Authenticating Across Trusted Domains

RiskVision solution supports multiple LDAP servers that span over different domains. Typically, an enterprise will have all user accounts stored within one primary Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) top-level domain or forest. User accounts may be dispersed into many organizational units under the domain.

In a large enterprise, especially those with global reach, users interfacing with the RiskVision solution may be located in multiple AD domains with trusted relationships. In this instance, connecting to one AD domain may not be sufficient for importing all necessary users. The authentication connector can be referred to the enterprise's global catalog as a solution to this problem.

To facilitate this scenario, the RiskVision solution administrator must use these settings when configuring a connector:

Setting	Value
Protocol	LDAP
Hostname/IP	IP or hostname of a global catalog server
Port	3268 (standard)
Base DN	Top-level domain shared by all trusted domains
UID Key	sAMAccountName or mail
Default Domain	Any existing domain will suffice

RiskVision will require a valid ID with read access to the external directory to perform user search. The search base does not have to be completed here. When the RiskVision solution administrator begins to import users from AD or LDAP, the search base field can be populated with any additional domain or OU details.

Allow users logging in for the first time using their email address by specifying the UID key field as 'mail' on the LDAP server Configuration tab and also, the 'userid' must be set to as 'mail in the User Attributes page of Attribute Mappings tab of LDAP server. Further, the following property must also be enabled:
`com..authenticate.ldap.user.using.email=true`

RiskVision does not authenticate the users with same email IDs when UID key is set to as 'mail.'