Password Policy Rules

AWARDS QUICK REFERENCE GUIDE

The Password Policy Rules feature in the AWARDS System Setup, Business Rules feature enables management to set agency-wide password rules for logins within their database. These rules include password expiration settings, requirements for password changes after having a password reset, password composition requirements, and lockout rules.

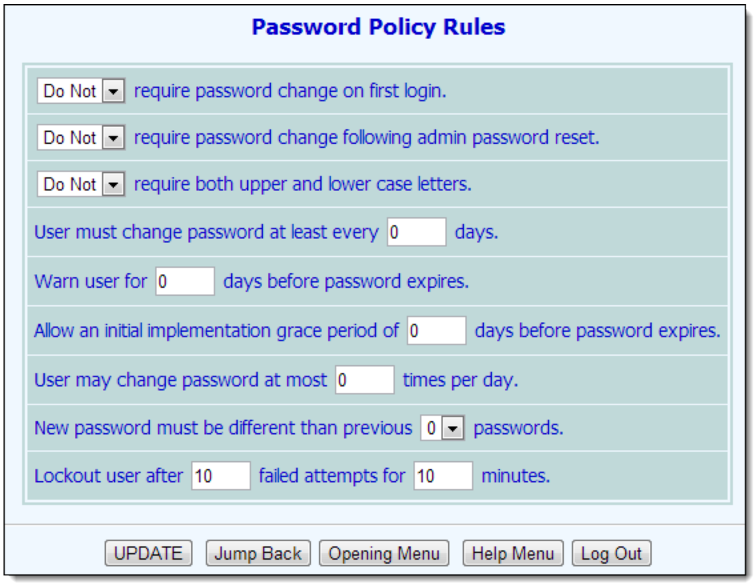
In order to access this feature, you must have access to the System Setup > Business Rules feature.

To enter or update agency password rules, complete the following steps:

1. From the *AWARDS Opening Menu* page, click **System Setup**. The *System Setup Menu* page is displayed.

2. Click **Business Rules**. The *Business Rules Menu* page is displayed.

3. Within the "Global Settings for All Programs" section, click **Password Policy Rules**. The *Password Policy Rules* page is displayed.



Password Policy Rules

Do Not ▾ require password change on first login.

Do Not ▾ require password change following admin password reset.

Do Not ▾ require both upper and lower case letters.

User must change password at least every 0 days.

Warn user for 0 days before password expires.

Allow an initial implementation grace period of 0 days before password expires.

User may change password at most 0 times per day.

New password must be different than previous 0 ▾ passwords.

Lockout user after 10 failed attempts for 10 minutes.

4. Configure the fields and options on this page as needed.

   - **Require password change on first login** – Click this drop-down and select "Do Not" or "Do" to indicate whether a user should be prompted to update his or her password after they successfully log in for the first time (the first time the password is ever used). The default selection is "Do Not."

     This does not apply to existing users that log in for the first time after password policy rules are set. See the grace period rule for an option for those users.

   - **Require password change following admin password reset** – Click this drop-down and select "Do Not" or "Do" to indicate whether a user should be prompted to update his or her password after it has been reset by a system admin or supervisor. The default selection is "Do Not."

   - **Require both upper and lower case letters** – Click this drop-down and select "Do Not" or "Do" to indicate whether passwords in the database should be required to contain both upper and lower case letters. The default selection is "Do Not."

     When this option is set to "Do," existing passwords are grandfathered in and users will not be prompted to update passwords to meet this requirement until they expire or are reset via other methods.

By default, AWARDS passwords must be between eight and twelve characters long and contain both letters and numbers. They are case sensitive and may contain special characters. However, they may not contain the user's Login ID or the agency name (in a multi-agency database).

*Special characters include: ! @ # $ % ^ & * ( ) _ + = | < > ? : ;*

- **User must change password at least every __ days** – In this field, enter the number of days after which a user's password should expire. Users will be prompted to change their password upon logging in once the set timeframe is reached, before accessing other AWARDS screens. The default value is 0, which means passwords will never expire. Since the default value of the grace period is 0, when setting this rule, all users will be forced to change password at next login unless that grace period is expanded.

- **Warn user for __ days before password expires** – If a value is set in the option above, in this field enter the number of days before a user's password expires. They will receive a warning letting them know their password is about to expire. The warning appears after a user logs in and states, "Your password will expire in _ days. Change your password soon." The default value is 0, which means no warning messages will be displayed prior to the expiration date.

- **Allow an initial implementation grace period of __ days before password expires** – In this field, enter the number of days that should act as an initial grace period before a user will be forced to change their password, if it is set to expire. **This applies only when these password rules are initially set and only if passwords are set to expire.** This grace period allows current users to see a warning each day of the grace period before their password expires. The default value is 0, which means no grace period will be provided and every current user will be forced to change their password as soon as they login after the policy rules are saved.

- **User may change password at most __ times per day** – In this field, enter the maximum number of times per day a user should be allowed to update his or her password. The default value is 0, which means there is no maximum number of updates.

  If you are also requiring a password change following an admin reset, setting this value too low could cause user to reach the limit while logging in for the first time following the reset. Limiting this field to one change a day is not recommended. In addition, higher values are also not recommended for security purposes.

- **New password must be different than previous __ passwords** – If a user's new password should not be the same as a previously used password, click this drop-down and select 0, 1, 2, 3, or 4 to indicate how many of the previous passwords should be unique. The default value is 0, which means passwords can be reused at anytime.

- **Lockout user after __ failed attempts for __ minutes** - By default, AWARDS locks out a user after 10 failed attempts for 10 minutes. Use these fields to adjust either the number of failed attempts before a user is locked out and/or the number of minutes they are locked out.

5. Click **UPDATE**. The *Password Policy Rules* confirmation page is displayed.

The process of entering password rules is now complete.