



StarTeam 16.3

LDAP QuickStart Manager
Administration Guide

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK
<http://www.microfocus.com>

Copyright © Micro Focus 2018. All rights reserved.

MICRO FOCUS, the Micro Focus logo and StarTeam are trademarks or registered trademarks of Micro Focus IP Development Limited or its subsidiaries or affiliated companies in the United States, United Kingdom and other countries.

All other marks are the property of their respective owners.

2018-03-27

Contents

About LDAP Quickstart Manager	4
Getting Started	5
Directory Services	5
LDIF Files	5
Overview of Setup and Import	5
Logging On	6
Sources Pane	7
Adding a Directory Service	7
Adding an LDIF File	8
Mappings	8
Creating an Initial Mapping	8
Checking the Initial Mapping	9
Investigating the LDAP Attributes	9
Improving the Mapping	10
Reviewing User Properties	11
Selecting LDAP Properties	11
Mapping LDAP Attributes to Custom User Properties	11
Reviewing Properties	12
Directory Service and LDIF File Properties	12
Group and User Properties	12
Refreshing Data in the Sources Pane	12
Targets Pane	14
Adding a Caliber Server	14
Adding a StarTeam Server	14
Displaying Group Information	14
Sorting User Information	15
Suspending Users	15
Refreshing Data in the Targets Pane	15
Importing Users	16
Importing Your Selections	16
Using the Wizard	17
Templates	18
Creating a Template	19
Using an Existing Template	19
Performing Other Template Operations	19
Configuring Default Import Options	19
Understanding Group Results	20
Using the Messages Pane	20

About LDAP Quickstart Manager

The LDAP Quickstart Manager allows you to import information about people from a directory service or LDIF file into Caliber or StarTeam Server as user properties.

In the main window, the configured directory services and LDIF files are in the **Sources** pane on the left. The configured servers are in the **Targets** pane on the right.

Getting Started

Directory Services

A directory service provides a place to store information about network-based resources, such as applications, files, printers, and people—although LDAP Quickstart Manager deals only with people and their attributes. The directory service provides a consistent way to name, describe, locate, access, manage, and secure information about these resources. A directory service helps an organization define and maintain its network infrastructure, perform system administration, and control the users' experience of its information systems.

StarTeam Server's Use of Directory Services

Both Caliber and StarTeam Server can use directory services (either Microsoft Active Directory or OpenLDAP) to perform password authorization. As users log on, they enter their product user names and their directory service passwords. Before allowing the users to access the server, the users then check a directory service for valid passwords.

For Caliber, all directory service configuration is done via the **Programs > Settings > Control Panel > CaliberRM Server utility**, via the **Directory Services** tab. See online help in Caliber for more information.

To set up directory service authentication in StarTeam Server, you must set options on the **Directory Service** tab of the **Server Administration** tool. These options enable directory service support and provide information about accessing the service. In addition, individual users cannot use this feature until their accounts are set up for directory service validation. You can use either StarTeam Server's **User Manager** or LDAP Quickstart Manager for this purpose. See the StarTeam Server *Administrator's Guide* for more information about the Server Configuration dialog and User Manager.

The distinguished name (DN), a unique identifier, is used by Micro Focus servers as they communicate with the directory service. Caliber and StarTeam Server must send each user's distinguished name (DN) to the directory service in order to verify the user's password. DNs can be long and not very intuitive. Also, some organizations change DNs occasionally, and updating these changes by hand can be very tedious. LDAP QuickStart Manager makes it easy to maintain the DNs and other directory service information that you choose to store in Caliber and StarTeam Server .

LDIF Files

A directory service uses the LDAP Data Interchange Format (LDIF) to describe entries in a UTF-8 encoded text format. Most of the directory service's command-line utilities rely on LDIF either for input or output. For example, LDIF is commonly used to build a directory database, add entries to it, or edit its existing entries. LDAP Quickstart Manager can use LDIF files to import information instead of directly accessing the directory service.

Overview of Setup and Import

LDAP Quickstart Manager simplifies maintenance of DNs and other user information. The following is a brief overview of setting up and importing users into LDAP Quickstart Manager. More details can be found elsewhere in this guide.

We recommend that you try importing users on a test server before importing users on a production server to make sure that you are importing users correctly.



Note: If you do not have the appropriate access rights on the servers that you want to access, you cannot import users with LDAP Quickstart Manager.

For Caliber Servers, the user must be a Caliber Administrator. For StarTeam Server, the user must have the server-level access right named Administer User Accounts. By default all members of the Administrators group have this and many other rights.

1. Configure one or more directory services and/or LDIF files. They appear in the **Sources** pane, on the left.

One of the required properties for each configured directory service or LDIF file is the name of the mapping to be used. You can start with one of the mappings that ship with the product: `Test Mapping`, `Microsoft Active Directory`, or `OpenLDAP`. Your directory service or LDIF file appears in the left pane as the root of a tree of nodes. Among these nodes you will find users and groups.

2. Configure one or more servers, which appear in the **Targets** pane, on the right.
Your server appears in the right pane as the root of a tree of nodes. Among these nodes you will find users and groups.
3. Select users, groups, or the entire directory service/LDIF file to be imported from the left pane.
4. Select a server or group from the right pane to receive the users and groups.
5. Click the **Import Selected Users** button. There is no *Undo* command. If you need to delete users or groups that have been added accidentally, you must do so from the StarTeam Server Administration tool (using User Manager) or from the Caliber Administrator. Be aware that users who are deleted and re-added to a StarTeam Server will have two internal user IDs and might have records for both. You cannot use LDAP Quickstart Manager to delete users, but you can select users in the right pane and suspend them. For Caliber, this is equivalent to making their accounts disabled. As mentioned, it is best to do a trial import on a test server before importing users on a production server.

Logging On

During each LDAP Quickstart Manager session, you must provide an acceptable DN or user identification and password the first time you access a directory service. You must also provide a user name and password the first time you access each Micro Focus server.

After that, LDAP Quickstart Manager remembers your credentials and continues to use them until you exit the session.

The following sections describe several situations in which a logon dialog may appear if you are accessing a directory service or a server for the first time. For example, you may need to log on when you open a directory service to select users and groups. Multiple logons may be required when you run a template. Logon instructions have been omitted from these procedures because the logon dialog is familiar and, if you have already logged on, it may not display.



Tip: The context menu for each server has a **Log On As** command which allows you to change from one user name to another, if necessary.

Sources Pane

The left pane in the LDAP Quickstart Manager main window displays LDAP sources: *Microsoft Active Directory*, *OpenLDAP* or *LDIF files* exported from one of the preceding two sources.

For each directory service or LDIF file used as a source of user information, you must define an object in the **Sources** pane.

The object's definition indicates:

- Whether the object is a directory service or an LDIF file.
- How to access the directory service or where to locate the LDIF file.
- A mapping that indicates:
 - How to recognize users and groups.
 - What attributes of those users and groups to import
 - What Caliber and StarTeam Server user properties will store the imported attributes

The mapping is specified only by name and can be reused in more than one directory service and/or LDIF file.

Adding a Directory Service

If LDAP Quickstart Manager will be used to access the directory service directly rather than via an intermediate LDIF file, you must add a directory service object to the **Sources** pane.

1. Click **Configure > Directory Service/LDIF File**. The **Directory Services/LDIF** dialog box opens.
2. Click **Add**. The **Add Source** dialog box opens.
3. Select the **Directory Service** option and click **OK**. The **Directory Services Properties** dialog box opens.
4. In the **Directory Services Properties** dialog box:
 - a) Enter a name in the **Name** field.
 - b) Enter the host name and port number in the **Host** and **Port** fields. The host name can be a computer name or an IP address. For Active Directory, you can use the domain name and locate a nearby instance of that directory service.
 - c) If the port is a secure (SSL) port, select the **Use a secure port** option.
 - d) Click **Test Settings**.
 - e) Select the correct version (2 or 3) of the protocol from the **Protocol Version** list.

LDAP Quickstart Manager negotiates with the LDAP service using either the LDAPv2 or LDAPv3 protocol. Version 3 is supported by most directory services. Your system administrator can tell you which version to select. If you must figure this out by trial-and-error, select 3 first, as that is the preferred protocol.
 - f) In the **Base DN** field, do one of the following:
 - Enter the base distinguished name (DN).
 - Click **Find**. The DNs it finds appear in the list.

If your host and port settings are incorrect or if the directory service is not running, you cannot use Find.
 - g) For now use one of the sample mappings: *Test Mapping*, *Microsoft Active Directory*, or *OpenLDAP*.

`Test Mapping` might be the best initial choice. However, you will need to change to a different mapping and/or adjust your selected mapping before you actually import users.

- h) Select the **Anonymous Logon** option if your directory service allows you to log on anonymously. This bypasses the Logon dialogs for the service.
- i) Click **OK**.



Note: From the **Directory Services/LDIF Files** dialog box, you can edit this object or delete it. For example, double-clicking the name opens its properties dialog so that you can review or edit those properties.

Adding an LDIF File

If LDAP Quickstart Manager will use an LDIF file instead of accessing the directory service directly, you need to add an LDIF file object to the **Sources** pane.

1. Click **Configure > Directory Service/LDIF File**. The **Directory Services/LDIF** dialog box opens.
2. Click **Add**. The **Add Source** dialog box opens.
3. Select the **LDIF File** option and click **OK**. The **LDIF File Properties** dialog box opens.
4. In the **LDIF File Properties** dialog box:
 - a) Enter a name in the **Name** field.
 - b) For now use one of the sample mappings: `Test Mapping`, `Microsoft Active Directory`, or `OpenLDAP`.

`Test Mapping` might be the best initial choice. However, you will need to change to a different mapping and/or adjust your selected mapping before you actually import users.
 - c) You can modify the sample or create a new mapping for this LDIF file later.
 - d) Enter or browse for the complete path to the LDIF file.
 - e) Click **OK**.



Note: From the **Directory Services/LDIF Files** dialog box, you can edit this object or delete it. For example, double-clicking the name opens its properties dialog so that you can review or edit those properties.

Mappings

Each object in the **Sources** pane that represents directory services or LDIF files must specify a mapping.

Mappings are used to do the following:

- Control the data from the directory service or LDIF file that appears in the **Sources** pane. Data is displayed in a meaningful way, allowing you to find and select users and groups more easily.
- Identify specific LDAP attributes that allow groups and users to be imported correctly. For example, you must identify the attribute that contains a group's name so that the servers can use the same name.
- Match specific LDAP attributes to specific user properties. Doing this allows you to control the values other than the DN that are imported for each user. DN names are imported automatically.

The only user property that you must specify is the LDAP attribute to be used as the user ID/user name on the server. The user whose name or ID has been imported must use this value to log on.

The following sections explain how to create your own mapping. These procedures should be followed in the order in which they are presented.

Creating an Initial Mapping

This section explains how to create a simple mapping. A simple mapping may not be suitable for immediately importing users and groups. You may have to refine it as explained in the next few sections.

1. Click **Configure > Mappings**. The **Mappings** dialog box opens.
2. Click **Add**. The **Mapping Properties** dialog box opens.
3. Enter the name in the **Name** field.
4. The **User Filter** and **Group Filter** fields are set to default settings often used by directory services. These settings may or may not work for your directory service or LDIF file, but leave them as they are for the time being.
5. The **Show All LDAP Nodes** check box is selected by default. Leave it that way so that you see all the possible nodes in the **Sources** pane.
6. Click **OK** and then **Close**.

Checking the Initial Mapping

Enter the prerequisites here (optional).

To determine if the default mapping settings are appropriate in your environment, you must assign the mapping to a directory service or LDIF file, open that object in the **Sources** pane, and see whether the data displayed is easily understood.

1. In the **Sources** pane, right-click a directory service or LDIF file object and select **Properties**. The **Directory Service Properties** or **LDIF File Properties** dialog box opens.
2. Select your mapping from the **Mapping** list.
3. Click **OK**.
4. In the **Sources** pane, expand the node for this object to see what information is displayed in the tree.

If the nodes represent your assets as you expect them to be, go to step 6 in [Investigating the LDAP Attributes](#) to verify.

If the nodes look more like long concatenated lists of strings, follow all the procedures in [Investigating the LDAP Attributes](#).

Investigating the LDAP Attributes

In this procedure, you will strip your initial mapping to its minimum settings so that you can review the nodes in the **Sources** pane for details that will help create a mapping with the best possible settings.

After investigating the effects of minimal mapping on the LDAP attributes, you can improve the mapping and the usability of the data shown in that pane.

1. Reduce your mapping to minimal settings:
 - a) Click **Configure > Mappings**.
 - b) Double-click the mapping to display the **Mapping Properties** dialog box.
 - c) In the **General** node, for the **User filter** and **Group filter** fields, specify an asterisk (*) as the value for `objectClass`. For example: `(objectClass=*)`
 - d) Select the **Group Attributes** node.
 - e) Clear all of the fields so that no settings exist for **Group Name**, **Child**, **Parent**, **User Display**, or **Group Display**.
 - f) Click **OK** and then **Close**.
2. Review the setting for your directory service or LDIF file object:
 - a) In the **Sources** pane, right-click a directory service or LDIF file object and select **Properties**. The **Directory Service Properties** or **LDIF File Properties** dialog box opens.
 - b) Make a note of the base DN.
 - c) Click **OK**.
3. In the **Sources** pane, expand the node for this object to see the information displayed in the tree. Note that the nodes are complete DNs.

4. Find the node that best matches your base DN and expand it, to look for users and groups.
5. Look for patterns and make notes about them. For example, before group names you may always find “OU” and before user names, you may always find “CN”. OU and CN are commonly used LDAP attribute names.
6. Examine the LDAP attributes for a group:
 - a) In the **Sources** pane, right-click a node that represents a group and select **Properties**. The **User/Group LDAP Properties** dialog box opens.
 - b) Select **All Properties**.
 - c) Find the `objectClass` attribute. Record your group’s `objectClass` values for later use.
 - d) Find the attribute for the group name. The name `AllGroups` is the value of the name and the OU attributes. Record one or both of these attributes for later use.
 - e) Look for attribute names that suggest that this object is the child or parent of another object, such as `Member` or `memberOf`. To complete this task, you may need help from your system administrator. If you find such attributes, write down the attribute names.
 - f) Click **OK**.
7. Examine the LDAP attributes for a user:
 - a) Right-click a node that represents a user, and select **Properties**. The **User/Group LDAP Properties** dialog box opens.
 - b) Select **All Properties**.
 - c) In the dialog, find the `objectClass` attribute. For example, the `objectClass` for a user may be `top`, `organizationalPerson`, and `user`. Record your user’s `objectClass` values for later use.
 - d) Look for attribute names that suggest that this object is the parent or child of another object, such as `Member` or `memberOf`. You may have to ask your system administrator for assistance with this task. For example, the user may have a `memberOf` attribute. Record that attribute name for later use.
 - e) Click **OK**.

Improving the Mapping

After you have located users and groups in the **Sources** pane and written down the attributes and values as explained in the previous section, return to the **Mapping Properties** dialog box.

1. Click **Configure > Mappings**.
2. Double-click the mapping to be edited.
3. Adjust the `objectClass` values in the **User Filter** and **Group Filter** with a value found for `objectClass` in the previous procedure.
4. Select **Group Attributes**.
5. Use the attribute names that you found in the **Sources** pane as values for the **User Display** and **Group Display** fields:

Group Name Attribute that will be imported into the server as the name of a group. This attribute is required if you intend to import one or more groups of users.

Child Attribute that will identify the children of an entry, in this case, a group. For example, you might use an attribute such as `Member` here. This attribute is usually used to identify group hierarchies.

Parent Attribute that will identify the parent of an entry, in this case, a user or group. For example, you might enter `memberOf` here. This attribute is usually used to determine membership in a group.

Group Display Attribute that will be displayed in the **Sources** pane instead of the DN for a group.

User Display Attribute that will be displayed in the **Sources** pane instead of the DN for a user.

6. Click **OK** and then **Close**.

7. In the **Sources** pane, expand the directory service or LDIF file object to see how information now displays in the tree.

The folders that correspond to neither the user nor group filter are shown in the tree as groups if you select the **Show All LDAP Nodes** check box. When you have finished fine-tuning the mapping, you can clear the **Show All LDAP Nodes** check box, and these nodes will be removed from the **Sources** pane.

If the Sources pane is now more readable and understandable, you have probably finished refining the display. To refine the mapping even more, you can repeat the last few procedures.

Your final mapping task is to identify the LDAP attributes that will replace Caliber and StarTeam user properties.

Reviewing User Properties

Every mapping needs to indicate what LDAP attributes are to be imported from the directory service or LDIF file into the selected server as user properties.

The DN is imported automatically, but you can import general Caliber and StarTeam user properties, too, as long as there are LDAP attributes that contain that information.

The **Mapping Properties** dialog in LDAP Quickstart Manager uses a similar dialog to show both Caliber and StarTeam user properties. In some cases, the applications have common properties, even though the names may be slightly different, such as **Location** and **Address**.

In the **Mapping Properties** dialog, you do not see the actual names and telephone numbers. Instead, you see the names of the LDAP attributes whose values are the actual names and numbers.

The only field in the **Mapping Properties** dialog box that must contain the name of an LDAP attribute for a successful import operation is the **User ID/User Name** field. The servers will not accept a new user without having an ID or name that can be used when the user logs on.

Selecting LDAP Properties

In an earlier section, you reviewed LDAP attributes for users to refine the mapping. Now you must review the same dialog to look for attributes whose values match Caliber and StarTeam user properties.

1. Right-click a node that represents a user, and select **Properties**. The **User/Group LDAP Properties** dialog box opens.
2. Select **All Properties**.
In the sample dialog, the **Given Name** attribute is a good match for the Caliber **First Name** property and the **Name** attribute is a good match the StarTeam **Full Name** property.
3. Scroll through the attributes, and list the matches that you want to use.
4. Be sure to identify an attribute that can be used as the `user ID` in Caliber or the `user name` in StarTeam because that user property is required.

Mapping LDAP Attributes to Custom User Properties

In an import operation, all LDAP attributes that you map to Custom user properties will be imported along with new users into the server.

1. Click **Configure > Mappings**.
2. Double-click the mapping to be edited.
3. Select **User Properties** mapping.
4. Enter the names of the LDAP attributes that correspond to the Custom properties in the appropriate fields.

5. Be sure to provide an attribute for the **User ID/User Name** field. Otherwise, the import operation will fail.
6. To limit the amount of data retrieved from the directory service or LDIF file to the values being mapped, select the **Retrieve Mapping Attributes Only** check box.
7. Click **OK** and **Close**.

Reviewing Properties

With the LDAP Quickstart Manager, you can review properties for directory services, LDIF files, groups, users, and so on. Every node in the **Sources** pane has a properties dialog, except the root node (named `Directory Services/LDIF Files`).

Directory Service and LDIF File Properties

The properties for a directory service or LDIF file are the same as those you see when you create a directory service or LDIF file object. After displaying these properties, you can edit them.

1. In the **Sources** pane, right-click a directory service or LDIF file object and select **Properties**. The **Directory Service Properties** or **LDIF File Properties** dialog box opens.
2. Review or edit the properties.
3. Click **OK** or **Cancel**.

Group and User Properties

The properties dialog for a group or an individual user shows the values of the LDAP attributes mapped to the Caliber and StarTeam group or user properties. By looking at the dialog, you can review how well the mapping matches.

The dialogs, which are read-only, also show all properties listed for the group or user in the directory service or LDIF file.

1. Right-click the group or user name in the **Sources** pane.
2. Select **Properties**.
3. Review the properties.
4. Click **OK**.

For more information, see [Reviewing User Properties](#).

Refreshing Data in the Sources Pane

LDAP Quickstart Manager performs refreshes automatically when you make changes to the **Sources** pane. However, you can also manually refresh this pane.

To refresh the **Sources** pane, do one of the following:

- Click the **Refresh Directory Services/LDIF Files** toolbar button.
- Select **View > Refresh > Refresh Sources** from the menu bar.
- Press **Alt+1**.
- Right-click the **Sources** pane root node (named `Directory Services/LDIF Files`) and select **Refresh** from the context menu.

To refresh both panes, do one of the following:

- Click the **Refresh All** toolbar button.

- Select **View > Refresh > Refresh All** from the menu bar.
- Press **F5**.


Targets Pane

To import users and groups from directory services and LDIF files, you must provide access information for at least one Caliber or StarTeam Server.

Adding a Caliber Server

For a Caliber server to receive user information from a directory service or LDIF file, it must be represented in the **Targets** pane of the main window.


1. Click **Configure > Caliber Server**.
2. Click **Add**.
3. Enter a name for this server in the **Name** field.
4. Enter a host name or IP address in the **Host** field.
5. Click **OK**. The server object appears in the **Targets** pane.


 **Tip:** From this dialog, you can edit the server object or delete it. For example, double-clicking the name of a server object opens its properties dialog so that you can review or edit those properties. You can also right-click the object in the **Targets** pane, and select **Properties** or **Delete**.

Adding a StarTeam Server

For a Caliber server to receive user information from a directory service or LDIF file, it must be represented in the **Targets** pane of the main window.

1. Click **Configure > StarTeam Server**.
2. Click **Add**.
3. Enter a name for this server in the **Name** field.
4. Enter a host name or IP address in the **Host** field.
5. Click **OK**. The server object appears in the **Targets** pane.

 **Note:** The `Directory Service Validation` node provides connection status information. If you review the properties for a server, you will see information about the connection. For example, if the server is not running, you will see the message: `Cannot connect to server`.

 **Tip:** From this dialog, you can edit the server object or delete it. For example, double-clicking the name of a server object opens its properties dialog so that you can review or edit those properties. You can also right-click the object in the **Targets** pane, and select **Properties** or **Delete**.

Displaying Group Information

You can control the data displayed in the **Targets** pane for all the servers and how it is sorted.

LDAP Quickstart Manager always displays the users in the servers to which it is connected. However, you can toggle group information on and off.

To display or hide information about server groups, do one of the following:

- Click the **Display StarTeam/Caliber Groups** toolbar button.
- Select **View > Display Groups** from the menu bar.
- Press **Ctrl+G**.
- Right-click **Servers** (the first node in the **Targets** pane). Then select **Display Groups** from the context menu.

Any of these changes the state of *Display Groups*. When displayed, a checkmark appears beside the **Display Groups** menu item.

Sorting User Information

Users can be listed alphanumerically by name or by user ID, whichever is appropriate. To sort by name, do one of the following:

- Select **View > Sort > By Name**.
- Press **Alt+N**.
- Right-click **Servers** (the first node in the **Targets** then select **Sort > By Name**.

To sort by user ID, do one of the following:

- Select **View > Sort > By User ID**.
- Press **Alt+I**.
- Right-click **Servers** then select **Sort > By User ID**.

Suspending Users

You can suspend users from the servers. A suspended user cannot log on to StarTeam or Caliber. You cannot delete users (or groups) through LDAP Quickstart Manager.

1. Right-click a user.
2. Select **Suspend**.
3. Click **Yes** to confirm.



Note: When you suspend a CaliberRM user in LDAP Quickstart Manager, Caliber shows the user as `Account Disabled`.

Refreshing Data in the Targets Pane

LDAP Quickstart Manager performs refreshes automatically when you make changes to the **Targets** pane. However, you can also manually refresh this pane.

To refresh the **Targets** pane, do one of the following:

- Click the **Refresh StarTeam/Caliber Servers** toolbar button.
- Select **View > Refresh > Refresh Targets**
- Press **Alt+2**.
- Right-click the **Target** pane's root node and select **Refresh**.



Note: You can refresh individual users, groups, and servers, by right-clicking on their names and select **Refresh** from their context menus. The data in the pane is updated based on changes in the server's database. Refreshing both panes, of course, also refreshes the **Targets** pane. See [Refreshing Data in the Sources Pane](#) for details about refreshing both panes simultaneously.

Importing Users

Once you have configured sources and targets, there are several ways to import and update information about users and groups. You can:

- Make your selections directly from the Sources and Targets panes.
- Make selections using the Import Users Wizard.
- Create templates that can be reused from the UI.

All of these operations are available through and briefly explained on the **Import Users** dialog box.

1. Click **Import > Users**. The **Import Users** dialog opens. It allows you to import users based on selections already made to the **Sources** and **Targets** pane, with the wizard, or with a template that you have previously created.
2. Select one of the three options and click **OK**. Each of the options is explained in the following sections.
3. After you click **OK** (or after you complete the wizard if you selected the **With The Wizard** option button), you should check the Messages pane for information about your import operation.



Note: To display or hide the Messages pane, select **View > Messages** from the menu bar or press **Alt+M**.

Importing Your Selections

One of the easiest ways to import users and groups is to make selections from the **Sources** and **Targets** panes of the main window and click the **Import Selected Users** toolbar button. Before you import this way, you should do two things:

- Select the **Configure > Default Import Options** command and review the **General**, **StarTeam**, and **Caliber** settings. These settings will be used during your import operation unless you change them before the import starts.
- Refresh the StarTeam and Caliber target servers (choose **View > Refresh > Refresh Targets**.)

To import users and groups based on selections in the main window:

1. From the **Sources** pane, select specific users, groups of users, or the entire directory service or LDIF file. You may have to expand the nodes to see users and groups.
2. From the **Targets** pane, select specific groups or entire servers. When you select a Caliber server, your selections from the **Sources** pane end up in the group named `LDAP Group`. When you select a StarTeam Server, your selections from the **Sources** pane end up in the group named `All Users`.
3. Do one of the following:
 - Click the **Import Selected Users** toolbar button.
 - Press **Ctrl+U**.
4. In the **Default Import Options** dialog box, verify the selections and click **OK**.



Note: You can also drag-and-drop one user or one group (and its children) from the **Sources** pane to a location in the **Targets** pane. You cannot drag users from one location to another in the same pane. You cannot drag users from the **Targets** pane to the **Sources** pane.

Using the Wizard

Using the wizard allows you to perform an import operation and at the same time create a template. If you prefer, you can use the wizard only to create a template. To import users and groups using the wizard:

1. Select **Import > Users**. The Import Users dialog box opens.
2. Select the **With the wizard** option and click **OK**. The **Import Wizard: Selecting Sources** opens and displays the directory services and LDIF files from the **Sources** pane. You must expand the nodes to see users and groups. You can also right-click any node to see and use its context menu.
3. Select specific users, groups of users, or the entire directory service or LDIF file and click **Next**. The **Import Wizard: Selecting Target Destinations** dialog displays the servers in the **Targets** pane. You must expand the nodes to see users and groups. You can also right-click any node to see and use its context menu.

When you select a Caliber server, your selections from the **Sources** pane end up in the group named **LDAP Group**.

When you select a StarTeam server, your selections from the **Sources** pane end up in the group named **All Users**.

4. Select at least one group or server to receive the imported users. Click **Next**. The **Import Wizard: Setting Options** dialog opens.
5. Use the **Import Wizard: Setting Options** dialog to control what exactly happens to the imported data.
6. Select or clear the **Import Users Now** check box.

When this box is selected, the import executes immediately after you complete the wizard.

When this box is cleared, the import does not execute. Presumably, you want to make a template and not import at this time.

7. Select or clear the **Overwrite Existing User Properties** check box.

When this box is selected, the values in the directory service or LDIF file become the values for the mapped user properties on the selected server. This updates the information on existing users.

When this box is cleared, only users who are not already in the server's database are added along with their properties. Existing users are ignored.

8. Select or clear the **Save Settings As Template For Future Use** check box.

When this box is selected, a template is made that allows you to perform this same import operation again.

When this box is cleared, this import operation becomes a one-time import.

9. If you have elected to create a template, enter a name for this template in the **Template Name** field.

10. Click **Advanced** to set up advanced options for users:

- a) To add StarTeam password authentication and licensing for any users that will be added to StarTeam as part of the import operation. Specify whether you want to apply the validation to all StarTeam users. When **Apply validation to all users** is unchecked, the validation setting only applies to new StarTeam users. Do one of the following:

- Specify that new users will have their passwords authenticated by a directory service, which means that the user will supply a StarTeam user name and a directory service password in order to log on. For each user whose password is validated by a directory service, a distinguished name (DN) must be stored for later use by the server. This option can be set from the StarTeam **Server Administration** tool or in LDAP Quickstart Manager (using LDAP is easiest.)



Note: Before StarTeam servers can request directory service validation of user passwords, you must enable directory service support in the StarTeam **ServerAdministration** tool. Set

- the **Directory Service** options on the **Configure Server** dialog box to enable directory service support and supply the connection information to a directory service such as Active Directory.
 - Specify that new users will have their passwords authenticated through StarTeam server, then select the **Assign initial password** check box if you want new users to be able to log on immediately, even though they all have the same password.
 - If you selected the **Assign initial password** check box, you must enter a password in both the **Password** and **Confirm** text boxes.
 - Select the **Force password change on next logon** check box if you want users to be forced to change from the specified password to a personal password when they first log on to the StarTeam server.
 - Select the Unassigned, StarTeam concurrent, StarTeam named, or License server option button to specify the type of license to be given to the users in this import operation. Do not confuse StarTeam named and StarTeam concurrent licenses with License server licenses. Even though License server licenses can be either named user or concurrent licenses, they come with slip IDs.
 - If you selected the **License server** option button, you must enter a slip ID number in the **Slip ID** field.
- b) To add Caliber password authentication and licensing for any users that will be added to Caliber as part of the import operation:
1. Select Caliber. The **Advanced Options** dialog changes.
 2. Specify whether you want to apply the validation to all Caliber users. When Apply validation to all users is unchecked, the validation setting only applies to new Caliber users. Do one of the following:
 - Indicate whether new users will have their passwords authenticated by Caliber server or by a directory service by selecting either the **Validate password through directory service** or the **Validate password through Caliber server** option.
 - If you select password validation through the Caliber server, select the **Assign initial password** check box if you want new users to be able to log on immediately, even though they all have the same password.

If you selected the **Assign initial password** check box, you must enter a password in both the **Password** and **Confirm** text boxes.

Select the **Force password change on next logon** check box if you want users to be forced to change from the specified password to a want users to be forced to change from the specified password to a personal password when they first log on to the Caliber server.
 3. Select the Not Authorized, Caliber Concurrent, Caliber Named, or License Server option button to specify the type of license to be given to the users in this import operation. Do not confuse Caliber Named and Caliber Concurrent licenses with License Server licenses. Even though License Server licenses can be either named user on concurrent licenses, they come with slip IDs.
 4. If you selected the License Server option button, you must enter a slip ID number in the Slip ID text box.
11. Click **OK**.
 12. Click **Next**.
 13. The **Import Wizard: Summary** dialog summarizes your choices so that you can review them.
 14. Click **Finish** to start the import.

Templates

Generally, when you create a template, you will select groups of users or the entire directory service or LDIF file from the first wizard dialog. Doing this allows you to update existing users and import information

about any new users. Selecting specific users in a template allows you to update information on those users only. You cannot import information about any other users.

Creating a Template

All templates are created using the wizard. However, there are a number of ways to display the wizard.

To create a template, do one of the following:

- Use the wizard directly. Follow the directions in [Using the Wizard](#).
- Click the **Templates** toolbar button. From the resulting **Templates** dialog, click **Add**. This displays the wizard.
- Press **Ctrl+T**. From the resulting **Templates** dialog, click **Add**. This action displays the wizard.

Using an Existing Template

After a template has been created, it can be reused any number of times. To use an existing template, do one of the following:

- Click the **Templates** toolbar button. From the resulting **Templates** dialog, select the template, and click **Import**.
- Press **Ctrl+T**. From the resulting **Templates** dialog, select the template, and click **Import**.
- Select **Import > Users**. From the resulting **Import Users** dialog, select the **With a Template** option button, select the template name from the list, and click **OK**.

Performing Other Template Operations

You can use the **Templates** dialog to review the information about a template or delete the template.

Review Summary

1. Click **Ctrl+T**.
2. Select a template.
3. Click **View**.

The **Template Properties** dialog lists the summary information that appeared in the wizard when you created the template.

Delete

1. Click **Ctrl+T**.
2. Select a template name.
3. Click the **Delete** button.

Configuring Default Import Options

If you want to override the default import options, you can do so within the **Import Wizard**. However, using the wizard does not allow you to drag-and-drop a user or group and its children from the **Sources** pane to the **Targets** pane. LDAP Quickstart Manager provides an alternative way to change these settings, so that you can drag-and-drop with the options you have chosen. To change default import selections (outside the **Import Wizard**):

1. Click **Configure > Default Import Options**. This action displays the **Default Import Options** dialog box, which has three nodes: **General**, **StarTeam**, and **Caliber**.
2. Click on the **General** node.
 - a) Determine whether you wish to **Overwrite** existing user's properties.
 - b) Indicate whether you want to show this dialog automatically.

3. Click the **StarTeam** node.
 - a) Specify whether you want to apply the validation to all StarTeam users. When Apply validation to all users is unchecked, the validation setting only applies to new StarTeam users.
 - b) Specify whether you wish to validate the password through directory service or StarTeam.
 - c) If you select password validation through StarTeam, enter an initial password and indicate whether you want to force a password change at next logon.
 - d) Select the appropriate type of user license. The choices are: Unassigned (default), StarTeam Concurrent, StarTeam Named, and License Server. If you select License Server, you must also enter a SLIP ID. Do not confuse StarTeam named and StarTeam concurrent licenses with License server licenses. Even though License server licenses can be either named user or concurrent licenses, they come with slip IDs.
4. Select the **Caliber** node.
 - a) Specify whether you want to apply the validation to all Caliber users. When Apply validation to all users is unchecked, the validation setting only applies to new Caliber users.
 - b) Specify whether you wish to validate the password through directory service or Caliber Server.
 - c) If you select password validation through the Caliber Server, enter an initial password and indicate whether you want to force a password change at next logon.
 - d) Specify the license type: Not Authorized, Caliber Concurrent, Caliber Named, or License Server option button to specify the type of license to be given to the users in this import operation. If you select License Server, you must also enter a SLIP ID. Do not confuse Caliber Named and Caliber Concurrent licenses with License Server licenses. Even though License Server licenses can be either named user on concurrent licenses, they come with slip IDs.
5. Click **OK** when you have adjusted the default settings as desired. These settings will apply to new users only.

Understanding Group Results

Groups in a directory service or LDIF file are hierarchical. StarTeam groups are also hierarchical, but, in Caliber, no group is a subgroup of another.

When you import a hierarchy of groups into StarTeam, that hierarchy is maintained in the new location.

When you import a hierarchy of groups into Caliber Server, the hierarchy disappears. If two imported groups have the same names, they are combined into a single group. For example, suppose during one import operation, you import a group named Detroit along with its two subgroups, Managers and Workers. This import operation would result in three new groups in Caliber: Detroit, Managers, and Workers. No parent/child relationships would be preserved. Suppose that you later import a group named Toronto and its two subgroups named Managers and Workers. The end result in Caliber would be four groups: Detroit, Toronto, Managers, and Workers. The Managers and Workers groups would contain users from both Detroit and Toronto, while the Detroit and Toronto groups might be empty.

Using the Messages Pane

The Messages pane displays messages about successful operations and errors encountered during the import. You can use the context menu to hide the messages, clear the pane, or save the pane's contents to a text file.

To use the context menu:

1. Right-click anywhere in the pane.
2. Click **Hide Info** to stop displaying the **Messages** pane.
3. Click **Clear** to empty the **Messages** pane.
4. Click **Save Log** to store the messages in a text file.

Index

A

- about 4
- adding a Caliber server 14
- adding a directory services 7
- adding a StarTeam server 14

C

- configure default options 19

D

- directory services 5
- displaying group information 14

G

- group results 20

I

- import your selections 16
- importing users 16
- investigating the LDAP attributes 9

L

- LDIF file
 - about 5
 - adding 8
- logging on 6

M

- mappings

- checking initial 9
- creating initial 8
- improving 10
- LDAP to custom 11
- selecting LDAP properties 11
- user properties 11
- messages pane 20

O

- overview 5

R

- refresh source pane 12
- refreshing Target pane data 15
- reviewing group/user properties 12
- reviewing properties 12

S

- sorting user info 15
- sources pane 7
- suspending users 15

T

- targets pane 14
- templates
 - additional operations 19
 - creating 19
 - use existing 19

U

- using the wizard 17