Registry Plus™ Security Features

Centers for Disease Control and Prevention

National Center for Chronic Disease Prevention and Health Promotion

Division of Cancer Prevention and Control

National Program of Cancer Registries

January 26, 2009

Registry Plus™ Security Features

Centers for Disease Control and Prevention • National Program of Cancer Registries

Security Feature	Abstract Plus 3	Web Plus	Prep Plus	CRS Plus
1. Strong passwords	Yes	Yes	Yes	Yes
2. Password history	Yes	Yes	Yes	Yes
3. Setup challenge questions	Yes	Yes	Yes	Yes
4. Challenge questions to login	No	Yes	No	No
5. Challenge questions to reset forgotten password	Yes	No	Yes	Yes
6. Administrator reset user's password	Yes	Yes	Yes	Yes
7. PIN at login	No	Yes	No	No
8. Allow Administrator to define password requirements	Yes	Yes	Yes	Yes
9. Number of failed logins lockout	No	Yes	No	No
10. Password expiration	Yes	Yes	Yes	Yes
11. Database password-protected	Yes	Yes	Yes	Yes
12. Database encryption	Yes	Registry is responsible	Registry is responsible	Registry is responsible
13. User passwords and challenge answers are stored in the database in hash format	Yes	Yes	Yes	Yes

Security Feature Definitions

1. **Strong passwords:** Good, strong passwords can help protect an organization's security. The password must contain a minimum number of characters and certain types of characters.

2. **Password history:** For example, the previous 10 passwords cannot be reused.

3. **Setup challenge questions:** Users select one or more challenge questions from a list.

4. **Challenge questions to login:** When this option is set, the user is required to answer security questions in addition to his or her user ID and password.

5. **Challenge questions to reset forgotten password:** When this option is set, staff members who have forgotten their passwords can reset them without contacting the system administrator. Questions provide for answers that are unique to the individual user.

6. **Administrator reset user's password:** The administrator can reset any user's password at any time.

7. **PIN at login:** When this option is set, the user is required to enter a personal identification number in addition to his or her user ID and password.

8. **Allow administrator to define password requirements:** Many password parameters are available, such as a minimum length, expiration date, and required complexity. The administrator can define the complexity of passwords by using regular expressions.

9. **Number of failed logins lockout:** When this option is set, users are locked out of the software for a defined number of minutes after a defined number of failed login attempts.

10. **Password expiration:** The administrator can optionally require users to change their passwords every defined number of days.

11. **Database password-protected:** Password-protecting the database allows the administrator to protect sensitive data.

12. **Database encryption:** Encryption converts plain text into ciphertext, giving the encrypted data the appearance of random characters. Encryption provides protection from on-site and off-site information loss.

13. **User passwords and challenge answers are stored in the database in hash format:** Registry Plus applications store passwords and challenge answers in the database using a one-way hashing function. Data stored in this way cannot be “unhashed” to get the original data; this is the most secure way to store passwords.

Authentication in Registry Plus™ Applications

All Registry Plus™ applications require, at a minimum, a user ID and password to log into the application. Registry Plus installation packages come with one or more predefined user accounts and passwords. It is strongly recommended that these accounts be deleted and new ones created before using these applications in production. All user passwords are stored in the database in the encrypted/hashed form.

Registry Plus applications provide several configurable options to suit your organization’s security needs. The following configuration options are available:

- **Enforce use of strong password:** Registry Plus applications have the option to enforce the use of strong passwords. When this option is selected, the administrator can configure the rule for strong password by using regular expressions. All applications come with the default regular expression that requires the password to be between 8 and 20 characters long, contain at least one digit and one alphabetic character, and not contain any special characters.

- **Enable password expiration and password history:** The administrator can optionally require users to change their passwords every <<*x*>> days and prohibit users from using their last <<*n*>> passwords.

- **Require users to answer security questions at login:** This option is available for Web Plus only. When this option is set, the user is required to answer security questions in addition to providing his or her user ID and password. For details about this option, please refer to the *Web Plus Administration* manual.

- **Require users to enter PIN at login:** This option is available for Web Plus only. When this option is set, the user is required to enter a personal identification number in addition to his or her user ID and password. For details about this option, please refer to the *Web Plus Administration* manual.

- **Allow a user to log in by answering security questions if the user forgets his or her password:** If a user forgets his or her password, an option can be set in the application to allow the user to log in by answering security questions. The user can then reset his or her password.

- **Resetting user passwords:** The administrator can reset any user’s password at any time. Users can also change their own passwords at any time.

- **Require security questions:** Web Plus may be set up to require security questions to be answered and a PIN to be entered at the time of login.