StarTeam/CaliberRM LDAP QuickStart Manager 2009

Administration Guide

Borland®
THE OPEN ALM COMPANY

Borland Software Corporation
8310 N Capital of Texas
Bldg 2, Ste 100
Austin, TX 78731 USA
http://www.borland.com

Part Number ST00-LDAP
June 2009
PDF

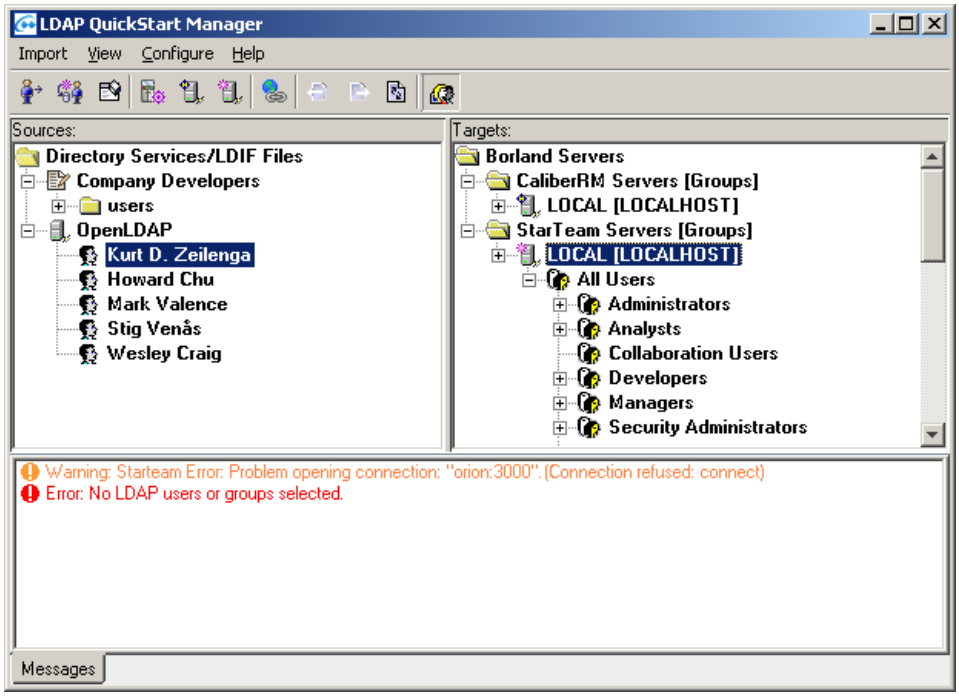
Contents

Chapter

1

Introducing StarTeam/CaliberRM LDAP QuickStart Manager

StarTeam/CaliberRM LDAP QuickStart Manager is a utility that allows you to import information about people from a directory service or LDIF file into a CaliberRM or StarTeam server as user properties.



In the main window of LDAP QuickStart Manager, the configured directory services and LDIF files are in the Sources pane on the left. The configured CaliberRM and StarTeam Servers are in the Targets pane on the right.

If you perform an import operation with the selections shown in this figure, the attributes for the selected user (Kurt D. Zeilenga) will be imported into the local StarTeam Server and placed in the All Users group. Any errors that occur during this process will appear iStarTeam/CaliberRM LDAP Messages pane at the bottom of the LDAP QuickStart Manager main window.

About This Release

Documentation

All documentation for StarTeam/CaliberRM LDAP QuickStart Manager 2009, including installation instructions, release notes, and this guide, can be found on the **Start>Borland StarTeam>Borland LDAP QuickStart Manager>Documentation** menu.

Understanding CaliberRM and StarTeam's Use of Directory Services

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

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

To set up directory service authentication in StarTeam Server, you must set options on the Directory Service tab of the *Server 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 Administrator's Guide* for more information about the Server Configuration dialog and User Manager.

The distinguished name (DN), a unique identifier, is used by Borland servers as they communicate with the directory service. CaliberRM and StarTeam 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 CaliberRM and StarTeam Servers.

Understanding 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.

Understanding 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.

Understanding LDAP QuickStart Manager

LDAP QuickStart Manager simplifies maintenance of DNs and other user informtion in CaliberRM and StarTeam Servers.

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.

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

To set up LDAP QuickStart Manager and import users:

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 Borland 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 CaliberRM or StarTeam server or group from the right pane to receive the users and groups.

5. Click the Import Selected Users toolbar button.

Caution 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 CaliberRM 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 CaliberRM, 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.

LDAP QuickStart Manager also offers an import wizard and templates to import users quickly, easily, and repeatedly. All of these operations are briefly explained on the *Import Users* dialog. They are also explained later in this Guide.

Having Appropriate Access Rights

If you do not have the appropriate access rights on the CaliberRM and StarTeam Servers that you want to access, you cannot import users with LDAP QuickStart Manager.

For CaliberRM Servers, the user must be a CaliberRM Administrator. For StarTeam Servers, 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.

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 Borland server.

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

The following chapters describe several situations in which a logon dialog may appear if you are accessing a directory service or a Borland 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.

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

Chapter

2

Using the Sources Pane

The left pane in the LDAP QuickStart Manager's 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 CaliberRM and StarTeam 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.

To add a directory service object to the Sources pane:

1 Do one of the following:

- Click the Directory Services/LDIF toolbar button.
- Select Configure > Directory Service/LDIF File from the menu bar.
- Press *Ctrl+L*.
- Right-click Directory Services/LDIF Files (the first node in the Sources pane) and select Add Directory Service from the context menu. Then go to Step 4.

The *Directory Services/LDIF* dialog opens.

2. Click Add.The *Add Source* dialog opens.
3. Select the Directory Service option button and click OK.

   The *Directory Services Properties* dialog opens.
4. In the *Directory Services Properties* dialog:
   a. Enter a name for this directory service in the Name text box.
   b. Enter the host name and port number in the Host and Port text boxes.

      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” check box.
   d. Click Test Settings to be sure that LDAP QuickStart Manager can access the directory service.
   e. Select the correct version (2 or 3) of the protocol from the Protocol Version drop-down list box.

      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 text box, do one of the following:
      - Enter the base distinguished name (DN)
      - Click Find to have LDAP QuickStart Manager find the DN for you. The DNs it finds appear in the drop-down list box.

      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 that comes with LDAP QuickStart Manager: 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 check box if your directory service allows you to log on anonymously. This bypasses the Logon dialogs for the service.
   i. Click OK.

Tip From the *Directory Services/LDIF Files* dialog, you can edit this directory service object or delete it. For example, double-clicking the name of a directory service object 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.

To add an LDIF file object to the Sources pane:

1. Do one of the following:
   - Click the Directory Services/LDIF toolbar button.
   - Select Configure > Directory Service/LDIF File from the menu bar.

- Press *Ctrl+L*.
- Right-click Directory Services/LDIF Files (the first node in the Sources pane). Then select Add LDIF File from the context menu and go to Step 4.

The *Directory Services/LDIF* dialog opens.

2. Click Add. The *Add Source* dialog opens.
3. Select the LDIF File option button and click OK.

   The *LDIF File Properties* dialog opens.
4. In the *LDIF File Properties* dialog:
   a. Enter a name for the LDIF file in the Name text box.
   b. For now use one of the sample mappings that comes with LDAP QuickStart Manager: 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.

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

Understanding 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. When LDAP QuickStart Manager displays the data in a meaningful way, you can 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 Borland servers can use the same name.
- Match specific LDAP attributes to specific StarTeam and/or CaliberRM 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 StarTeam or CaliberRM 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 by using a sample mapping named "My Company's Mapping" for an imaginary directory service. 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.

To create a mapping:

1 Do one of the following:

- Click the Mappings toolbar button.
- Select Configure > Mappings from the menu bar.
- Press *Ctrl+M*.

The *Mappings* dialog opens.

2 Click Add. This action opens the *Mapping Properties* dialog.

3 Enter the name for your mapping in the Name text box.

4 The User Filter and Group Filter text boxes 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 to exit the *Mapping Properties* dialog.

7 Click Close to return to the main window.

You now have created an initial mapping. Now you must determine how well the default settings work in your environment.

Checking the Initial Mapping

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.

To check the initial mapping:

1 In the Sources pane, right-click a directory service or LDIF file object and select Properties from the context menu.

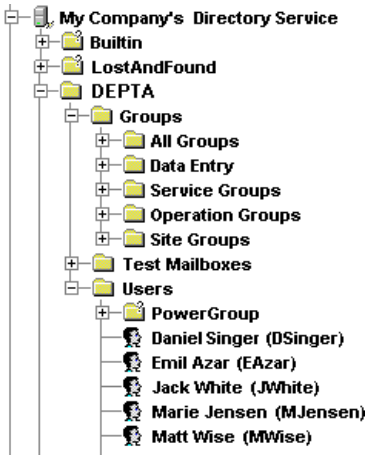
2 In the resulting *Directory Service Properties* or *LDIF File Properties* dialog, select your mapping from the Mapping drop-down list box.

3 Click OK to exit the dialog.

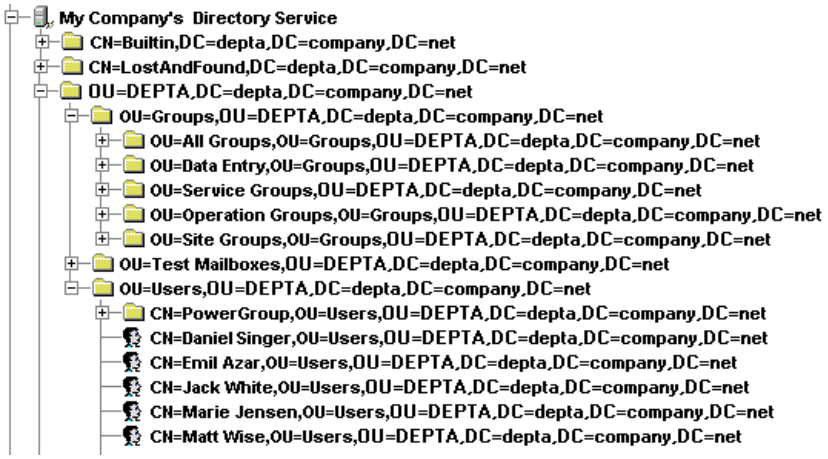
4 In the Sources pane, expand the node for this object to see what information is displayed in the tree.

5 Check the nodes for readability.

For example, does the tree look like this figure?



Or does the tree look like this figure?



If the tree resembles the first illustration, much of your work is done, but you still need to determine whether the values on the Group Attribute page of the *Mapping Properties* dialog in your mapping are correct. Go to step 6 in "Investigating the LDAP Attributes".

If the tree resembles the second illustration, you must learn how to select the LDAP attributes used in a mapping. Complete all the steps in "Investigating the LDAP Attributes".

When the tree resembles the first illustration, you can sort by the user's name or ID (for example by Daniel Singer or by DSinger). Select View > Sort > By Name or View > Sort > By User ID.

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 in the Sources pane, you can improve the mapping and the usability of the data shown in that pane.

To investigate LDAP attributes:

1 Reduce your mapping to minimal settings:

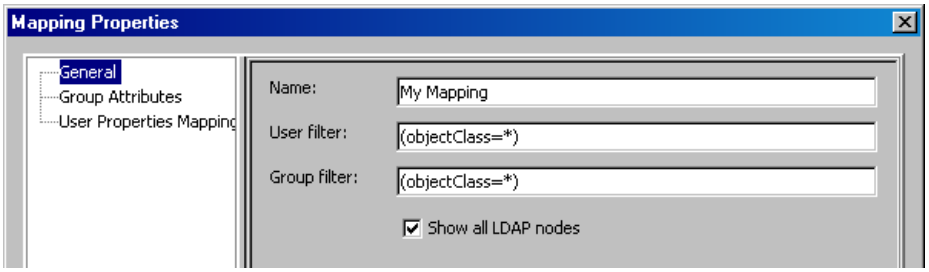
a Do one of the following:

- Click the Mappings toolbar button.
- Select Configure > Mappings from the menu bar.
- Press *Ctrl+M*.

The *Mappings* dialog opens.

b Double-click the mapping to display the *Mapping Properties* dialog.

c For the user and group filters, specify an asterisk (*) as the value for objectClass as shown below.



d Select Group Attributes.

e Clear all of the text boxes so that no settings exist for Group Name, Child, Parent, User Display, or Group Display.

f Click OK to exit the dialog.

g Click Close to return to the main window.

2 Review the setting for your directory service or LDIF file object.

a In the Sources pane, right-click the directory service or LDIF file object and select Properties from the context menu.

b In the resulting *Directory Service Properties* or *LDIF File Properties* dialog:

1 Make a note of the base DN.

2 Make sure that your mapping is the one shown in the Mapping drop-down list box.

3 Click OK to exit the dialog.

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 from the context menu. The *User/Group LDAP Properties* dialog opens.

b Select All Properties.

c In the dialog, find the objectClass attribute. Record your group’s objectClass values for later use.

d Find the attribute for the group name. In the example above, 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 from the context menu. The *User/Group LDAP Properties* dialog 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 section named "Investigating the LDAP Attributes", return to the *Mapping Properties* dialog to apply what you have learned.

To update the mapping:

1. Do one of the following:
   - Click the Mappings toolbar button.
   - Select Configure > Mappings from the menu bar.
   - Press *Ctrl+M*.

   The *Mappings* dialog opens.
2. Double-click the mapping to be edited. The *Mapping Properties* dialog opens.
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 text boxes.

   Group Name: Attribute that will be imported into the CaliberRM or StarTeam 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 to exit the *Mapping Properties* dialog.
7. Click Close to return to the main window.

8 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.

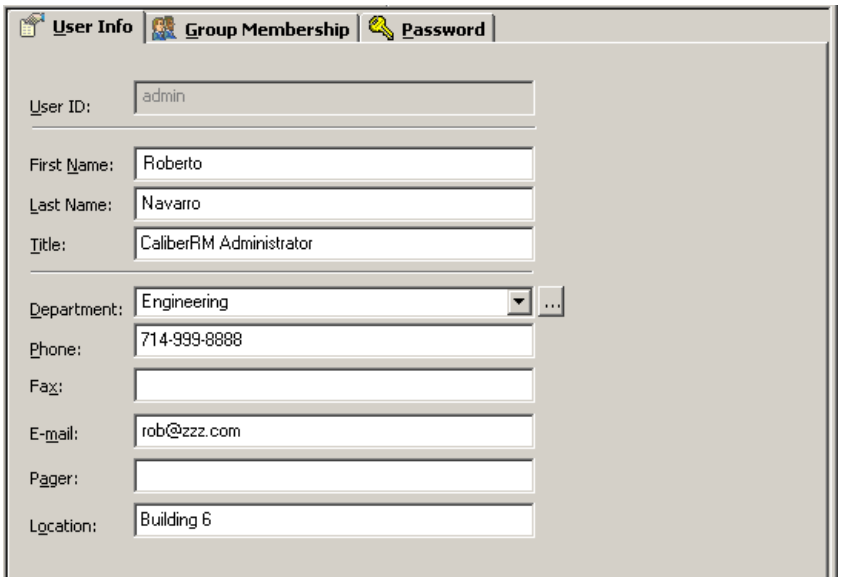
Your final mapping task is to identify the LDAP attributes that will replace CaliberRM and StarTeam user properties.

Reviewing Borland User Properties

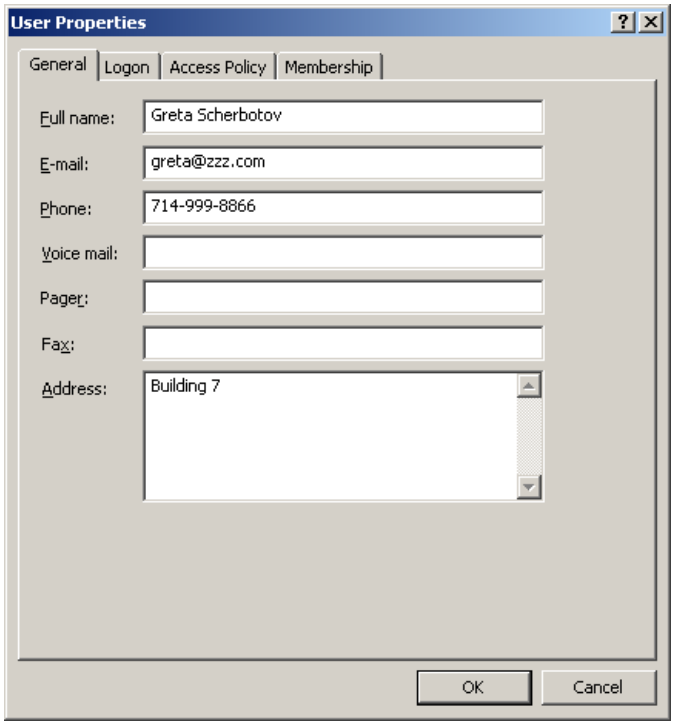
Every mapping needs to indicate what LDAP attributes are to be imported from the directory service or LDIF file into the selected CaliberRM and/or StarTeam Servers as user properties.

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

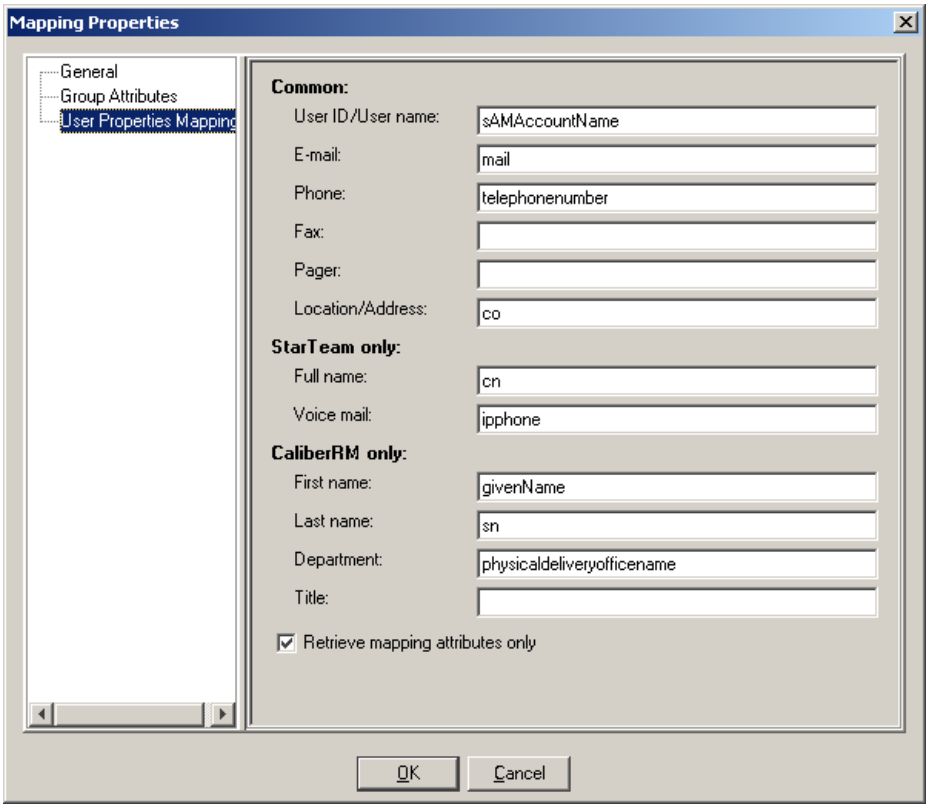
The following dialog shows the general user properties for CaliberRM:



The following dialog shows the general user properties for StarTeam:



The *Mapping Properties* dialog in LDAP QuickStart Manager uses a similar dialog to show both CaliberRM 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 text box in the *Mapping Properties* dialog that must contain the name of an LDAP attribute for a successful import operation is the User ID/User Name text box. 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 Attributes

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 CaliberRM or StarTeam user properties.

To review LDAP user attributes:

1. Right-click a node that represents a user, and select Properties from the context menu. The *User/Group LDAP Properties* dialog opens.
2. Select All Properties. In the sample dialog, the “given name” attribute is a good match for the CaliberRM “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 CaliberRM or the user name in StarTeam because that user property is required.

Mapping LDAP Attributes to Borland User Properties

In an import operation, all LDAP attributes that you map to Borland user properties will be imported along with new users into the CaliberRM or StarTeam Servers. An import operation can also, optionally, update the properties of existing users.

To map LDAP attributes to Borland user properties:

1. Do one of the following:
   - Click the Mappings toolbar button.
   - Select Configure > Mappings from the menu bar.
   - Press *Ctrl+M*.

   The *Mappings* dialog opens.
2. Double-click the mapping to be edited. The *Mapping Properties* dialog opens.
3. Select User Properties Mapping.
4. Enter the names of the LDAP attributes that correspond to the Borland properties in the appropriate text boxes.
5. Be sure to provide an attribute for the User ID/User Name text box. 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 to exit the *Mapping Properties* dialog.
8. Click Close to return to the main window.

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.

To review or edit the properties of a directory service or LDIF file:

1. Right-click the directory service or LDIF file name in the Sources pane.
2. Select Properties from the context menu.
3. Review or edit the properties.
4. 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 CaliberRM 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.

To review the properties for a group or user:

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

Tip If you decide that the properties are mapped incorrectly, you can change the mappings for the directory service or LDIF file. See "Reviewing Borland User Properties" on page 14 for more information.

If you find that the properties contain the wrong values, you must make corrections from the directory service. To do this, you may have to re-export an LDIF file.

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*.

Chapter

3

Using the Targets Pane

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

Adding a CaliberRM Server

If a CaliberRM Server is to receive user information from a directory service or LDIF file, it must be represented in the Targets pane of the main window.

To add a CaliberRM Server:

1 Do one of the following:

- Click the CaliberRM Servers toolbar button.
- Select Configure > CaliberRM Servers from the menu bar.
- Press *Ctrl+R*.

The *CaliberRM Servers* dialog opens.

2 Click Add. The *CaliberRM Server Properties* dialog opens.

3 Enter a name for this server in the Name text box.

4 Enter a host name or IP address in the Host text box.

5 Click OK. A CaliberRM Server object appears in the Targets pane.

Tip From the *CaliberRM Servers* dialog, you can edit the CaliberRM 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 from the context menu.

Adding a StarTeam Server

If a StarTeam Server is to receive user information from a directory service or LDIF file, it must be represented in the Targets pane of the main window.

To add a StarTeam Server:

1. Do one of the following:
   - Click the StarTeam Servers toolbar button.
   - Select Configure > StarTeam Servers from the menu bar.
   - Press *Ctrl+S*. The *StarTeam Servers* dialog opens.
2. Click Add.

   The *StarTeam Server Properties* dialog opens.
3. Enter a name for this server in the Name text box.
4. Enter a host name or IP address in the Host text box.
5. Click OK. A StarTeam Server object appears in the Targets pane.

Note The Directory Service Validation node provides connection status information. If you review the properties for a StarTeam Server, you will see information about the connection. For example, if the server is not running, LDAP QuickStart Manager displays the message: “Cannot connect to server.”

Tip From the *StarTeam Servers* dialog, you can edit this StarTeam 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 from the context menu.

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/CaliberRM Groups toolbar button.
- Select View > Display Groups from the menu bar.
- Press *Ctrl+G*.
- Right-click Borland 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 from the menu bar.
- Press *Alt+N*.
- Right-click Borland Servers (the first node in the Targets pane). Then select Sort > By Name from the context menu.

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

- Select View > Sort > By User ID from the menu bar.

- Press *Alt+I*.
- Right-click Borland Servers (the first node in the Targets pane). Then select Sort > By User ID from the context menu.

Suspending Users

You can suspend users from the CaliberRM and StarTeam Servers. A suspended user cannot log on to StarTeam or CaliberRM. You cannot delete users (or groups) through LDAP QuickStart Manager.

To suspend a user:

1. Right-click the user to be suspended.
2. Select Suspend from the context menu.
3. Click Yes to confirm the suspension.

NOTE: When you suspend a CaliberRM user in LDAP QuickStart Manager, CaliberRM shows the user as “Account Disabled” function.

Reviewing Properties

You can review properties for a specific CaliberRM Server, StarTeam Server, group, or user. There is a properties dialog for every node in the Targets pane except for the root node for the pane (named Borland Servers) and the parent nodes for CaliberRM and StarTeam Servers (named CaliberRM Servers and StarTeam Servers, respectively).

CaliberRM and StarTeam Server Properties

The properties for a CaliberRM Server or a StarTeam Server are the same properties that you see when you create a CaliberRM Server or StarTeam Server object. Once you have displayed the properties, you can also edit them.

When you create a StarTeam Server, you are not connected to it. After LDAP QuickStart Manager connects to the server, you see connection information in the dialog. The properties on this page of the dialog are not editable.

To review or edit the properties for a server:

1. Right-click the server’s name in the Targets pane.
2. Select Properties from the context menu.
3. Review or edit the properties.
4. Click OK or Cancel.

Group and User Properties

The properties dialog for a group or an individual user show the values related to that user or group.

To review the properties for a group or user:

1. Right-click the group or user’s name in the Sources pane.
2. Select Properties from the context menu.
3. Review the properties.
4. Click OK.

CaliberRM User and Group Properties

CaliberRM initially displays the General properties of a group (that is, the name of the group and its description) on the *Group Properties* dialog. To see the members in the CaliberRM group, click Members in the left pane of the dialog. On this screen you can also add new members to the group or remove existing members.

The General properties of a CaliberRM user (name and other identifying information) initially display on the *User Properties* dialog.

To see the groups to which a CaliberRM user belongs, click Group Membership in the left pane. The next dialog shows you these groups. and allows you to add the user to other groups or remove the user from existing groups.

By clicking Password in the left pane, you can set password standards for a specific CaliberRM user or disable a user account. The available options are:

- User must change password at next logon
- User cannot change password
- Password never expires (the default)
- Account disabled

StarTeam User and Group Properties

As noted earlier, the StarTeam group and user properties dialogs in LDAP QuickStart Manager are similar to those used for CaliberRM. The *StarTeam Group Properties* dialog has only a General node, which shows the name and description for the group.

The *StarTeam User Properties* dialog has General, Logon, and Group Membership pages, which resemble those found in StarTeam.

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 CaliberRM/StarTeam Servers toolbar button.
- Select View > Refresh > Refresh Targets from the menu bar.
- Press *Alt+2*.
- Right-click the Targets pane's root node (named Borland Servers) and select Refresh from the context menu.

Tips

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 CaliberRM or StarTeam Server's database.

Refreshing both panes, of course, also refreshes the Targets pane. See "Refreshing Data in the Sources Pane" on page 17 for details about refreshing both panes simultaneously.

Chapter

4

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 graphical user interface

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

1 Do one of the following:

   - Select Import > Users from the menu bar.
   - Press *Ctrl+I*.

   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.

Tip 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 CaliberRM settings. These settings will be used during your import

operation unless you change them before the import starts. For information on changing these settings, see “Configuring Default Import Options” on page 28.

- 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 CaliberRM 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.

Tip 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. Do one of the following:
   - Click the Import Wizard toolbar button.
   - Press *Ctrl+W*.
   - Select Import > Users from the menu bar. From the resulting *Import Users* dialog, select the “With the wizard” option button, and click OK.

   The *Import Wizard: Selecting Sources* dialog 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.
2. Select specific users, groups of users, or the entire directory service or LDIF file.
3. Click Next.

   The *Import Wizard: Selecting Target Destinations* dialog displays the CaliberRM and StarTeam 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 CaliberRM 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.

5 Click Next. The *Import Wizard: Setting Options* dialog opens.

6 Use the *Import Wizard: Setting Options* dialog to control what exactly happens to the imported data.

a 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.

b 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.

c 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. For more details, see "Creating and Using Templates" on page 27.

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

d If you have elected to create a template, enter a name for this template in the Template Name text box.

e Click Advanced to set up advanced options for users.

The *Advanced Options* dialog opens.

1 To add StarTeam password authentication and licensing for any users that will be added to StarTeam as part of the import operation:

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 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.

Important Before StarTeam Servers can request directory service validation of user paswords, you must enable directory service support in the StarTeam Administration tool. Set the Directory Service options on the Configure Server dialog to enable directory service support and supply the connection information to a directory service such as Active Directory.

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.)

- 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.

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

2. 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.

a. 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.

b. If you selected the License server option button, you must enter a slip ID number in the Slip ID text box.

1. To add CaliberRM password authentication and licensing for any users that will be added to CaliberRM as part of the import operation:

a. Select CaliberRM.

   The *Advanced Options* dialog changes.

b. Specify whether you want to apply the validation to all CaliberRM users. When Apply validation to all users is unchecked, the validation setting only applies to new CaliberRM users.

c. Do one of the following:

- Indicate whether new users will have their passwords authenticated by CaliberRM Server or by a directory service by selecting either the Validate password through directory service or the Validate password through CaliberRM Server option button.
- If you select password validation through the CaliberRM 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.

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

  2. 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 CaliberRM Server.

d. Select the Not Authorized, CaliberRM Concurrent, CaliberRM 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 CaliberRM Named and CaliberRM Concurrent licenses with License Server licenses. Even though License Server licenses can be either named user on concurrent licenses, they come with slip IDs.

e. If you selected the License Server option button, you must enter a slip ID number in the Slip ID text box.

2. Click OK.

a. Click Next.

   The *Import Wizard: Summary* dialog summarizes your choices so that you can review them.

1. Do one of the following:

- Click Finish to start the import operation.
- Click Previous one or more times to edit your selections for the import operation.

Creating and Using 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 New 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" on page 24.
- Click the Templates toolbar button. From the resulting *Templates* dialog, click Add. This displays the wizard. Then follow the directions in "Using the Wizard" on page 24.
- Press *Ctrl+T*. From the resulting *Templates* dialog, click Add. This action displays the wizard. Then follow the directions in "Using the Wizard" on page 24.

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 menu bar. From the resulting *Import Users* dialog, select the "With a Template" option button, select the template name from the drop-down list box, and click OK.

Performing Other Template Operations

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

To review the summary for a template:

1 Do one of the following:

- Click the Templates toolbar button.
- Press *Ctrl+T*.

The *Templates* dialog opens.

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.

To delete a template:

1 Do one of the following:

- Click the Templates toolbar button.
- Press *Ctrl+T*.

The *Templates* dialog opens.

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 Quick Start 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 From the menu, select Configure > Default Import Options. This action displays the *Default Import Options* dialog., which has three nodes, General, StarTeam, and CaliberRM.

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 Select 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 Server.

   c If you select password validation through the StarTeam Server, 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 CaliberRM node.

   a Specify whether you want to apply the validation to all CaliberRM 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 CaliberRM Server.

   c If you select password validation through the CaliberRM 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, CaliberRM Concurrent, CaliberRM 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 CaliberRM Named and CaliberRM 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 Server groups are also hierarchical, but, in CaliberRM Server, no group is a subgroup of another.

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

When you import a hierarchy of groups into CaliberRM 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 CaliberRM Server: 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 CaliberRM 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:

- Right-click anywhere in the pane.
- Do one of the following:
  - Click Hide Info to stop displaying the Messages pane.
  - Click Clear to empty the Messages pane.
  - Click Save Log to store the messages in a text file.

Index

O

P

R

S

T

U

V