Setting User Defaults

When you create a user, the defaults that you set on the Configure User page take effect. Use these procedures to specify the password policy for users. This default set of parameters is applied when a new user is created.

Note Even after you have set defaults in this window, you can change the password policy for an individual user. See Adding a New User in the Configuring Users module.

- Configuring Password Options
- Configuring the Account Lockout Policy for Passwords

Configuring Password Options

Procedure

Step 1 Log in to the Cisco UMG GUI. See the Logging In to the Cisco UMG Graphical User Interface (GUI) module.

Step 2 Choose **Configure > User Defaults**.

The system displays the Configure User Defaults page.

Step 3 Configure password options by performing the following tasks in the Password column:

Note Although there is space to set a PIN, the Cisco Unified SRSV system does not use PINs. If you set values here, they will not be used.

a. Select whether the auto-generation policy will be random or blank.

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

c. Set the history depth, in days. The range is 1 to 10.

d. Set the minimum length of the password. The range for the password is 3 to 32.

Step 4 Click **Apply**.

Configuring the Account Lockout Policy for Passwords

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

Procedure

Step 1 Log in to the Cisco UMG GUI. See the Logging In to the Cisco UMG Graphical User Interface (GUI) module.

Step 2 Choose **Configure > User Defaults**.

The system displays the Configure User Defaults page.

Step 3 Choose one of the following account lockout policy for the password:

Note Although there is space to set a PIN, the Cisco Unified SRSV 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 attempts for temporary lock. The range is 1 to 200.
  - Temporary lockout duration, in minutes.
  - Maximum number of failed attempts. The range is 1 to 200.

Step 4 Click **Apply**.