Set User Defaults

When you create a user, the defaults that you set in the Configure User window take effect. Use these procedures to specify the default global password and PIN policy settings for all users. This default set of parameters is applied when a new user is created.

Configure Password and PIN Options

If you chose to generate passwords and PINs for users automatically, they are configured in the following steps.

Procedure

Step 1 Choose **Configure** > **User Defaults**.

The system displays the Configure User Defaults page.

Step 2 Choose the default language from the drop-down list.

Step 3 Configure password and PIN options by performing the following tasks in the Password and Pin columns.

a) Although there is space to set a PIN, the Cisco Unified SIP Proxy system does not use PINs. If you set values here, they will not be used. (Optional) Select whether the auto-generation policy will be **random** or**blank**.

b) (Optional) Check **Enable expiry (days)** to set an expiration date for the password. The range is 3 to 365.

c) Set the history depth. The range is 1 to 10.

d) Select the minimum length of the password and PIN. The range for the PIN is 3 to 16. The minimum length of the password ranges from 8 through 64 characters. There is no limit on the maximum length of the password. A valid password should have at least one uppercase letter, one lowercase letter, one number, and a symbol.

Note The change in the minimum password length range is applicable when a new user is created or the password of an existing user is updated. It does not apply to passwords that are already in use.

Step 4 Click **Apply**.

Configure Account Lockout Policy

The account lockout policy determines how the system acts when a user tries to log in and fails.

Step 1 Choose **Configure**> **User Defaults**.

The system displays the Configure User Defaults page.

Step 2 Choose one of the following lockout policy types for the Password and PIN fields:

- Although there is space to set a PIN, the Cisco Unified SIP Proxy system does not use PINs. If you set values here, they will not be used. Disable lockout—The user can continue to try to login with no consequences for failing.
- Permanent—The user is permanently locked out after a certain number of failed login attempts. Enter the maximum number of failed attempts. The range is 1 to 200.
- Temporary—The user is temporarily locked out of the system. Enter values for the following:
  - Number of allowable attempts. The range is 1 to 200.
  - Temporary lockout duration. Pick any number in minutes.
  - Maximum number of failed attempts. The range is 1 to 200.

Step 3 Click **Apply** to save your settings.