Set Password Preferences

Setting Password Expiration

Administrators with appropriate rights can set password expiration for user accounts. If you set up this option, Access ACS users must periodically create new passwords.

1. Point to **Admin**, click **Security**, and select **Users**.
2. On the Users page, click the user account for which you want to set password expiration.
3. Under **User Options**, click **Edit**.
4. Select **Require password change**.
5. In the **Set Number of Days** field, enter the number of days before the password expires. For example, if you want the password to expire every 30 days, type **30** in the field.
6. Click **Save**.

Setting Password Strength Requirements

You can change the password strength requirements for the organization. By default, password strength is set to level 3 (Average).

Password strength ranges from level 0 (minimal requirements) to level 4 (multiple requirements).

1. Point to **Admin**, then click **Security**.
2. Click the **Security Preferences** tab.
3. Under **Password Strength Requirements**, select the strength level from the drop-down list.
4. Click **Save**.

Password Strength Requirement Levels

Level 0 — The lowest level of password security. The password must be between 5 and 15 characters long, and can match part of the user name or e-mail address.

Level 1 — At this level, the password must be between 5 and 15 characters long. It can contain a sequence of consecutive (123456) or repeated (111111) characters.

Level 2 — At this level, the password must be between 6 and 15 characters long. It cannot contain a sequence of consecutive (123456) or repeated (111111) characters.

Level 3 — At this level, the password must be between 6 and 15 characters long. It cannot contain a sequence of consecutive (123456) or repeated (111111) characters. It must include one of the following conditions: at least 2 letters and 2 numbers, a symbol, or a total of at least 8 characters. This is the default password strength level activated during initial setup.

Level 4 — At this level, the password must be between 6 and 15 characters long. It cannot contain a sequence of consecutive (123456) or repeated (111111) characters. It must include two of the following conditions: at least 2 letters and 2 numbers, a symbol, or a total of at least 8 characters.

Setting up Password Reuse Requirements

You can also limit the number of previous passwords that can be reused for log in. By default, the limit is set to 6. Password reuse can be set to **0**, **no limit**, **up to 10**, **track 10 previous passwords**.

1. Point to **Admin**, then click **Security**.
2. Click the **Security Preferences** tab.
3. Under **Saved Passwords**, select the number of previous passwords you want to limit in the drop-down list.
4. Click **Save**.

Related Topics

Set up and Work with User Security
Upload ACS People Records