Connecting to an LDAP server

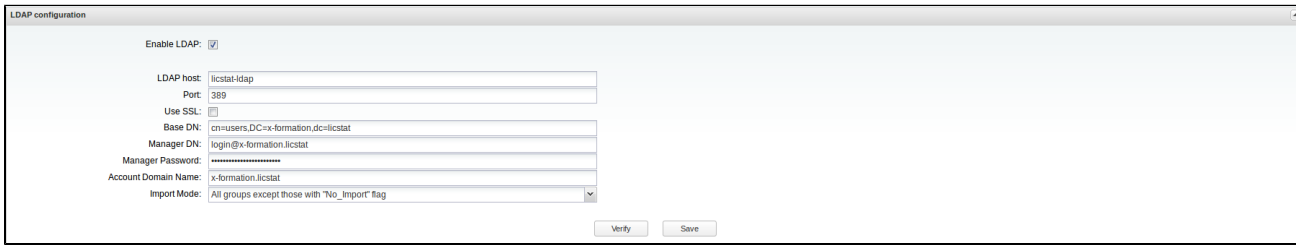
Some information on this page refers to License Statistics v5.1 or newer, which added the ability to connect to an LDAP server over SSL protocol. If you are using an earlier version of License Statistics, see v4.18 to v5.1 documentation or refer to documentation for versions prior to v4.18.

License Statistics lets you connect to an LDAP server to access user accounts (see Automating user account creation using LDAP) and user groups you have defined in an LDAP directory (see Importing LDAP user groups).

Currently, License Statistics has been tested only with Microsoft Active Directory. You may use other LDAP directories, but they are untested with License Statistics at this time. The following instructions for setting up LDAP apply to Active Directory, but may be used as a basis for connecting to other LDAP directories.

To set up connection to LDAP:

1. Select the **LDAP** tab from the Administration page. (This page is visible only for License Statistics administrator users.)
2. Toggle on Enable LDAP to allow the connection to the LDAP server. (You can toggle this box off if you want to suspend the LDAP connection at any time.)
3. Enter the appropriate information for connecting to your LDAP server. An example setup is shown in the screenshot below. Also see the following section, LDAP settings, for more information.
    a. LDAP Host: The hostname of the LDAP server.
    b. Port: The port for the LDAP server. The default is 389.
    c. Use SSL: Check this box if you would like to connect to your LDAP server over SSL protocol.
    d. Base DN: The base DN (Distinguished Name) under which to search for users. (See LDAP settings, below, for more information on obtaining the base DN.)
    e. Manager DN: The DN for the manager account to be used for initial binding (authentication).
    f. Manager Password: The password for the manager account.
    g. Account Domain Name: The sub-domain of the LDAP directory.
    h. Import Mode: The mode you specify to be able to import user groups you have defined in an LDAP directory.
4. Save your settings.
5. Enter a valid username and password in the Test connection area and click **Verify** to ensure that your connection to the LDAP server works as expected. A message will indicate whether the test was successful. If the test is not successful, make the needed changes to the setup, save the changes, and retest the connection.



Enabling LDAP over SSL

By default, LDAP traffic is transmitted unsecured. You can, however, make LDAP traffic confidential by installing a valid certificate issued by a certificate authority (CA). The CA certificate, which contains a public key and the identity of the owner, is needed to enable encrypted communication between License Statistics and your LDAP server.

To connect over SSL:

If you want to verify that the LDAP server's certificate is properly signed:

1. Set the variable LDAP_SSL_CERTIFICATE_KEY_FILE in the License Statistics configuration file (xflicstat.cfg). This variable defines the path and filename of the CA certificate and allows the client to verify the LDAP server's certificate.
2. Leave the default settings of the variable LDAP_SSL_CERTIFICATE_VERIFY. By default, this variable is set to the "demand" value, indicating that the server certificate will be checked to verify that it is properly signed and your CA certificate, which you set in LDAP_SSL_CERTIFICATE_KEY_FILE variable, will be used to verify that.
3. Restart License Statistics.

If you do not want to verify that the LDAP server's certificate is properly signed:

1. Set the variable LDAP_SSL_CERTIFICATE_VERIFY to "allow". This way, the connection will be allowed even if it turns out that the certificate is missing or it is not valid. In this case, setting the variable LDAP_SSL_CERTIFICATE_KEY_FILE is not obligatory.
2. Restart License Statistics.

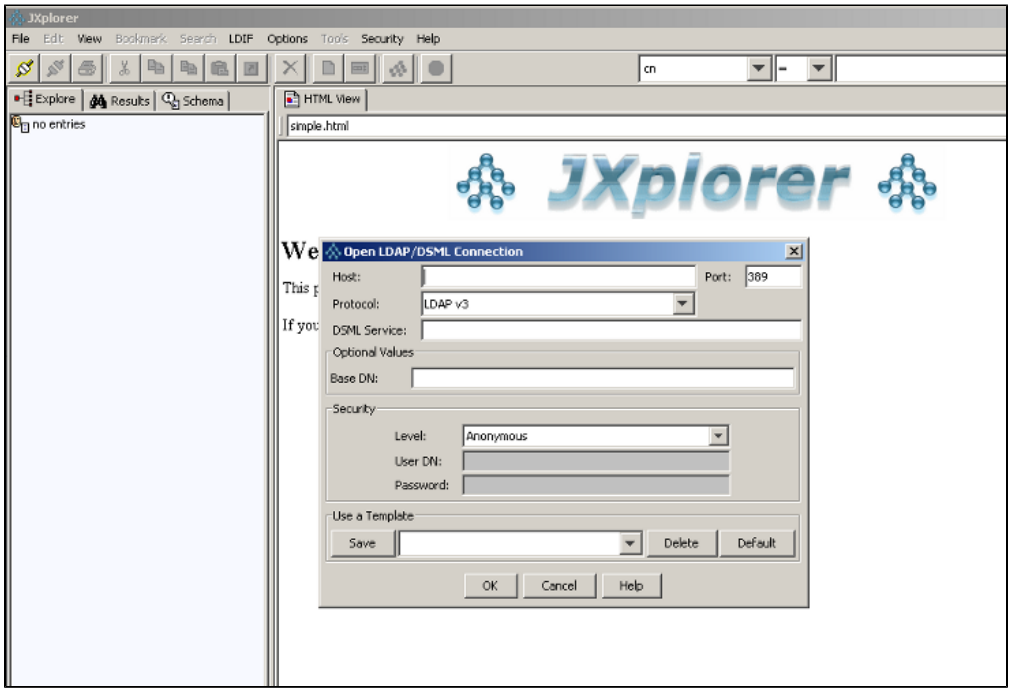
Note: We recommend using the predefined settings and leaving the variable LDAP_SSL_CERTIFICATE_VERIFY set to "demand" so you can perform the validation of the LDAP server's certificate using your CA file.

LDAP settings

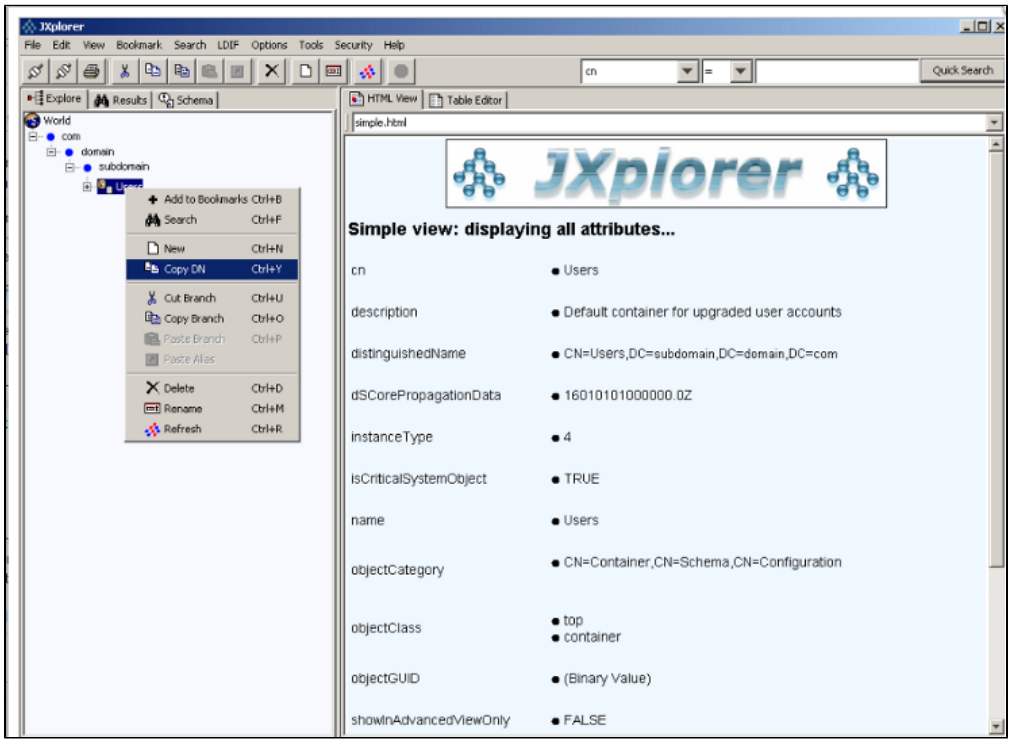
A tool such as JXplorer is an excellent way to test your LDAP settings. Using such a tool can save a lot of time when configuring License Statistics, because you can test that credentials and other settings are correct.

You can use JXplorer to copy the DN from LDAP. To do this:

1. Log into JXplorer as shown below.



2. After logging into JXplorer, use the Copy DN option to copy the base DN. When selecting the base DN, it's important to choose the path in the tree that contains the groups you want to see in License Statistics for reporting usage.



3. After copying the base DN, you can simply paste the string into License Statistic's Base DN field instead of typing it.

To learn more about LDAP, see http://en.wikipedia.org/wiki/LDAP.