Users and Application Management - Application Management

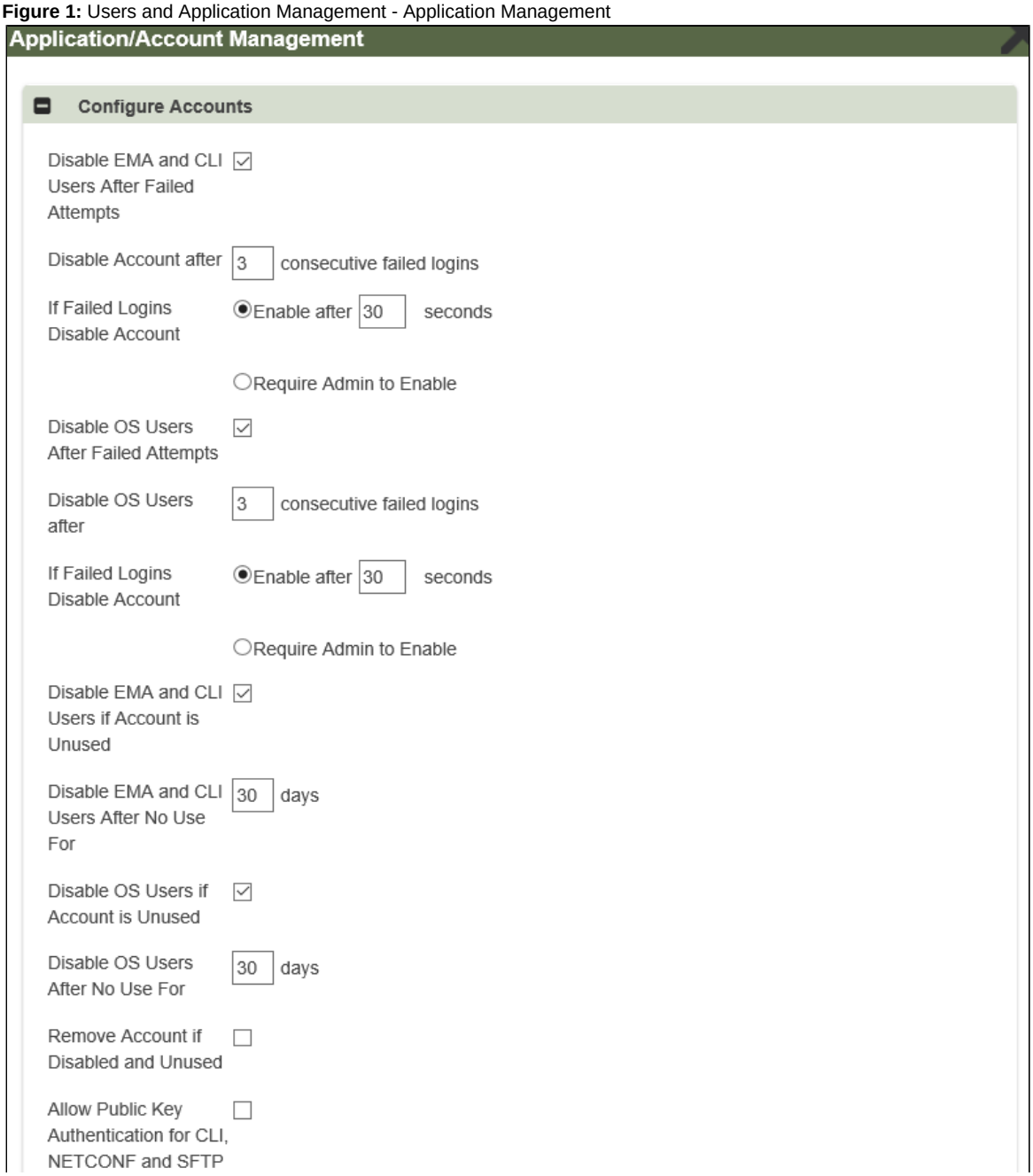
In this section:

Application Management is a new tool that provides the capability to manage many security-related system settings.

On SBC main screen, navigate to **Administration** > **Users and Application Management** > **Application Management**.

The **Application Management** window displays.

Figure 1: Users and Application Management - Application Management



Access

Undo Edits | Save

Configure OS Account Re-Enable

Enter the name of the user whose Account has to be Re-Enabled. [ ]

Undo Edits | Re-Enable

Configure Sessions

Limit Sessions To [5] per user

Force Session Timeout [ ]

Undo Edits | Save

Configure Login Banner

Show Login Banner [ ]

Undo Edits | Save

Configure Password Rules

Use Separate Password Rules for Administrators [ ]

Enable Password Expiration for EMA and CLI Users [x]

Expire Password after [90] days

Warn User of Expiring Password [12] days before expiring

Enable Password Expiration for OS Users [ ]

Minimum Number of Days Before Password can be Changed [ ] days

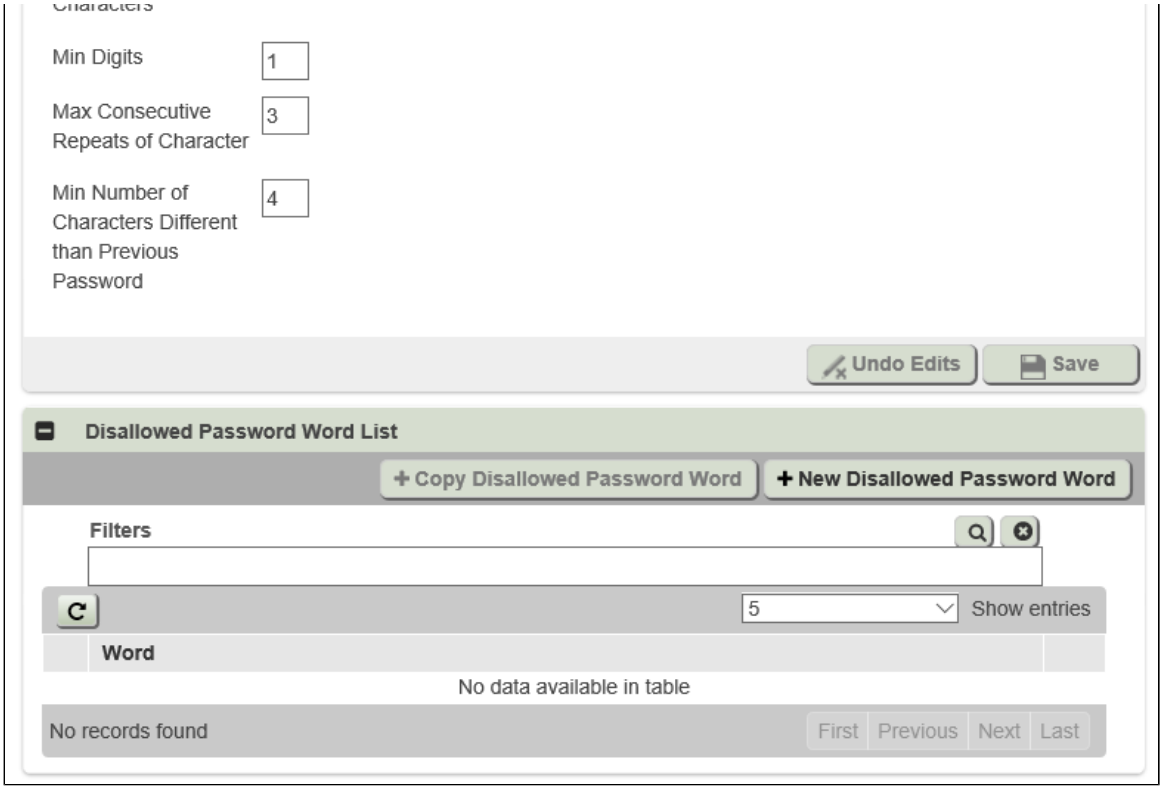
Prevent Reuse of Last [4] passwords

Min Length [8] characters

Min Uppercase Characters [1]

Min Lowercase Characters [1]

Min Special Characters [1]



Configure Accounts

This section provides you an option to disable accounts. Enter the following fields and click **Save**:

- **Disable CI and EMA Users After Failed Attempts** - If checked, the following options display:
  - **Disable Account after consecutive failed logins** - Number of failed attempts after which the SBC Users account gets locked temporarily.
  - **If Failed Logins Disable Account** - If the account is disabled, the following options are presented to ensure the account gets unlocked:
    - **Enable after seconds** - The number of seconds after which the SBC Users account is automatically enabled and is available for login.
    - **Require Admin to enable** - The administrator must manually enable the SBC Users disabled account.

- **Disable OS Users After Failed Attempts** - If checked, the following options display:
  - **Disable Account after consecutive failed logins** - Number of failed attempts after which the Linux OS Users account gets locked temporarily.
  - **If Failed Logins Disable Account** - If the Linux OS Users account is disabled, the following options are presented to ensure the account gets unlocked:
    - **Enable after seconds** - The number of seconds after which the Linux OS Users account is automatically enabled and is available for login.
    - **Require Admin to enable** - The administrator must manually enable the disabled Linux OS Users account.
- **Disable CLI and EMA Users Account if Unused** - If checked, the following option displays:
  - **Disable CLI and EMA Users After No Use For** - Number of days for which the SBC waits since the last use of an SBC user's account, before disabling the account.

- **Disable OS Users if Account is Unused** - If checked, the following option displays:
  - **Disable OS Users After No Use For** - Number of days for which the SBC waits since the last use of an OS user's account, before disabling the account.

- **Remove Account if Disabled and Unused** - If checked, the following option displays:
  - **Remove After No use for** - Number of days for which the SBC waits after an account is unused and disabled, before removing the account.
- **Allow Public Key Authentication for CLI, NETCONF and SFTP Access -** If the user checks this box and the SSH keys are populated,

the SSH users can log into their servers without the need to enter their passwords. For more details, see the Allow SSH Public Key Authentication section.

Configure Sessions

You can configure the options for sessions in this section. You can set the number of sessions allowed for each user along with the time for each session to be alive.

Enter the following fields and click **Save**:

- **Limit Sessions to**: You can limit the number of sessions assigned to each user. The maximum sessions for a user is 5.
- **Force Session Timeout**: The application closes once the session time expires.

  > **Tip**
  > Sonus recommends that Force Session Time option is always checked. This allows the software to automatically clean up the abandoned browser sessions after the specified timeout period. An abandoned browser session occurs when the user closes the browser without logging out of the application. If Force Session Timeout is unchecked, these abandoned sessions are not cleaned up and cause the user to reach their maximum number of allowed sessions.

- **End Session after**: Specify the time in minutes after which the session times out.

Configure Login Banner

This section provides an option to configure your own banner which would displays on the Login screen of the EMA for all your users. Follow the steps below and click **Save**:

1. Enable **Show Login Banner** option to display all fields.
2. Enable **Require User to Acknowledge Banner before Logging in** option to receive acknowledgement from the users every time they try to login.
3. Enter your text that should be displayed as Banner in the text box next to Banner Text option.

Once the changes are saved, the Banner text will displays on the login screen.

Configure Password

This section provides an option to configure passwords for users. It also specifies the criteria to establish a good password to access the EMA. Enter the following fields and click **Save**:

- **Use Separate Password Rules for Administrators** - If checked, separate password rules can be configured for Administrators and other types of users. The password rules are configured based on the following parameters:

  Table 1: Password Rule Parameters

Parameter	Range	Default/Required	Description
`Prevent Reuse of Last`	NA	4 passwords	This field prevents the user from re-using the last few passwords.
`Min Length`	8-24 characters	8 characters (required)	Specifies the minimum number of characters in a password.
`Min Uppercase Characters`	NA	1 character (required)	Specifies the minimum number of uppercase characters that can be used to create the password.

Min Special Characters	NA	1 character (required)	Specifies the minimum number of special characters that are allowed in a password.
Min Digits	NA	1 digit (required)	Specifies the minimum number of digits that are allowed in a password.
Max Consecutive Repeats of Character	NA	3 repeats (max)	Specifies the number of times a character can be reused in a password.
Min Number of Characters Different than Previous Password	NA	4 character (min)	Specifies the number of characters that should be different from the last password created.

- **Enable Password Expiration for CLI and EMA Users**: If checked, every password will have an expiration date. Also, the following options display:

Table 2: Password Expiration

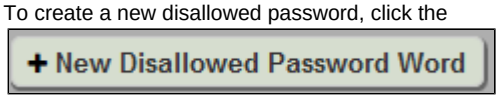
Parameter Name	Range	Default / Required
Expire Password after	30-180 days	90 days
Warn User of Expiring Password	3-14 days	12 days

- **Enable Password Expiration for OS Users** - If checked, passwords of Linux OS users also gets expired after a set number of days.
- **Minimum Number of Days Before Password can be Changed** -The value for this field denotes the minimum number of days (1 - 365 days) before the password can be changed. Counting starts from the day of changing the password for the last time. The default value is 1 day.

Disallowed Password Word List

To Create New Disallowed Password Word

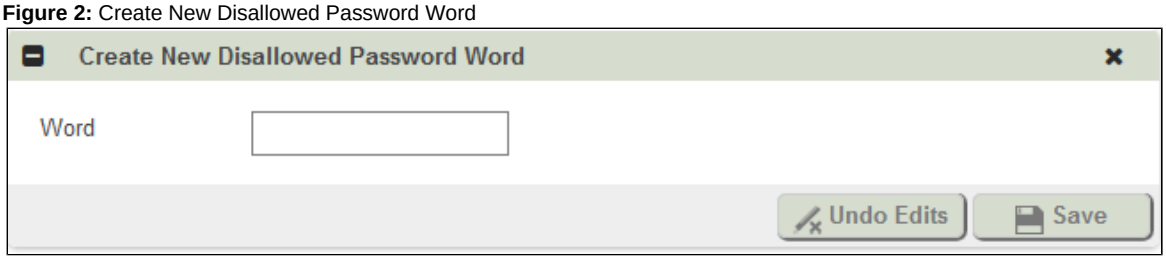
To create a new disallowed password, click the



button.

The **Create New Disallowed Password Word** frame displays.

Figure 2: Create New Disallowed Password Word



The description of the parameter is given below:

Table 3: Create New Disallowed Password Word - Parameter Description

Parameter	Description

`Word`	A word (1-23 characters) which is not allowed as password.

Provide the word that is disallowed as password, and click **Save**. Click **Undo Edits** to cancel all changes.

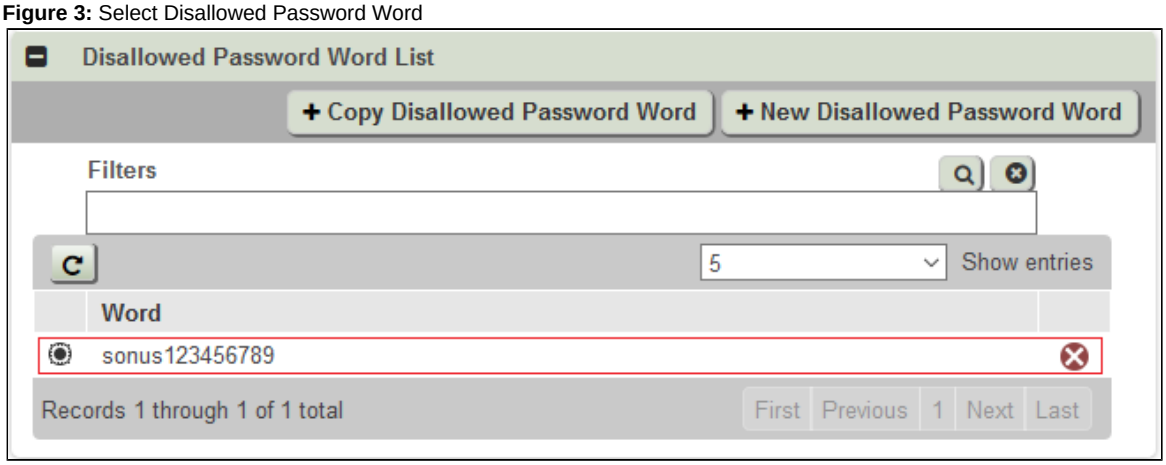
Note

- The number of words allowed in the dictionary is 0 (empty) to 5000.
- A word is defined as a string of up to 255 ASCII characters.

To Edit Disallowed Password Word

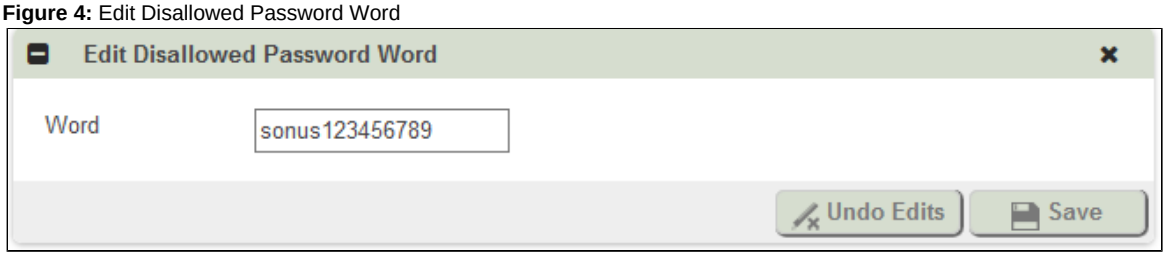
To edit a disallowed password, select the password from the **Disallowed Password Word List** frame.

Figure 3: Select Disallowed Password Word



The **Edit Disallowed Password Word** frame appears.

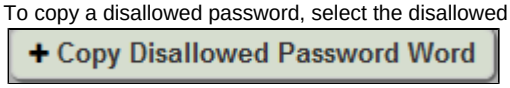
Figure 4: Edit Disallowed Password Word



Make necessary changes in the disallowed word, and click **Save**. Click **Undo Edits** to cancel all changes.

To Copy Disallowed Password Word

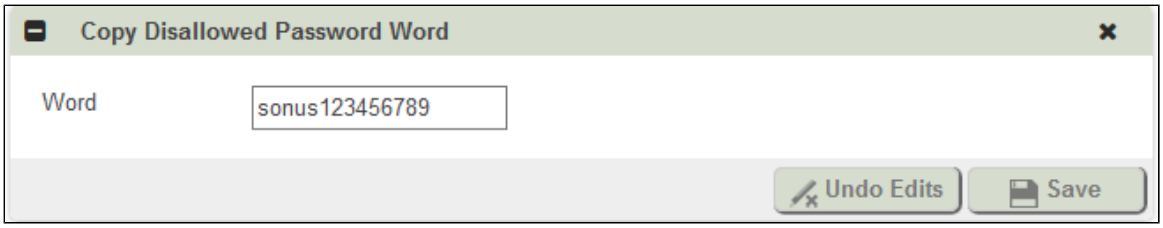
To copy a disallowed password, select the disallowed password from the **Disallowed Password Word List** frame, and click the



button.

The **Copy Disallowed Password Word** frame appears.

Figure 5: Copy Disallowed Password Word



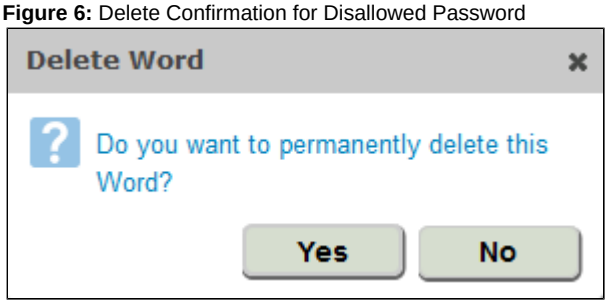
Make necessary changes in the disallowed word, and click **Save**. Click **Undo Edits** to cancel all changes.

To Delete Disallowed Password Word

To delete a disallowed password, select the disallowed password from the **Disallowed Password Word List** frame, and click the **Delete** symbol at the end of the selected row.

A pop-up displays seeking confirmation to proceed with the deletion.

Figure 6: Delete Confirmation for Disallowed Password



Click **Yes** to finish deletion.

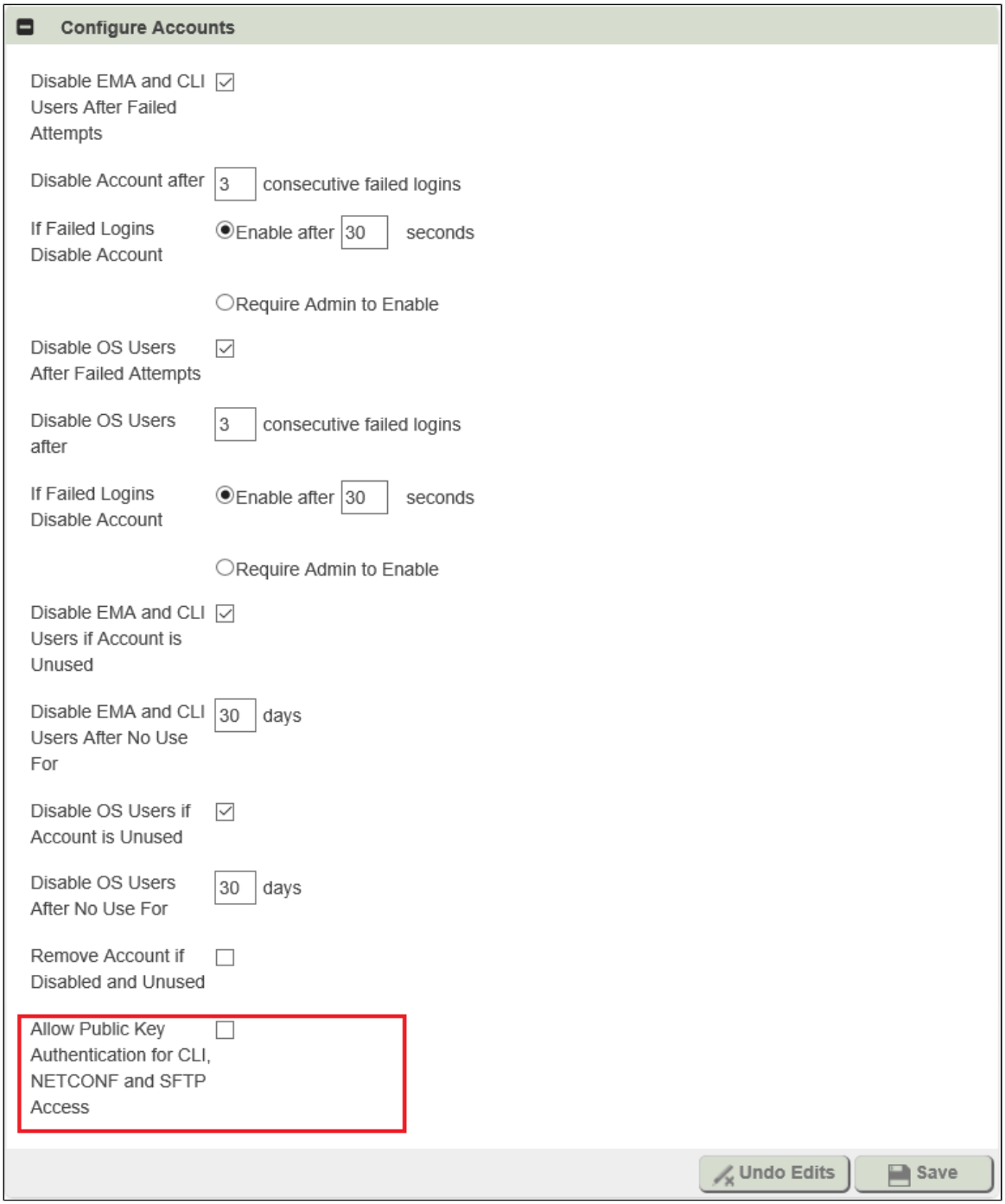
Allow SSH Public Key Authentication

The SBC SSH public key authentication feature allows application management users to provision, delete, and display up to five SSH public keys for the purpose of accessing CLI (port 22), NETCONF(port 2022) as well as SFTP (port 2024).

This feature provides a user interface through which application management users can add, delete, and display authorized client public keys. Up to five keys are supported for each configured user.

A checkbox named **Allow Public Key Authentication for CLI, NETCONF and SFTP Access** is included in the **Application Management** dialog box.

Figure 7: Allow Public Key Authentication



Click the check box to enable SSH Public Key Authentication.

> **Note**
> Disabling public key access has no effect on CAC card access to EMA.