PEARSON

Chancery SMS® 7.4.1 and higher
Setting Up Strong Log On Passwords
Technical Bulletin

Overview

Chancery SMS provides the option to set up and manage strong passwords for the users in your district.

When server settings and email addresses have been set up, you can have Chancery SMS automatically generate a password and send it to a user (e.g., a new user or an existing user who has been locked out) through email. When the user logs on to Chancery SMS for the first time, he or she is prompted to change this password.

As a password gets close to expiry, Chancery SMS presents a message informing the user of the number of days left before their password expires, and requesting a new password. The message is displayed each time the user logs on until the password is changed. When the number of days left until expiry is zero, Chancery SMS presents the user with the password change page.

NOTE
If your district uses Active directory, you cannot use the password functionality in Chancery SMS.

Password Complexity

A Chancery SMS password must consist of six or more characters in the following combination:

- Alphabetic characters, in upper and lower case combination (characters cannot be all upper or all lower case).
- At least one non-repeating consecutive numeric or special character. For example, 67PeA#R$.

To achieve this complexity, you must configure the following password settings:

- Minimum password length is at least 6 characters and no more than 52.
- Maximum number of repeating characters is at least 3 and no more than 10.
- Minimum number of special characters is at least 1 and no more than 10.
- Number of password changes before a password can be reused is at least 5 and no more than 100.
- A password expiration can be no less than 7 days and no more than 180 days. When a password expires, the user is forced to change their password.

Chancery SMS rejects a password when one of the following occurs:

- The password is the same as the User ID.
- The password matches a previously used password (one that is not yet eligible for reuse).
- The password does not meet the complexity level.

System Lockout

When you set up strong passwords, you must specify the number of unsuccessful logon attempts after which the user will be unable to log on. When a user reaches the specified number of consecutive unsuccessful logon attempts, he or she is locked out of Chancery SMS. After the final failed logon attempt, a message appears indicating the account is now locked and the district administrator must be notified.

When unlocking a user account, the district administrator provides the user with a new default password. When a user whose account was unlocked by the district administrator logs on to the application for the first time, Chancery SMS requires the user to change the password provided by the district administrator.

Setting Up Password Complexity and System Lockout

1. Log on as district administrator.
2. In the control bar, under **Admin**, click **District Setup**.
3. On the **District Setup** page, under **Users**, click **Password Settings**.
4. On the **Password Settings** page, in the **Strong Password Settings** panel, select **Enable Strong Password** and enter the following information:

Field	Description
Minimum Password Length	Enter the number of characters the password must contain. Password length must be between 6 and 52.
Maximum Number of Repeating Characters	Enter the maximum number of repeating characters the password can contain. Maximum number of repeating characters must be between 3 and 10.
Minimum Number of Special Characters	Enter the minimum number of special characters the password can contain. Minimum number of special characters must be between 1 and 10.
Password Reuse Count	Enter the number of times before a password can be reused. The reuse count must be between 5 and 100.

5. On the **Password Settings** page, in the **System Lock-out Settings** panel, select **Enable System Lock-out** and enter the following information:

Field	Description
Password Expires After	Enter the number of days after which a password expires. When the password expires, the user account is locked. The number of days before expiration must be between 7 and 180.
Logon Attempts Before Lockout	Enter the number of logon attempts before a user account is locked. The number of logon attempts must be between 3 and 100.

6 In the **Password Email Settings** panel, enter the following information:

Field	Description
SMTP Server Address	Enter the address of the server that manages email.
SMTP Server Port	Enter the port number of the server that manages email.
Sender	Enter the email address of the district administrator who configures email settings.
Subject	Enter the subject line for the email message that will be sent to the user. The default subject line is **Important! Your User ID and Password**.
Body	Enter the content of the email message that will be sent to the user. The default content is: **Welcome to Chancery SMS <FIRST_NAME>! A user account has been set up for you. Please click http://localhost/chancerysms to log on.** **Your logon information is:** **- User ID: <USER_ID>** **- Password: <PASSWORD>** **Both user ID and password are case sensitive.** **You are required to change your password when you log on for the first time.** **Regards,** **Chancery SMS System Administrator**

7 Click **OK**.

Generating a Password

1 Log on as district administrator.

2 In the control bar, under **Admin**, click **District Setup**.

3 On the **District Setup** page, under **Users**, click **Accounts**.

4 On the **Accounts** page, search for and select the user.

5 From the **Actions** menu, click **Edit User**.

6 On the **Edit User** page, in the **General** panel, verify the following user information:

- **Last name**
- **First name**
- **User ID**
- **Email**

7 Click **Generate Password**.

8 Click **OK**.

A password is automatically generated and sent in an email to the user.

Activating a User Account

While you set up a new user, or when a user is locked out of the system, the user's account is deactivated on the **Accounts** page. Use the activate functionality to activate or re-activate an account and send the user a new password.

To activate an account:

1 Log on as district administrator.

2 In the control bar, under **Admin**, click **District Setup**.

3 On the **District Setup** page, under **Users**, click **Accounts**.

4 On the **Accounts** page, search for and select the user.

5 From the **Actions** menu, click **Edit User**.

6 On the **Edit User** page, in the **General** panel, verify the following user information:

- **Last name**
- **First name**
- **User ID**
- **Email**

7 Click **Activate**.

8 Click **OK**.

A password is automatically generated and sent in an email to the user.