

# User Data Retrieval Settings

Authenticated users usually have access to User DN attributes in the LDAP database. If user information retrieval is enabled and User DN attributes are accessible to the authenticated user, Teamwork Server retrieves their values and sets them for the corresponding external users.

If the **Simple User+Password** authentication type is enabled (either by using a static User DN template or by querying the LDAP server(s) for User DN), the User DN is retrieved in the same way. This connection is further reused for retrieving user information when the user logs in to the LDAP server.

Teamwork Server creates an external user with the login name specified by the user upon authentication if the user information retrieval is disabled or User DN attributes are not accessible to the authenticated user.

The screenshot shows the 'Teamwork Administrator's Console' window. The 'LDAP Integration' tab is selected, and the 'Properties' sub-tab is active. The 'Enable LDAP Integration' checkbox is checked, and a 'Test Connection' button is visible. The 'User Data Retrieval Settings' section is expanded, showing the 'Enable Authenticated User Data Retrieval' checkbox checked. Under 'User DN Attribute-to-Full Name Mapping\*', the text '\$(givenName) \$(sn), \$(l), telephoneNu' is entered, with an example 'Example: \$(cn) \$(sn)'. The 'Use User DN template' radio button is selected. The 'User DN\*' field is empty, with an example 'Example: cn=\$(login),dc=example,dc=com'. The 'Retrieve User DN by using an LDAP query' radio button is selected. The 'Query\*' field contains '(sAMAccountName=\$(login))', with an example 'Example: (sAMAccountName=\$(login))'. The 'Search Base\*' field contains 'dc=NoMagic, dc=com', with an example 'Example: dc=example,dc=com'. The 'Search Scope\*' dropdown is set to 'One level'. At the bottom, there are 'Refresh', 'Apply Changes', and 'Exit' buttons.

Teamwork Administrator's Console, LDAP Integration tab. User Data Retrieval Settings

**User Data Retrieval Settings** are described in the following table:

| Setting Name | Description |
|--------------|-------------|
|--------------|-------------|

|   |   |
|---|---|
| User DN<br>Attribute-to-Full<br>Name Mapping  | <p>After a specific User DN is found, the name of a local user created on the authentication is generated using the Full Name Mapping template for this User DN. The Full Name Mapping template supports placeholders in the form of <i>\$(attribute)</i>, where attribute is an attribute of DN.</p> <p>An example:</p> <p><code>\$(cn) \$(sn)</code></p> <p>This will form the Name of the created user out of two LDAP attributes - <i>cn</i> and <i>sn</i>.</p> |
| Settings that are active when the <b>Use User DN template</b> is selected.                    |   |
| User DN   | <p>User DN specifies a template used to search for a specific DN by the supplied login name. An example:</p> <p><code>cn=\$(login), dc=example, dc=com</code></p>   |
| Settings that are active when the <b>Retrieve User DN by using an LDAP query</b> is selected. |   |
| Query   | <p>An LDAP query for retrieving User DN, for example:</p> <p><code>sAMAccountName=\$(login)</code></p> <p><code>\$(login)</code> is a username a user types when <a href="#">connect to a server</a> from the modeling tool.</p> <p><code>aSAMAccount</code> is used for authorization to Windows OS and Active Directory as a directory service is set by default. You need to contact your system administrator if other OS or parameters are used.</p>           |
| Search Base   | <p>DN where the searching should begin, for example:</p> <p><code>dc=example,dc=com</code></p>  |
| Search Scope  | <p>Specifies whether the search must be restricted to the directly owned DNs only or performed in the whole subtree.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• One level</li> <li>• Subtree</li> </ul>   |