

Configuring LDAP Service

The Authentication connector is used to import users from the LDAP Directory service into RiskVision. The Authentication connector will communicate with the LDAP directory, verify the user's authentication, and allow them to log in to RiskVision.

In addition to using the built-in RiskVision solution authentication mechanism, you can configure a local LDAP directory service for authentication. When using LDAP for authentication, the RiskVision solution prompts the user to type a login user name and password. Once the user is authenticated by LDAP (credentials validated with the underlying AD or LDAP directory service), the RiskVision solution retrieves the corresponding user's attributes and permissions based on mapping roles stored in the RiskVision database.

Providing LDAP authentication for the RiskVision solution requires installation of the following:

- A supported LDAP Directory service such as Active Directory (AD).
- Optionally, if LDAP users will be imported into the RiskVision database, login names defined for LDAP users that you want to grant access to the RiskVision solution.

AD or LDAP users are assigned initial roles with access to the Console based on settings and roles defined on the Administration > Login Integration page in the Administration application.

If you want to allow a user to configure an LDAP service, you should assign the System User Manage permission. This permission is assigned to the default Administrator role in RiskVision.

Secure LDAP service prerequisites:

1. Back up the default trust store file cacerts located in the `%AGILIANCE_HOME%\Java\jre\lib\security` directory.
2. Create an empty file with any name to store the AD certificate in the machine where RiskVision is installed. For example, `C:\SecureLDAP\keystore.cer`.
3. Open the command prompt and navigate to the path where OpenSSL is installed. For example, `C:\Program Files\GnuWin32\bin`.
4. Run the following command to generate the certificate from the AD server where you want the secure LDAP service to be.
 - `openssl s_client -connect :636 -showcerts`

```

C:\WINDOWS\system32\cmd.exe - openssl s_client -connect :636 -showcerts

C:\Program Files\GnuWin32\bin>openssl s_client -connect :636 -showcerts
Loading 'screen' into random state - done
CONNECTED(00000784)
depth=0 /CN=
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 /CN=
verify error:num=27:certificate not trusted
verify return:1
depth=0 /CN=
verify error:num=21:unable to verify the first certificate
verify return:1
-----
Certificate chain
 0 s:/CN=
  i:/DC=com/
-----BEGIN CERTIFICATE-----
MIIFwDCCBKigaAwIBAgIQYQGHgAAAAAAAAAzANBgkqhkiG9w0BAQUFADBAMRMwEYqK
CZImiZPyLQGQBGRYDY29tMRUwEwYKZlInIZPyLQGQBGRYFaWRjYVWQxEjAQBgNUBAMT
CWLkY2FkLmNvbTAEFw0xMzA3MzEwOTExMTAhaFw0xNDM3MzEwOTExMTAhaMBsGTAX
BgNUBAMTEGRldjE2MjY5pZGnhZC5jb20wgGEMa0GCSqGS1b3DQEBBQUAA4IBDwAw
ggEKAoIBAQCAa62AeTuw1WOCcIS98Yjgfbs4bm0tuoIO1GcZ9F8Y1CfmuXPA0nHCA
KEcY8GrLXy50b2JLRNlvkPyEyjBQU6NkptNSkGgrQF0v8dmApPWIuLuEU0dFuz6E
UZ5wxs8t61BTX/PPHPLS+1FeMRr1aseoulf2KNNBOM78AUQ48BhDbDjktP5AuB+NS
rtm/+s1du1g0oisF0nyyalQC54nbjgFGn4h5a+zUiz1lkbFELCR/wz/DQ0wRFQc
5oCTn/aFnhkKuUdgUxMb/Tp4+rE9s iGjne1I5Rz618/wuwNozSXo6D/+zKjJgzK
hgXQML5KJH7IB99UqGYNeNCa.jEws7JtbAgMBAAGjggLfMIIC2zAUBgkrBgEEAYI3
FAIEIh4gAeQAabwBtAGEAaQBwEMAAbwBuAHQAcgBwAGwAbAB1AH1wHQYDUR01BBYw
FAyIKwYBBQUHAI GCCsGAQUFBwMBMA4GA1UdDwEB/wQEAwIFoDB4BgkqhkiG9w0B
CQ8EazBpMA4GCCqGSIb3DQMCAGIAGDAOBggqhkiG9w0DBAICAI AuCwYJYIZIAWUD
BAEqMASGCWCGSAF1AwQBLTALEBglghkgBZQM EAQIwCwYJYIZIAWUDBAEFMAcGBS0
AwIHMAoGCCqGSIb3DQMHMB0GA1UdDgQWBBTIdLhkQTFyzVT9/dioyKT BzMSdUDaf
BgNUHSMEDAWgBQJgeG7tQJNUHz+Q2ffnXgB+cj59TCBxAVDUR0fBI G8MI G5MI G2
oIGzoIGwoGtbGRhcDovLy9DTj1pZGnhZC5jb20sQ049ZGU2MTYzLENOPUNEUCxD
Tj1QdWJsawM1MjBLZkxk1MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1
cmF0aW9uLERDPWlkY2FkLERDPWVubT9jZXJ0aWZpY2F0ZUJldm9jYXRob25MaXN0
P2Jhc2U/b2JqZWNoQ2xhc3M9Y2UyJmRGRzdhJmRGRzdhJmRGRzdhJmRGRzdhJmRGRz
BwEBBI GsMI GpMI GmBgggrBgEFBQcwAoAaBmWxkYXA6L290L290L290L290L290L290
PUFJQSxDtj1QdWJsawM1MjBLZkxk1MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1D
b25maWd1cmF0aW9uLERDPWlkY2FkLERDPWVubT9jQU1cnRpZmljYXR1P2Jhc2U/
b2JqZWNoQ2xhc3M9Y2UyYkdG1naWNoG1ubkF1dGhvcml0eTA8BgNUHREENTAz0B8G
CSsGAQQBqjczZAAASBBDENFqXGQ9FQKZ+njEQI+ncghBkZXVxNjMuaWRjYVWQuY29t
MA0GCSqGSIb3DQEBBQUAA4IBAQCMboMfprUESiftJgLYvhu06R1lwCURrZSG3K
5LCUNBRF0aY09wR90JfrUfv1TnrXpkQblcjtIhDUb4tgXq8vUdftd1DR2Ne++ZN
KgsYmZajojt90/5GFpvXxJLuCTEy+P5BjD040ktpkA15uf03ZURdRsAgfSN9u47
BR5tKQ1IHnwI pDRIPpR1juPIWd/fcKhq94SvL72aYxNX202jzX2F4JXSggJY/ZJZ
9qsKC+mpKnoA/R3EvbumqFCz iSwJYRE1M9LXINwvRd/x9phRLc7ND02NyET4jZv
wJ3Y4m6WAsWnIHOKmqESz0dtDDm5UyEcG2DFOAONbAH28dZX
-----END CERTIFICATE-----

```

An example of a generated certificate.

- Copy and paste the text between -----BEGIN CERTIFICATE-----and -----END CERTIFICATE-----into the file that was created in step 2.
- Verify if the content is corrupted by using the following command:
 - `openssl x509 -in \keystore.cer -text`
- Navigate to the location where keytool is installed (E.g., %AGILIANCE_HOME%\java\bin).
- Import the AS certificate file made in step 5 into the `jre\lib\security\cacerts` certificate file by running the following command in one line.
 - `keytool -import -alias ldap1 -keystore %AGILIANCE_HOME%\Java\jre\lib\security\cacerts -trustcacerts -file \keystore.cer`



The system will require a keystore password in order to import the certificate. The default password for cacerts is **changeit**.

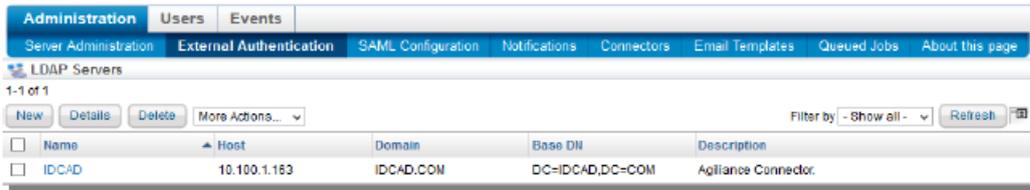
- Restart the Tomcat server and test the secure LDAP connection in RiskVision by configuring the Authentication Connector.

To set up the LDAP service connection:

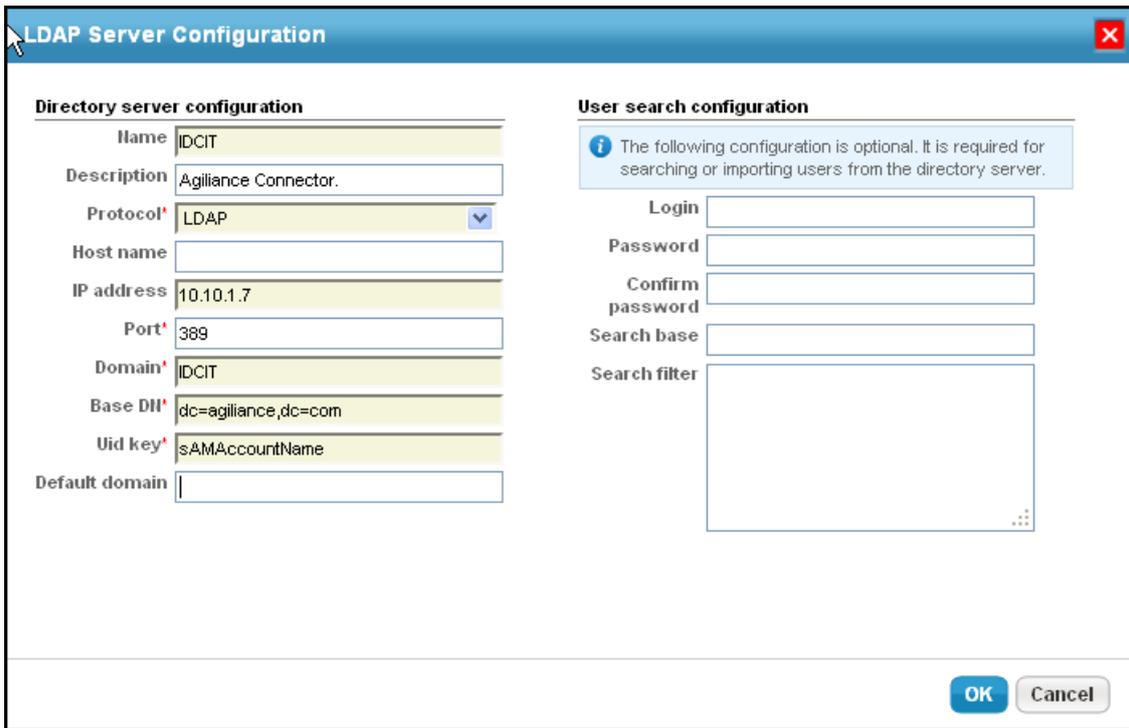
- (Note: In a multi-tenant environment, only the 'sysadmin' user in the system tenant space can access the Authentication Connector.)

In the Administration application, go to **Administration > External Authentication**.

The LDAP Servers page is displayed.



2. A default Authentication Connector is available for you to set up an LDAP service. Modify the default LDAP setup or click **New** to create a new LDAP server. When you click new, the **LDAP Server Configuration** dialog appears.



3. Enter the configuration information.
 - o Name: Specify the LDAP name.
 - o Description: Provide information explaining the purpose to set up an LDAP.
 - o Protocol: Select the connection type.
 - o Host name: Enter the host name or the IP address.
 - o IP address: Enter the IP address.
 - o Port: Enter the connection port, the default is 389 (LDAP) or 636 (Secure LDAP).
 - o Domain: Specify the domain name. Display domain name for users to select while logging in to RiskVision.
 - o Base DN: Enter the base domain such as dc=,dc=com.
 - o Uid key: Enter the name of the field that specifies the unique user identifier, For example, uid for standard LDAPs or sAMAccountName for AD.
 - o Default domain: Enter the domain name to use as default domain when there multiple configured domains
4. Enter the connection and search details.
 - o Login: Optional, enter the account information that the application should use to authenticate users against the LDAP service. The account requires at least read access to the DN and search base.
 - o Password: Optional, enter the account password.
 - o Confirm password: Verifies if you have entered the correct password when you save.
 - o Search base: Used for large directories to prevent time outs, this field is combined with the base DN; for example enter OU=Security.
 - o Search filter: Limit the scope of the search to certain objects, for example to search only user in AD enter ObjectClass=User.

5. Click **OK**.

Next, [test the connection](#).