Locking User Accounts

To reduce the chances that an unauthorized user will be able to compromise the account of an authorized RiskVision application user, suggests that you lock user accounts after a predefined number of consecutive login attempts. This is only applicable to internal users (users who authenticate against the RiskVision database), and does not apply to external users (users who authenticate against an LDAP source). RiskVision would then lock any user account that has a greater number of consecutive failed login attempts than the value set in the **password.disableAfterNFailedLogin** property. When an account is locked, the user will not be authenticated even if a user inputs the correct credentials. You will need to follow the steps mentioned below to unlock the user account.

To enable locking of user accounts:

1. Open the `agiliance.properties` file using a text editor
2. Add the `password.disableAfterNFailedLogin =` property.
3. Save the **agiliance.properties** file.
4. To apply the latest changes, do one of the following:
   - Reload the server configuration.
     1. Go to **Administration** > **Server Administration**
     2. Click the **Commands** tab.
     3. Expand the **Configuration** section and click **Reload**.
   - Restart the RiskVision Tomcat service.