LDAP Configuration

Document ID: Q000041
Last Revised On: Thursday, December 27, 2007

This article applies to the following:
Component(s):
Administrator

Solutions(s):
All

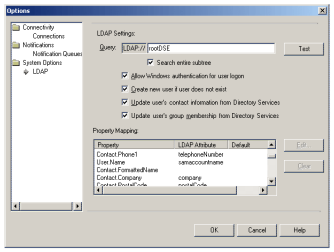
Introduction to LDAP Configuration

IssueNet LDAP integration provides services to automate and maintain users and security privileges in IssueNet based on end users domain settings. By enabling the LDAP integration, IssueNet can create users, authenticate logons, maintain contact information, and update security privileges when the user logs on to the solution.

When configuring the LDAP integration for your environment you will need to specify a query that your LDAP server can use to return user information, property mapping values from your LDAP server property names to IssueNet contact property names, and simple options on how you wish to manage these users.

Enabling LDAP Integration

To configure LDAP integration, logon to the solution with the IssueNet Administrator. Select the **Tools | Options...** menu option and select the **System Options | LDAP** section.



The first value to enter is an LDAP query that can successfully return user information from your LDAP server. You may test this query by clicking the **Test...** button and entering a valid domain user name. When you click the **Query** button on the **LDAP Verification** dialog the results for the specified user will be returned in the output window.

Additionally, you may specify whether to search an entire subtree under a given node that you query for. This option is made available for environments who may want to limit the query to a specific node in their Active Directory. Examples of potential LDAP queries you may use would be;

- **LDAP://rootDSE** - search the default domain
- **LDAP://<domainname>.local** - search a specific domain

If you do not get results back from the LDAP Verification dialog you have either specified an invalid query for your LDAP server or you lack security privileges to interrogate your LDAP server. Check with your network administrator if you have questions about your security privileges or how to address your LDAP server.

LDAP Options

The LDAP integration options are designed to give you control over discreet areas of user management. You may choose any option that suites your needs but should understand what each option does for you to avoid confusion at runtime.

- **Allow Windows authentication for user logon:** Users are logged on to IssueNet with their domain UserID
- **Create new user if user does not exist:** IssueNet will create a new user automatically when logging on to IssueNet Client. The IssueNet user name will match the Windows domain user name.
- **Update user contact information from Directory Services:** When an IssueNet user logs on, their contact information is created and updated based on the current values in Active Directory.
- **Update user group membership from Directory Services:** When an IssueNet user logs on, their group membership information is created and updated based on the current values in Active Directory.

It is important to note that the LDAP integration will not create or maintain security groups within IssueNet. The LDAP integration simply takes the list of Active Directory groups the user belongs to and looks for matching groups in IssueNet by name. If a match is found, the user is added to the IssueNet group when that user is created. If no matches are found the user is added to the default IssueNet users group.

LDAP Property Mapping

User and contact property names can vary among LDAP implementations. A simple property mapping mechanism is used to handle the transfer of information from the LDAP server to IssueNet for the creation and maintainence of users and contacts. In the Property Mapping list view you may edit the property names that map to specific IssueNet contact and user properties by selecting the property and clicking the **Edit...** button.

You may also specify default values for required IssueNet properties that do not map to any LDAP property. As an example if you had added required property to the contact that was specific to your issue management solution you would add a default value in the Property Mapping to allow the new contact to be created.

LDAP Through Web Service Connection

When using an IssueNet web service connection, LDAP is interrogated from within the security context of the web service. The security context of the web service is controlled by both the identity tag in the web.config file and by the site Directory Security settings for the web site. A user with security privileges sufficient to interrogate the LDAP server must be used. In a typical situation, this would be a domain user account.

To change the security context of the web service for the LDAP integration you should first change the web service identity tag set in site web.config file. To do this, open the IssueNet Assistant, select Access IssueNet Utilities, then select Configure web service security and logging. Select theMMFWebService site, click Edit and then enable the Use Identity Tag **for Authentication** option. Enter the domain user name and password to use for the web service security context. If you choose to encrypt the identity tag, you must ensure that the domain user you picked has read privileges to the HKEY_LOCAL_MACHINE\SOFTWARE\Elsinore\IssueNet registry key.

The next step is to change the site directory security settings. To do this, open Internet Information Server and navigate to the MMFWebService site. Select the **Actions | Properties** menu option then click on the **Directory Security** tab. Click the **Edit...** button in the Anonymous access and authentication control group at the top of the tab. Unselect the **Anonymous access** option and leave only **Integrated Windows authentication** selected. Click **OK** until you are back in Internet Information Server.

Additional Resources

Web Service Security Configuration
Windows Server 2003 Active Directory