About System Users

The RiskVision application authenticates users against an internal user directory. You can add additional users and define user roles in the internal directory. Optionally, you can choose to integrate with an LDAP directory service, such as Active Directory.

The RiskVision application uses a role-based Access Control List (ACL) policy with granular permission configuration. It is possible to define new roles with permission to access specific objects and perform specific operations on those objects, such as view, create, update, and delete. In addition, filters can be used in conjunction with roles to restrict specific permissions for a user assigned one or more roles. So, when a user logs in, they are granted the combined permissions of the roles to which they assigned membership and restricted by any access filters that might also be attached to their user account.

The RiskVision solution has the following types of user accounts

- **System administrator** : User accounts in the system space that manage the host computer settings.
- **System users**: Accounts that participate in assessments, manage assessment data, and connectors for their own space. This is the only type of user account that has roles you can customize.
- **Vendor users**: Limited-access accounts for questionnaire-taking and vendor user management only. Vendor accounts allow an organization to involve third-parties in the risk assessment process.