and account lockout policies for phone and web-tool access, and to specify the logon policy for web-tool access for all users who access Cisco 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, logon, and lockout policies in Cisco Unity Connection Administration, you can change a Connection user password on the user account page. See the "Passwords" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*. Alternatively, users can change their own passwords in the Cisco Unity Assistant.

Cisco Unity Connection Only

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

See the following sections:

Specifying Password, Logon, and Lockout Policies by Using Authentication Rules (Cisco Unity Connection Only)

In Cisco Unity Connection, authentication rules govern user passwords and account lockouts for all user accounts. You use authentication rules to secure how users access 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 logon 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
- The number of days before a password expires

Creating and Modifying Authentication Rules, and Assigning Rules to Users (Cisco Unity Connection Only)

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

Recommended Voice Mail Authentication Rule	By default, Connection applies this rule to the Voice Mail password on the Password Settings page of each user account and user template for which you set up user access to Connection by phone.
Recommended Web Application Authentication Rule	By default, 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 Connection. For information on specifying an authentication rule for a user account or template, see the "Passwords" section in the "Setting Up Features and Functionality That Are Controlled by User Account Settings" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.