Managing External User Accounts

During Active Directory maintenance, it is likely that your Windows administrator may change attributes of an user account or may simply disable an user account. When an account is disabled in the Active Directory, the RiskVision administrator has the responsibility to secure the RiskVision domain by ensuring that a user is not be able to access the RiskVision application when an inactive user is imported into RiskVision. Anticipating that these changes can cause security breach, the RiskVision administrator can make use of an external user attribute called "Status" to affect the changes made in Active Directory to reflect in RiskVision. By default, each LDAP Server has Status attribute set to “userAccountControl.”

If you have upgraded to RiskVision 6.5, you must manually add the Status attribute by setting the value to "userAccountControl" for the existing LDAP server. This attribute can be added on the External User Attributes tab of Administration > SAML Configuration page. To get updates from the Active Directory, run the LDAP User Synchronization system job manually.

It is necessary to familiarize yourself with the behavior of user accounts that are made active or inactive in the Active Directory before or after the user accounts are imported into RiskVision.

- A deactivated user in Active Directory when imported into RiskVision will be shown as deactivated.
- From Active Directory, importing an active user into RiskVision will be shown as active.
    - Afterwards, if the same user is deactivated in Active Directory and when the LDAP Users Synchronization system job is run, the user account status is changed to as inactive in RiskVision.
    - Afterwards, if the same user is deactivated in RiskVision and when the LDAP Users Synchronization system job is run, the user account status remains inactive in RiskVision.