LDAPCONF Utility

User's Guide

Software Release 11.6
January 2016

Two-Second Advantage®

Important Information

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This document contains confidential information that is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of TIBCO Software Inc.

TIBCO, Two-Second Advantage, TIBCO ActiveMatrix BusinessWorks, TIBCO Business Studio, TIBCO Enterprise Message Service, TIBCO Hawk, TIBCO iProcess, TIBCO iProcess Suite, and TIBCO Rendezvous are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

Enterprise Java Beans (EJB), Java Platform Enterprise Edition (Java EE), Java 2 Platform Enterprise Edition (J2EE), and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle Corporation in the U.S. and other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. SEE THE README FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

Copyright © 1994-2016 TIBCO Software Inc. All rights reserved.

TIBCO Software Inc. Confidential Information

Contents

Preface

This guide describes how to use the LDAPCONF utility. This utility allows you to use an LDAP directory service with the TIBCO iProcess Engine to manage iProcess user, group, role and attribute data.

Topics

Related Documentation

This section lists documentation resources you may find useful.

TIBCO iProcess Engine Documentation

The following documents form the TIBCO iProcess Engine documentation set:

- *TIBCO iProcess Engine Installation* Read this manual for instructions on site preparation and installation.
- *TIBCO iProcess Engine Release Notes* Read the release notes for a list of new and changed features. This document also contains lists of known issues and closed issues for this release.
- TIBCO iProcess Suite Documentation This documentation set contains all the manuals for TIBCO iProcess Engine and other TIBCO products in TIBCO iProcess® Suite. The manuals for TIBCO iProcess Engine are as follows:
  - *TIBCO iProcess Engine Architecture Guide*
  - TIBCO iProcess Engine Administrator's Guides:
    TIBCO iProcess Engine Administrator's Guide
    TIBCO iProcess Objects Director Administrator's Guide
    TIBCO iProcess Objects Server Administrator's Guide
  - TIBCO iProcess Engine Database Administrator's Guides:
    TIBCO iProcess Engine (DB2) Administrator's Guide
    TIBCO iProcess Engine (Oracle) Administrator's Guide
    TIBCO iProcess Engine (SQL) Administrator's Guide
  - *TIBCO iProcess swutil and swbatch Reference Guide*
  - *TIBCO iProcess Engine System Messages Guide*
  - *TIBCO iProcess User Validation API User's Guide*
  - *LDAPCONF Utility User's Guide*

Other TIBCO Product Documentation

You may find it useful to read the documentation for the following TIBCO products:

- TIBCO ActiveMatrix BusinessWorks™

- TIBCO Business Studio™
- TIBCO Enterprise Message Service™
- TIBCO Hawk®
- TIBCO Rendezvous®

Typographical Conventions

TIBCO iProcess Engine can be run on both Microsoft Windows and UNIX/Linux platforms. In this manual, the Windows convention of a backslash (\) is used. The equivalent pathname on a UNIX or Linux system is the same, but using the forward slash (/) as a separator character.

UNIX or Linux pathnames are occasionally shown explicitly, using forward slashes as separators, where a UNIX or Linux-specific example or syntax is required.

Any references to UNIX in this manual also apply to Linux unless explicitly stated otherwise.

The following typographical conventions are used in this manual

Table 1 General Typographical Conventions

Convention	Use
SWDIR	TIBCO iProcess Engine installs into a directory. This directory is referenced in documentation as *SWDIR*. The value of *SWDIR* depends on the operating system. For example, • on a Windows server (on the `C:` drive) if *SWDIR* is set to `C:\swerver\staffw_nod1`, then the full path to the `swutil` command is `C:\swerver\staffw_nod1\bin\swutil`. • on a UNIX or Linux server:en if *SWDIR* is set to `/swerver/staffw_nod1`, then the full path to the `swutil` command is `/swerver/staffw_nod1/bin/swutil` or *$SWDIR*`/bin/swutil`. Note: On a UNIX or Linux system, the environment variable $*SWDIR* should be set up to point to the iProcess system directory for the **`root`** and **`swadmin`** users.
`code font`	Code font identifies commands, code examples, filenames, pathnames, and output displayed in a command window. For example: Use `MyCommand` to start the foo process.

Table 1 General Typographical Conventions (Cont'd)

Convention	Use
`bold code font`	Bold code font is used in the following ways: • In procedures, to indicate what a user types. For example: Type **`admin`**. • In large code samples, to indicate the parts of the sample that are of particular interest. • In command syntax, to indicate the default parameter for a command. For example, if no parameter is specified, `MyCommand` is enabled: `MyCommand [`**`enable`**` | disable]`
italic font	Italic font is used in the following ways: • To indicate a document title. For example: See *TIBCO ActiveMatrix BusinessWorks Concepts*. • To introduce new terms For example: A portal page may contain several portlets. *Portlets* are mini-applications that run in a portal. • To indicate a variable in a command or code syntax that you must replace. For example: `MyCommand` *PathName*
Key combinations	Key name separated by a plus sign indicate keys pressed simultaneously. For example: Ctrl+C. Key names separated by a comma and space indicate keys pressed one after the other. For example: Esc, Ctrl+Q.
	The note icon indicates information that is of special interest or importance, for example, an additional action required only in certain circumstances.
	The tip icon indicates an idea that could be useful, for example, a way to apply the information provided in the current section to achieve a specific result.
	The warning icon indicates the potential for a damaging situation, for example, data loss or corruption if certain steps are taken or not taken.

Table 2 Syntax Typographical Conventions

Convention	Use
`[ ]`	An optional item in a command or code syntax. For example: `MyCommand [optional_parameter] required_parameter`

Table 2 Syntax Typographical Conventions

Convention	Use
`|`	A logical OR that separates multiple items of which only one may be chosen. For example, you can select only one of the following parameters: `MyCommand para1 | param2 | param3`

`{ }`	A logical group of items in a command. Other syntax notations may appear within each logical group.
	For example, the following command requires two parameters, which can be either the pair `param1` and `param2`, or the pair `param3` and `param4`.
	`MyCommand {param1 param2} | {param3 param4}`
	In the next example, the command requires two parameters. The first parameter can be either `param1` or `param2` and the second can be either `param3` or `param4`:
	`MyCommand {param1 | param2} {param3 | param4}`
	In the next example, the command can accept either two or three parameters. The first parameter must be `param1`. You can optionally include `param2` as the second parameter. And the last parameter is either `param3` or `param4`.
	`MyCommand param1 [param2] {param3 | param4}`

Connecting with TIBCO Resources

How to Join TIBCOmmunity

TIBCOmmunity is an online destination for TIBCO customers, partners, and resident experts. It is a place to share and access the collective experience of the TIBCO community. TIBCOmmunity offers forums, blogs, and access to a variety of resources. To register, go to http://www.tibcommunity.com.

How to Access TIBCO Documentation

You can access TIBCO documentation here:

https://docs.tibco.com

How to Contact TIBCO Support

For comments or problems with this manual or the software it addresses, contact TIBCO Support as follows:

- For an overview of TIBCO Support, and information about getting started with TIBCO Support, visit this site:

  http://www.tibco.com/services/support

- If you already have a valid maintenance or support contract, visit this site:

  https://support.tibco.com

  Entry to this site requires a user name and password. If you do not have a user name, you can request one.

Chapter 1 Overview

This chapter provides an overview of how you use an LDAP directory service with the iProcess Engine to manage iProcess user, group, role and attribute data.

Topics

Using the iProcess Engine With an LDAP Directory Service

You can manage iProcess user, group, role and attribute data through any LDAP-compliant directory service, such as X.500, Microsoft Active Directory, Open LDAP or Oracle Internet Directory. For detailed information about the supported LDAP versions, see *TIBCO iProcess Engine Installation*.

Why Use LDAP?

Managing user information is a complex problem for modern organizations, often involving the management of separate and incompatible user directories; each of which has to be updated every time an employee joins, leaves, changes department or personal details and so on.

LDAP offers a solution to this problem by providing:

- a distributed, global directory.
- fast, efficient, client/server-based access to the directory.
- integrated user validation.

How Does iProcess Work With LDAP?

iProcess **user data** (that is - user, group, role and attribute data) is maintained as part of the LDAP directory. For each LDAP directory entry that represents an iProcess user, **LDAP directory attributes** are mapped to corresponding **iProcess properties**. iProcess Engine can use these entries in the LDAP directory as possible iProcess users, rather than creating operating system accounts for each registered iProcess user. This information is kept as part of the iProcess database.

Note that in previous versions of the LDAPCONF utility, this information was kept in a file, *SWDIR***util****swldap**.

You can also optionally use LDAP to provide integral user validation; that is, LDAP passwords can be used to validate users.

You must run the LDAPCONF utility after upgrading the iProcess Engine to any new release, to ensure that user information is up to date in the database. See Upgrading iProcess on page 34.

Whenever the iProcess Engine performs a MoveSysInfo operation, it sends a **synchronization** request to the iProcess **BG** process to obtain iProcess user data from the LDAP directory. The synchronization request:

1. searches the LDAP directory for entries that may contain iProcess user data.
2. downloads those entries to the iProcess Engine, where the entries' attributes are processed and converted into their corresponding iProcess properties.

Differences from Normal iProcess Operation

Using the iProcess Engine with an LDAP directory differs from normal iProcess operation in three areas:

- **User administration**. iProcess user data must be created and maintained in the LDAP directory using LDAP directory administration tools. When the iProcess Engine is running against the LDAP directory, you cannot add, modify or delete iProcess users, groups, roles or attributes using *SWDIR***bin****swutil** or the TIBCO iProcess Administrator.

You can still use the TIBCO iProcess Administrator to view user information.

- **LDAPCONF**. LDAPCONF is a utility which allows you to manage the interface between the LDAP server and the iProcess Engine. See The LDAPCONF Utility on page 6 for more information.
- **MoveSysInfo**. When you perform a MoveSysInfo operation, it synchronizes the iProcess Engine's current user data with the contents of the LDAP directory. See Automating Synchronization on page 45 for more information.

How to Set Up the iProcess Engine to Work With an LDAP Directory

Setting up the iProcess Engine to work with an LDAP directory requires knowledge of both iProcess user administration and LDAP server administration. TIBCO recommend that you work with your local LDAP server administrator on the following procedures.

By default the iProcess Engine is configured to use normal iProcess user data and administration tools. To use iProcess with an LDAP directory you must:

1. Modify the LDAP directory to include iProcess data:
   a. Decide which LDAP directory attributes to map to which iProcess properties.
   b. Create or modify the necessary entries in the LDAP directory. Each iProcess user, group or role requires an entry in the LDAP directory.

   See Creating and Maintaining iProcess User Data in the LDAP Directory on page 11 for more information.
2. Use LDAPCONF to set up the interface between the LDAP server and the iProcess Engine:
   a. Set up the connection parameters.
   b. Set up the search parameters, which define the point in the LDAP directory from which to start searching for iProcess user data, and any filters to apply to that search.
   c. Set up the mapping between LDAP directory attributes and iProcess properties.

   See Configuring the Interface to the LDAP Server on page 25 for more information.
3. Test the interface to prove that the connection is working and that the correct information is being downloaded.

   See Testing the LDAP Interface on page 35 for more information.
4. Synchronize the iProcess Engine's user data with the contents of the LDAP directory.

   See Synchronizing iProcess User Data with the LDAP directory on page 44 for more information.
5. If you wish to use LDAP for user validation, switch the iProcess Engine over to use it by setting the LDAP_UV attribute.

See Configuring iProcess to use LDAP User Validation on page 46 for more information.

The LDAPCONF Utility

LDAPCONF is a utility which allows you to manage the connection between the LDAP server and the iProcess Engine. You use it to:

- establish and test the connection between the LDAP server and the iProcess Engine.
- test that the correct information is being downloaded.
- define which LDAP directory attributes are mapped to which iProcess properties.
- turn the use of the LDAP directory on or off for data synchronization.
- optionally, to specify the information needed for integral user validation to work, such as the hostname, port number, the attribute mapping, and search base and search criteria. This information is maintained in the iProcess database.
- synchronize the iProcess Engine's user data with the LDAP directory.

LDAPCONF acts as an LDAP client program.

Using LDAPCONF

To use LDAPCONF:

- the iProcess Engine must be running if there is a requirement to synchronize the user data. Otherwise, the iProcess Engine does not need to be running.

You can either use LDAPCONF interactively from a menu, or issue LDAPCONF commands directly from a command line.

LDAPCONF Menu

To start LDAPCONF for interactive use, run the following:

- if you are using Windows, run *SWDIR***util****ldapconf.exe**
- if you are using UNIX, run *SWDIR***util****ldapconf**

The LDAPCONF menu is displayed, as shown below.

```
=====================================================================
TIBCO iProcess LDAP Connection Administration Utility
Copyright (c) 2001-2013 TIBCO Software Inc.
=====================================================================

[1]   Set Connection Information
[2]   Set Search Parameters
[3]   Set Attribute Mappings
[4]   Group Membership in MEMBER LIST format
[5]   View Connection Information
[6]   Test Connection
[7]   Return to LDAP DIT
[8]   Save
[9]   Synchronise
[10]  Enable Attribute Value Translation from UTF-8
[11]  Quit

Please enter your selection:
```

Type in the number of the option you wish to select and press ENTER:

- Depending on the option you choose, information or prompts for further input are displayed.
- If a prompt has a default option available, it is shown in brackets at the end of the prompt. For example:

```
Enter the LDAP attribute for the iProcess Username (cn):
```

To accept the default option for a prompt, simply press ENTER.

The following table summarizes the available options:

Option		Description
1.	Set Connection Information	Set up the connection between the LDAP server and the iProcess Engine. See Setting up the Connection on page 27.
2.	Set Search Parameters	Define where to start searching the LDAP directory for iProcess users, and any filter criteria to use in the search. See Defining Search Criteria on page 30.
3.	Set Attribute Mappings	Define which LDAP directory attributes will be mapped to which iProcess properties. See Mapping LDAP Directory Attributes to iProcess Properties on page 31.
4.	Group Membership in MEMBER LIST / LDAP DN format	Define whether LDAPCONF should read the value of an LDAP <GROUPUSERS> directory attribute as a list of iProcess user names, or as a list of LDAP Distinguished Names (DN). See Defining Group Membership on page 18.
5.	View Connection Information	View the current connection information, search parameters and attribute mappings. See Viewing Configuration Settings on page 36.
6.	Test Connection	Test the connection to the LDAP server, the search parameters and attribute mappings. See Testing the Interface on page 37
7.	Return to LDAP DIT	Configure the iProcess Engine to obtain its user data either from its own database or from the LDAP directory. See Synchronizing iProcess User Data with the LDAP directory on page 44.
8.	Save	Save the current connection information, search parameters, attribute mappings and LDAP_DIT flag setting to the iProcess database. If the encrypted file *SWDIR***util****swldap** (used by previous versions of the LDAPCONF utility) exists, it is deleted. You must run this command when upgrading your iProcess Engine from a version prior to version 11.0. See Upgrading iProcess on page 34. **Note: This option is not available from the command line.**

Option		Description
9.	Synchronize	Synchronize the iProcess Engine's user data with the contents of the LDAP directory. See Configuring iProcess to Obtain User Data from the LDAP Directory on page 42. **Note: Make sure that the iProcess Engine is configured to obtain user data from the LDAP directory before using this option. It has no effect otherwise.**
10.	Enable/Disable Attribute Value Translation from UTF-8	Defines whether attribute values are translated from UTF-8 format to the iProcess Engine's locale when they are downloaded from the LDAP server. See Setting up the Connection on page 27. **Note: This option is intended for use with LDAP servers that store directory information internally in UTF-8 format.**
11.	Quit	Quit from LDAPCONF and return to the command prompt.

LDAPCONF Commands

LDAPCONF Commands on page 47 describes the commands which you can issue directly to LDAPCONF from the command line.

Chapter 2 Creating and Maintaining iProcess User Data in the LDAP Directory

This chapter explains how to create and maintain iProcess user data in the LDAP directory.

Topics

LDAP Directory Entries and Attributes

iProcess users, groups and roles are stored as **entries** in the LDAP directory. Each entry has a number of **attributes** which provide the information about the entry that is used by the iProcess Engine. There are two types of attributes:

- attributes that map to iProcess properties. The following section discusses these attributes.
- attributes that map to application specific data. See page 17 for more information about these.

Attributes That Map to iProcess Properties

LDAP directory attributes are mapped to iProcess properties to provide the necessary information about iProcess users in the LDAP directory. Mapping LDAP Directory Attributes to iProcess Properties on page 31 explains how to use LDAPCONF to set up these mappings.

Note that:

- LDAP directory attributes that are mapped to iProcess properties are indicated in this guide by the use of angled brackets. For example, <MENUNAME> indicates the LDAP directory attribute that is mapped to the iProcess MENUNAME property. (By default, this is the LDAP **menuname** attribute, but it can be any other LDAP attribute - for example, **groupname**.)
- An LDAP directory attribute that is mapped to an iProcess property must have a name that is no longer than 15 characters. Longer names will be truncated when the entries are downloaded to the iProcess Engine, which means that the mapping will be treated as invalid.
- An LDAP directory attribute does not allow the attribute to contain an underscore. An attribute with an underscore in iProcess Engine is mapped to an attribute without an underscore in LDAP. For example, the `SW_WISINST` attribute in iProcess Engine is mapped to the `SWWISINST` attribute in LDAP.

The following table describes the mappings between LDAP directory attributes and iProcess properties.

LDAP Directory Attribute Name	Default Attribute Value	iProcess Property Mapping (Sheet 1 of 4)
<MENUNAME>	menuname	Maps to the iProcess MENUNAME attribute. This mapping defines whether the entry represents an iProcess user, group or role. **This attribute must be specified! If this attribute is not specified the entry is not added to iProcess (or is deleted if it already exists) when it is synchronized with the LDAP directory** (see Synchronizing iProcess User Data with the LDAP directory on page 44). It can take the following values: • **USER** - The entry is an iProcess user with a MENUNAME of USER. • **MANAGER** - The entry is an iProcess user with a MENUNAME of MANAGER. • **PRODEF** - The entry is an iProcess user with a MENUNAME of PRODEF. • **ADMIN** - The entry is an iProcess user with a MENUNAME of ADMIN. • **GROUP** - The entry is an iProcess group. • **ROLE** - The entry is an iProcess role. • **NONE** - The entry is not an iProcess user, group or role. (If the entry already exists in iProcess, it will be removed the next time synchronization takes place.) For example: menuname=PRODEF menuname=GROUP

LDAP Directory Attribute Name	Default Attribute Value	iProcess Property Mapping (Sheet 2 of 4)
<USERNAME>	sn	Maps to the iProcess user name. **Note: Remember that a valid iProcess user name must be 24 characters or less; if the LDAP directory attribute chosen has a value longer than 24 characters, the corresponding iProcess username is truncated to 24 characters (though usernames may also be constrained by the underlying operating system).** For example: uid=johnf
<GROUPNAME>	groupname	Maps to the iProcess group name. For example: swgroup=purchas
<ROLENAME>	rolename	Maps to the iProcess role name. For example: swrole=chfpurch
<DESCRIPTION>	description	Maps to the iProcess DESCRIPTION attribute (for a user or group). For example: description=John Ford description=Purchasing Group
<LANGUAGE>	language	Maps to the iProcess LANGUAGE attribute (for a user or group). For example: lang=ENGLISH
<SORTMAIL>	sortmail	Maps to the iProcess SORTMAIL attribute (which defines how iProcess work items should be sorted for a user or group). For example: sort=PROCEDURE

LDAP Directory Attribute Name	Default Attribute Value	iProcess Property Mapping (Sheet 3 of 4)
<GROUPUSERS>	groupusers	Defines the iProcess users who are members of the group defined by this entry. See Defining Group Membership on page 18 for more information about how to define values for this attribute.
<ROLEUSERS>	roleuser	Defines the iProcess user who is assigned to the role defined by this entry. For example: assignto=johnf
<QSUPERVISORS>	Optional	Specifies the iProcess users who are allowed to supervise the queue defined by this entry. For example: supervisors=johnb, swadmin If no value is specified for an entry, the default entry is that no supervisors are allowed to supervise the queue. If an incorrect value is specified (i.e. a user who is not a valid iProcess user), an error is reported in the TIBCO iProcess Administrator when the mappings are imported into iProcess.

LDAP Directory Attribute Name	Default Attribute Value	iProcess Property Mapping (Sheet 4 of 4)
<USERFLAGS>	Optional	Specifies what work items the user is allowed to forward in Work Queue Manager. It can take the following values: • **null** - Step Forward. The user is allowed to forward a work item only if the step's **Forward** permission has been set by the procedure definer. • **r** - Forward None. The user is not allowed to forward any work item, even if the step's **Forward** permission has been set by the procedure definer. • **f**- Forward Any. The user is allowed to forward any work item, even if the step's **Forward** permission has not been set by the procedure definer. For example: forwardperms=f If one of the listed values is not specified the entry defaults to NULL.

Application Specific Attributes

You can also define application specific attributes for use in the iProcess Suite. For example, you may want to make users' email addresses or telephone numbers available to iProcess procedures.

Do not use the *_XX* string to name attributes where *XX* is a 2-digit number. This string is reserved for TIBCO iProcess Engine internal use.

Mapping LDAP Directory Attributes to iProcess Properties on page 31 explains how to use LDAPCONF to make application specific attributes available to iProcess.

Managing User Information

All changes to iProcess user data must be made in the LDAP directory. Use your normal LDAP directory management tools to perform the following operations.

When the iProcess Engine is configured to use the LDAP directory you cannot create, modify or delete users, groups, roles or attributes using the iProcess Suite's user administration tools (*SWDIR*`\bin\swutil and User Manager`). You can still view user data using User Manager.

Adding a User to the LDAP Directory

To add an iProcess user to the LDAP directory, create or modify a directory entry as follows:

1. Assign one of the following values to the <MENUNAME> attribute: **USER**, **MANAGER**, **PRODEF** or **ADMIN**.
2. Assign a name for this iProcess user to the <USERNAME> attribute.
3. Define any other mappings for iProcess properties or application-specific data that you require.

Adding a Group to the LDAP Directory

To add an iProcess group to the LDAP directory, create or modify a directory entry as follows:

1. Assign the value **GROUP** to the <MENUNAME> attribute.
2. Assign a name for this iProcess group to the <GROUPNAME> attribute.
3. Specify the group's membership, using the <GROUPUSERS> attribute. See Defining Group Membership below for more information about how to do this.
4. Define any other mappings for iProcess properties or application-specific data that you require.

Defining Group Membership

You can use the <GROUPUSERS> attribute to define iProcess group membership in a number of ways:

- An entry can contain one or more <GROUPUSERS> values. If multiple <GROUPUSERS> values are used, LDAPCONF includes the usernames from each entry in the group.
- All <GROUPUSERS> attribute values must be specified *either:*
  - — as iProcess user names. See page 16 for more information.

    or
  - — as LDAP Distinguished Names (DN) that reference other entries in the LDAP directory, that in turn contain iProcess user names. See page 20 for more information.
- You must configure LDAPCONF to read <GROUPUSERS> attribute values as either iProcess user names (MEMBER LIST format) or as LDAP DNs (LDAP DN format). You cannot combine both methods. See page 33 for more information about how to do this.

Using iProcess User Names to Define Group Membership (MEMBER LIST Format)

A <GROUPUSERS> attribute value can be *either* a single iProcess user name, *or* a comma-separated list of iProcess user names. In the following example, the **groupusers** attribute value defines **johnb**, **roystonh** and **bobb** as members of the **reviewers** group:

```
menuname=group
groupname=reviewers
groupusers=johnb,roystonh,bobb
```

Note that:

- Each specified user name must already exist as an iProcess user. (When iProcess user data is synchronized with the LDAP directory, a user that does not already exist will simply not be added to the group.)
- A specified name must not contain an **@** or **=** character, as this will cause the value to be truncated. For example, the value:

```
groupusers = johnb,roystonh@acme,bobb
```

will result in **johnb** and **roystonh** being added as group members. **bobb** will not be added to the group.

- You can use wildcard characters to match all or part of a user name. For example, the following value defines all users whose name starts with **swusr** as group members:

```
groupusers = swusr*
```

Using LDAP Distinguished Names to Define Group Membership (LDAP DN Format)

A <GROUPUSERS> attribute value can contain *either* a single DN, *or* a list of DNs. Each DN references another entry in the LDAP directory, that must contain the iProcess user name that is to be added to the group.

When iProcess user data is synchronized with the LDAP directory, LDAPCONF reads the LDAP entry defined by each DN. If it finds:

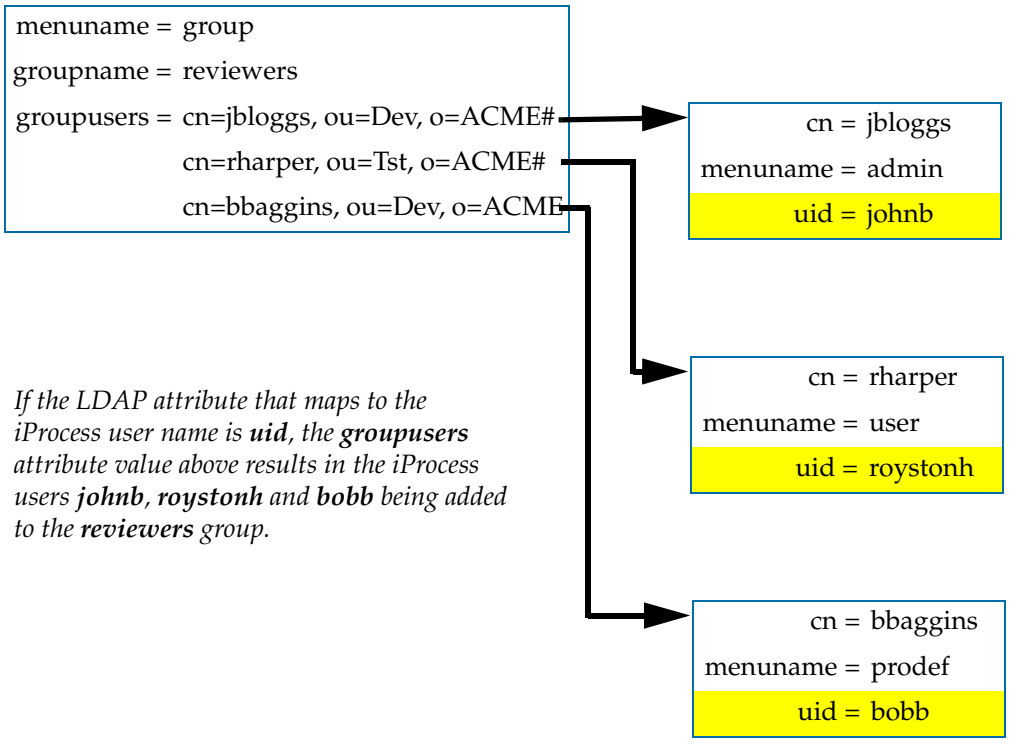
- a <USERNAME> attribute value that maps to an existing iProcess user, it adds that user to the group.
- a <USERNAME> attribute value that is not already an iProcess user, it creates the iProcess user, and then adds it to the group.

The value must be a valid iProcess user name.

- no <USERNAME> attribute value, or an empty <USERNAME> attribute value, it ignores the entry.

In the example on the next page, the **groupusers** attribute value contains a list of three DNs. The LDAP attribute that maps to the iProcess user name is **uid**. When iProcess user data is synchronized with the LDAP directory, LDAPCONF searches the LDAP entry defined by each DN for a **uid** value. Users **johnb**, **roystonh** and **bobb** are therefore added to the **reviewers** group.

In this example, the # character is the delimiter for individual DNs in the **groupusers** value. The # character is the MS Active Server delimiter; other LDAP Directory servers may use different characters.



*If the LDAP attribute that maps to the iProcess user name is **uid**, the **groupusers** attribute value above results in the iProcess users **johnb**, **roystonh** and **bobb** being added to the **reviewers** group.*

Note that:

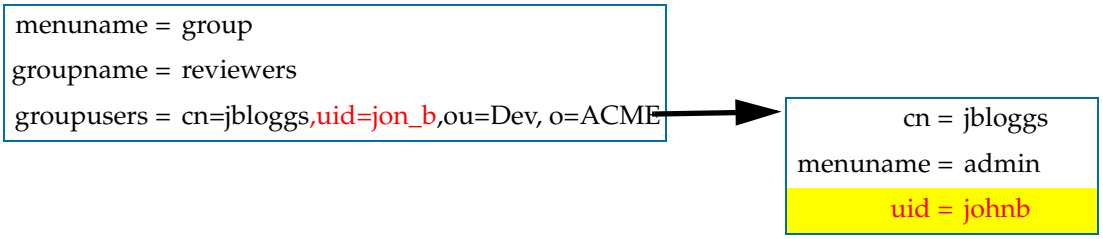
- A DN must not contain an @ character, as this will cause the DN to be truncated. For example, the value:

```
groupusers = cn=jbloggs,ou=Dev,o=ACME#
             cn=rharper@ACME,ou=Tst,o=ACME#
             cn=bbaggins,ou=Dev,o=ACME
```

will result in the second DN being interpreted as **cn=rharper**. The first and third DNs will be interpreted normally.

- If a DN contains the LDAP <USERNAME> attribute, LDAPCONF checks if the value of that attribute is an iProcess user:
  - — If it is, LDAPCONF adds that user to the group and does not interpret the DN any further.
  - — If it is not, LDAPCONF continues to interpret the DN as previously described.

In the following example, we again assume that **uid** is the LDAP attribute that maps to the iProcess user name.



LDAPCONF reads the DN and, finding that it already contains a **uid** value, checks if **jon_b** is an iProcess user:

— If **jon_b** is an iProcess user, **jon_b** is added to the **groupusers** group. The entry pointed to by the full DN is not examined.

— If **jon_b** is not an iProcess user, LDAPCONF searches the entry pointed to by the full DN. It finds the **uid** value **johnb**, and so adds user **johnb** to the **groupusers** group.

Adding a Role to the LDAP Directory

To add an iProcess role to the LDAP directory, create or modify a directory entry as follows:

1. Assign the value **ROLE** to the <MENUNAME> attribute.
2. Assign a name for this iProcess role to the <ROLENAME> attribute.
3. Specify the user assigned to the role, using the <ROLEUSER> attribute.
4. Define any other mappings for iProcess properties or application-specific data that you require.

Deleting a User, Group or Role

You can delete an iProcess user, group or role from the LDAP directory in three ways:

- Set the <MENUNAME> attribute for the relevant entry to **NONE**. The user, group or role will be removed when iProcess is next synchronized with the LDAP directory.

- Delete the <MENUNAME> attribute for the relevant entry. The user, group or role will be removed when iProcess is next synchronized with the LDAP directory.
- Delete the relevant entry. The user, group or role will be removed when iProcess is next **fully** synchronized with the LDAP directory.

If an entry is deleted from the LDAP directory a partial synchronization will not remove the user, group or role from the iProcess database. See Automating Synchronization on page 45 for more information.

Changing the Membership of a Group

Each entry defining a group should have one or more <GROUPUSERS> values, which define the members of that group. To change the membership of the group, add users to or remove them from this list. See Defining Group Membership on page 18 for more information.

Changing a Role Assignment

Each entry defining a role should have a <ROLEUSER> attribute, which specifies the <USERNAME> assigned to that role. To change this assignment, edit this value.

Creating, Deleting or Editing Attributes

You can create, delete or edit any attributes for use with the iProcess Engine as required. See Application Specific Attributes on page 17.

Chapter 3 Configuring the Interface to the LDAP Server

This chapter explains how to use LDAPCONF to configure the interface between the LDAP server and the iProcess Engine. See The LDAPCONF Utility on page 6 for general information about how to use LDAPCONF.

Topics

Overview

Configuring the interface between the LDAP server and the iProcess Engine involves:

1. Setting up the basic connection between the LDAP server and the iProcess Engine.
2. Defining the point in the LDAP directory at which to start searching for entries that contain iProcess data, and any filter criteria to use in the search.
3. Defining the mappings between LDAP directory attributes and iProcess properties.

The following sections explain these steps in more detail.

Setting up the Connection

To set up the connection to the LDAP server:

1. Select the following option from the LDAPCONF menu:

```
[1] Set Connection Information
```

   The following prompt is displayed:

```
Enter name of host on which the LDAP server resides (localhost):
```

2. Enter the name of the machine where the LDAP server is running, either as a host name specified in your local machine's hosts file, or as an IP address. The LDAP server supports Internet Protocol version 6 (IPv6), you can input an IPv6 host name or an IPv6 address under the prompt.

   The network and machines that host LDAP servers must support IPv6.

   The following prompt is displayed:

```
Enter port number on host to connect to (389):
```

3. Enter the TCP port number (a valid numeric value greater than 1) to connect to on the specified *host*. The default value for LDAP servers is **389**.

   The following prompt is displayed:

```
Enter the distinguished name of the entry to bind as (NULL):
```

4. Enter the distinguished name (DN) of the entry which will be used to authenticate this connection to the LDAP server. (If you accept the default option LDAPCONF will connect as a default LDAP user.)

   The following prompt is displayed:

```
Do you wish to change the password (Y/N):
```

5. Enter:
   - **Y**, if you want to change the password associated with this entry. You will then be prompted to enter and confirm the new password.
   - **N**, if you want to use the existing password.

   If you are using UNIX, the following prompt is displayed:

```
SSL is enabled, do you wish to disable it (Y/N):
```

   or

```
SSL is disabled, do you wish to enable it (Y/N):
```

6. Enter:
   - **Y**, if you want to change the status of SSL.
   - **N**, if you want to keep the current status of SSL.

   If you enable SSL, the following prompt is displayed:

```
PATH to the Certificate Database for SSL(/home/certs/):
```

   Enter the path to the SSL Certificate Database.

7. If you are using UNIX and have enabled SSL, or if you are using Windows, the following prompt is displayed:

```
Is the target LDAP provider Microsoft Active Directory [No] (Y/N):
```

   This is necessary because Microsoft Active Directory handles password changes differently from other LDAP providers.

   Enter:
   - **Y**, if the LDAP server to which you are connecting uses Microsoft Active Directory.
   - **N**, if the LDAP server does not use Microsoft Active Directory. This is the default value.

   The LDAPCONF menu is re-displayed.

8. If the LDAP server you are connecting to stores directory information internally in UTF-8 format, select the following option from the LDAPCONF menu:

```
[10] Enable Attribute Value Translation from UTF-8
```

This ensures that any attribute information that uses characters from multi-byte character sets (such as Chinese, Japanese and Korean) is downloaded correctly to the iProcess Engine.

If you subsequently need to reconfigure the iProcess Engine *not* to translate downloaded attribute values from UTF-8, you can do so by selecting the same option from the LDAPCONF menu:

```
[10] Disable Attribute Value Translation
```

The LDAPCONF menu is re-displayed.

Remember to Save these settings if you want to use them in a future LDAPCONF session.

Defining Search Criteria

To define the point in the LDAP directory that a synchronization request should start searching for iProcess user data:

1. Select the following option from the LDAPCONF menu:

```
[2] Set Search Parameters
```

   The following prompt is displayed:

```
Enter the search start DN (o=base):
```

   Enter the distinguished name (DN) of the LDAP directory entry from which to start searching for iProcess data.

2. The following prompt is displayed:

```
Enter the search filter (cn=*):
```

   Enter the filter criteria to be used to widen or refine the search. By default the search will find any entries that have a **cn** attribute.

3. The following prompt is displayed:

```
Enter the pattern to construct DN from the user id:
```

   Enter a C/C++ style pattern to construct the DN string from the user ID. For example, if your DN is:

   `uid=michael,dc=people,dc=company,dc=com`

   for the ID **michael**, you should enter:

   uid=%s,dc=people,dc=company,dc=com

   You can nullify this field by entering **NULL**. If so, then iProcess Engine will use the DN and password specified in option [1] Set Connection Information to connect to the server and search a DN for **uid=michael**.

   The LDAPCONF menu is re-displayed.

Remember to Save these settings if you want to use them in a future LDAPCONF session.

Mapping LDAP Directory Attributes to iProcess Properties

See LDAP Directory Entries and Attributes on page 12 for more information about how iProcess properties are mapped to LDAP directory attributes.

To define the mappings of LDAP directory attributes to iProcess properties:

1. Select the following option from the LDAPCONF menu:

```
[3] Set Attribute Mappings
```

2. You are prompted, in turn, to enter the name of the LDAP directory attributes that map to the following iProcess properties:

Prompt for iProcess....	Default Mapping	Description
Username	sn	Enter the name of the LDAP directory attribute that maps to the iProcess user name.
Groupname	groupname	Enter the name of the LDAP directory attribute that maps to the iProcess group name.
Rolename	rolename	Enter the name of the LDAP directory attribute that maps to the iProcess role name.
Description	description	Enter the name of the LDAP directory attribute that maps to the iProcess DESCRIPTION attribute
Language	language	Enter the name of the LDAP directory attribute that maps to the iProcess LANGUAGE attribute.
Menu Name	menuname	Enter the name of the LDAP directory attribute that maps to the iProcess MENUNAME attribute. **Note: This attribute is used to determine whether an LDAP directory entry found as a result of a search is an iProcess user, group or role.**
Sortmail	sortmail	Enter the name of the LDAP directory attribute that maps to the iProcess SORTMAIL attribute.
iProcess Group User	groupusers	Enter the name of the LDAP directory attribute that contains the members of a group.

Prompt for iProcess....	Default Mapping	Description
iProcess Role User	roleuser	Enter the name of the LDAP directory attribute that contains the name of the iProcess user who is assigned to a role.
Qsupervisors	qsupervisors	Enter the name of the LDAP directory attribute that maps to the iProcess QSUPERVISORS attribute.
Userflags	userflags	Enter the name of the LDAP directory attribute that maps to the iProcess USERFLAGS attribute.

These mappings must be unique. A warning message is displayed if you try to map an LDAP directory attribute to an iProcess property if you have already mapped that LDAP directory attribute.

The following prompt is displayed:

```
Please Enter option (L)ist/(C)hange/(D)elete/(A)dd/(Q)uit
```

3. This allows you to select additional LDAP directory attributes to be used in the iProcess Suite. Select:
   - — **List** to display the list of additional LDAP directory attributes currently in use. (The first time you select this option the previously saved list is displayed.)
   - — **Change** to replace an LDAP directory attribute in the list with a new one.
   - — **Delete** to delete an LDAP directory attribute from the list.
   - — **Add** to add an LDAP directory attribute to the list.
4. Select **Quit** when the list matches your requirements.

Remember to Save these settings if you want to use them in a future LDAPCONF session.

Here is an example of the **Set Attribute Mappings** option.

```
Enter the LDAP attribute for the iProcess Username (sn): username
Enter the LDAP attribute for the iProcess GroupName (groupname):
Enter the LDAP attribute for the iProcess Rolename (rolename):
Enter the LDAP attribute for the Description (description):
Enter the LDAP attribute for the Language (language):
Enter the LDAP attribute for the Menu Name (menuname):
Enter the LDAP attribute for the Sortmail (sortmail):
```

```
Enter the LDAP attribute for the iProcess Group User (groupusers):
ugroup
Enter the LDAP attribute for the iProcess Role User (roleuser):
urole
Enter the LDAP attribute for the Qsupervisors (qsupervisors):
Enter the LDAP attribute for the Userflags (groupflags):
Please Enter option (L)ist/(C)hange/(D)elete/(A)dd/(Q)uit : A
Value to add : email
Please Enter option (L)ist/(C)hange/(D)elete/(A)dd/(Q)uit : A
Value to add : telephone
Please Enter option (L)ist/(C)hange/(D)elete/(A)dd/(Q)uit : L
email telephone
Please Enter option (L)ist/(C)hange/(D)elete/(A)dd/(Q)uit : Q
```

5. If you want LDAPCONF to read the value of an LDAP <GROUPUSERS> directory attribute as a list of iProcess user names, not as a list of LDAP Distinguished Names (DN), select the following option from the LDAPCONF main menu:

```
[4] Group Membership in MEMBER LIST format
```

If you subsequently want to change this option, so that LDAPCONF reads <GROUPUSERS> directory attribute values as LDAP DNs, select option [4] again from the LDAPCONF menu:

```
[4] Group Membership in LDAP DN format
```

See Defining Group Membership on page 18 for more information about how to define <GROUPUSERS> attribute values.

Upgrading iProcess

If you upgrade your iProcess Engine installation from a previous version to Version 11.0 or later, the LDAP information needs to be transferred from the file *SWDIR***util****swldap**, where it was kept in previous versions of the LDAPCONF utility, to the iProcess database.

To do this, after you have completed upgrading the iProcess Engine:

1. Start the LDAPCONF menu. See LDAPCONF Menu on page 7.
2. Select the following option from the LDAPCONF menu:

```
[8] Save
```

   The LDAPCONF utility then reads the existing configuration information from the *SWDIR***util****swldap** file, saves it to the database, and deletes the file. See Save on page 8.

3. Select the following option from the LDAPCONF menu:

```
[5] View Connection Information
```

4. The current settings are displayed, as shown in Viewing Configuration Settings on page 36. Check that the information is correct, as described in Verifying the Data on page 38.
5. If it is, select **[8] Save** again.

Chapter 4 Testing the LDAP Interface

Having configured the LDAP interface, you can view your settings and test the interface. This allows you to establish:

- that the connection is working.
- whether or not your search settings and mappings will extract the appropriate information from the LDAP directory.

You are strongly advised to test the interface in this way **before** configuring the iProcess Engine to use the LDAP directory.

Topics

Viewing Configuration Settings

To view your current configuration settings, select the following option from the LDAPCONF menu:

```
[5] View Connection Information
```

The current connection settings, search settings and mappings are displayed. For example:

```
DIT                 = iProcess
GRP USERS FORMAT    = LDAP DN

CONNECTION :-
     hostname       = node1
     portno         = 329
     credentials    = cn=admin,o=aco,c=gb
     password       = *******

SEARCH :-
     base           = o=aco,c=gb
     filter         = cn=*

ATTRIBUTE MAPPINGS :-
     username       = sn
     Groupname      = groupname
     Rolename       = rolename
     description    = description
     language       = language
     menuname       = menuname
     sortmail       = sortmail
     groupusers     = groupusers
     roleuser       = roleuser
     Qsupervisors   = qsupervisors
     Userflags      = userflags

     extra [1]      = email
     extra [2]      = telephone
```

Testing the Interface

To test the connection to the LDAP server and the data from the LDAP directory:

1. Select the following option from the LDAPCONF menu:

```
[6] Test Connection
```

2. The iProcess Engine tests the connection and displays whether the connection attempt succeeded or failed. For example:

```
Testing connection...
Connect successful.
```

   If the attempt fails, information about the possible cause of the failure is shown. For example, the following error indicates a problem with the DN entry used to authenticate the connection. You should check the validity of the supplied name (and password).

```
Testing connection...
SW_LDAP_connect() failed : Error whilst binding to connection
(-1230)
Press [ENTER] to continue...
```

3. If the connection attempt succeeds, the following prompt is displayed:

```
Do you wish to download user information from LDAP (Y/N):
```

   — If you enter **N**, the LDAPCONF menu is re-displayed.

   — If you enter **Y**, LDAPCONF searches the LDAP directory using the current search root and filter criteria and displays the number of matching entries found. For example:

```
Number of entries found : 10
```

4. You are then prompted whether to output the results of the search:
   a. in iProcess format (**S**) or LDAP directory format (**L**). See *Verifying the Data on page 38*.

```
iProcess Mapping/LDAP (S/L): s
```

   b. to the screen (**S**) or to a text file (**F**).

```
Output to File or Screen (F/S): s
```

The search results are displayed or written to the requested file.

Verifying the Data

You should use the information downloaded from the LDAP directory to verify your configuration settings, as follows:

1. Examine the information downloaded in LDAP directory format (**L**) to check whether your search criteria are finding the appropriate entries in the LDAP directory. (See Defining Search Criteria on page 30.)
2. Compare the information downloaded in iProcess format (**S**) and LDAP directory format (**L**) to check whether your defined mappings are converting the LDAP directory user data into the appropriate iProcess data. (See Mapping LDAP Directory Attributes to iProcess Properties on page 31.)

The following example shows an entry displayed in LDAP directory (**L**) format:

```
objectclass     mhs-user
cn              Andy Jones
sn              Jones
iProcess        PRODEF
description     Senior Consultant
telephone       +44 1234 123456
email           AJones@acompany.com
```

The following example shows the same entry displayed in iProcess (**S**) format:

```
NAME            Jones
DESCRIPTION     Senior Consultant
LANGUAGE        english
MENUNAME        PRODEF
SORTMAIL        PROCEDURE
GROUPUSERS
ROLEUSER
```

In the above examples:

- the **iProcess** LDAP directory attribute is mapped to the iProcess MENUNAME attribute.
- LDAP directory attributes which are not mapped to iProcess attributes (such as **telephone**) are not shown in iProcess format.

Note that:

- If an entry displayed in LDAP directory format either has no <MENUNAME> attribute, or has a <MENUNAME> attribute with a value of NONE, it will not be displayed in iProcess format, as it does not represent an iProcess user, group or role.
- If the <GROUPUSERS> entry is longer than 24 characters, the output displayed for this entry in iProcess format is truncated to 24 characters. This only affects the output from the Test Connection option; not the data for the entry itself.

Chapter 5 Using the LDAP Directory

When you have verified that the LDAP interface is operating correctly and that the correct information is being downloaded from the LDAP directory (as described in Chapter 4), you can start using the LDAP directory.

Topics

Configuring iProcess to Obtain User Data from the LDAP Directory

To configure iProcess to obtain user data from the LDAP directory, select the following option from the LDAPCONF menu:

```
[7] Return to LDAP DIT
```

Once iProcess has been configured to obtain user data from the LDAP directory:

- a MoveSysInfo operation will synchronize the iProcess Engine's user data with the contents of the LDAP directory.
- you should request a synchronization immediately. See Synchronizing iProcess User Data with the LDAP directory on page 44 for more information.
- you cannot create, modify and delete user information using *SWDIR***bin****swutil** or the TIBCO iProcess Administrator.

If you subsequently need to reconfigure iProcess *not* to use user data from the LDAP directory for any reason (for example, if the LDAP server is not available for an extended period of time), you can do so by selecting the same option from the LDAPCONF menu:

```
[7] Return to iProcess DIT
```

If you select this option:

- the iProcess Engine will obtain its user information from its own database. All user information downloaded from the LDAP directory is retained.
- You can create, modify and delete user information using *SWDIR***bin****swutil** or the TIBCO iProcess Administrator.
- You can still use iProcess Engine's integral LDAP User Validation feature.

The LDAP_DIT Flag

Selecting the **Return to LDAP|iProcess DIT** option from the LDAPCONF menu toggles the value of the **LDAP_DIT** configuration flag in the *SWDIR***etc****staffcfg** file. This flag determines whether or not iProcess uses the LDAP directory to obtain its user information. If LDAP_DIT is set to:

- **1**, the LDAP directory is used.
- **0**, the LDAP directory is not used. (This is the default option).

This flag was previously called the **X500_DIT** flag. If your SWDIR**etc****staffcfg** file still contains an **X500_DIT** flag, it will be recognized and treated as the **LDAP_DIT** flag.

Synchronizing iProcess User Data with the LDAP directory

To synchronize iProcess user data with the LDAP directory:

1. Select the following option from the LDAPCONF Main menu:

```
[9] Synchronise
```

2. If you have not already saved them, you are prompted to save any configuration changes you have made.
3. The following prompt is then displayed:

```
Perform Full or Partial Synchronisation or Quit (F/P/Q):
```

Enter:

— **F** to perform a full synchronization. This downloads all entries from the LDAP directory which are found by the current search criteria.

— **P** to perform a partial synchronization. This downloads only those entries which are found by the current search criteria *and* which have changed since the last synchronization was performed. (Every entry in the LDAP directory is timestamped with both its creation and modification time.)

On a partial synchronization, entries which have been deleted since the last synchronization are not found by this search, and so are not deleted from iProcess. If iProcess users are removed by setting their <MENUNAME> attribute to NONE, rather than by deleting their LDAP directory entry, they will be deleted from iProcess.

On a partial synchronization, if the LDAP server and the iProcess Engine are hosted on different computers, you must ensure that the GMT times on each computer are the same. If they are not, incorrect data may be down-loaded when a partial synchronization is performed.

This results from the implementation of CR 13245. The synchronization operation now compares the timestamp of the last synchronization (which is recorded from the iProcess Engine's current time, in GMT format) to the LDAP DIT entry's modification timestamp on the LDAP server (in GMT format).

— **Q** to return to the LDAPCONF menu without downloading any user data from the LDAP directory.

Automating Synchronization

When the iProcess Engine is configured to use the LDAP directory, synchronization with the LDAP directory automatically occurs whenever a MoveSysInfo operation is performed as a result of an LDAPCONF request (which records the time that it last performed a synchronization).

You can automate the synchronization process to perform regular, scheduled updates of user information by using the LDAPCONF MOVESYSINFO command (See MOVESYSINFO on page 54), using the Windows **at** command or a UNIX/Linux **cron** job.

TIBCO recommends the use of a 'two-tiered' update strategy:

- Perform partial synchronizations on a short timescale (for example, every hour or every day, depending on the frequency with which user information changes).
- Perform full synchronizations on a longer timescale (for example, every day or every week).

Configuring iProcess to use LDAP User Validation

You can switch the iProcess Engine over to use the LDAP integral user validation API by using the following **swadm** command:

*SWDIR***util\swadm set_attribute 0 ALL 0 LDAP_UV 1**

You can turn this feature off by deleting the attribute, or setting its value to **0**.

See "Administering Process Attributes" in the *TIBCO iProcess™ Engine Administrator's Guide* for more information on setting process attributes.

Setting up the Proxy User

If you are using iProcess Engine on a UNIX or Linux system, and you use UNIXRUN or UNIXEXEC script commands, you can define a proxy operating system user to perform the commands. If this value is missing, no proxy OS user is defined and the iProcess Engine service user will be used.

A configurable proxy OS user is provided in line 16 of the file *SWDIR***/etc/staffpms**. See the section "Specifying a Proxy User" in the *TIBCO iProcess Engine Administrator's Guide* for further details.

Appendix A LDAPCONF Commands

This appendix describes the *SWDIR***util****ldapconf* commands which you can issue directly to LDAPCONF from the command line.

Topics

CONNECT

Set up the connection between the LDAP server and iProcess Engine. See Setting up the Connection on page 27 for more information.

Syntax

```
ldapconf CONNECT [-h hostname] [-port number] [-dn name]
[-pwd password]
```

where:

- *hostname* is the name of the machine where the LDAP server resides.
- *number* is the TCP port number to connect to on *hostname*. This must be a valid numeric value greater than 1. The default value is **389**, used for all LDAP servers.
- *name* is a distinguished name (DN) entry that will be used to authenticate the connection to the LDAP server.
- *password* is the password associated with *name*.

Example

The following example connects to the LDAP server on machine **scotty** using port **341**, using the distinguished name **cn=user1** with a password of **1a7pass9** to authenticate the connection.

```
LDAPCONF CONNECT -h scotty -port 341 -dn cn=user1 -pwd 1a7pass9
```

SEARCH

Set up the search base and filter criteria to use when searching the LDAP directory for entries to download to the iProcess Engine. See Defining Search Criteria on page 30 for more information.

Syntax

```
ldapconf SEARCH [-dn name] [-s filter]
```

where:

- *name* is a distinguished name (DN) entry which defines the starting point for the search in the LDAP directory.
- *filter* is the filter criteria to be used to refine or widen the search.

Example

The following example defines a search which begins at the organization entry **aco** in the country **gb**, searching for all entries with a Common Name attribute (cn) beginning with the letter **s**.

```
LDAPCONF SEARCH -dn “o=aco,c=gb” -s “cn=s*”
```

ATTRIB

Set up the mapping of LDAP directory attributes to iProcess properties when LDAP directory entries are downloaded to the iProcess Engine. See Mapping LDAP Directory Attributes to iProcess Properties on page 31 for more information.

Syntax

```
ldapconf ATTRIB [-u username] [-r roleuser] [-g groupusers]
-menu menuname [-desc description] [-lang language] [-sort sortmail]
[-x new_attr]
```

where:

- *username* is the LDAP directory attribute which maps to the iProcess username.
- *roleuser* is the LDAP directory attribute to be used to assign an iProcess user to a role.
- *groupusers* is the LDAP directory attribute to be used to contain the list of users who are members of a group.
- *menuname* is the LDAP directory attribute which maps to the iProcess MENUNAME attribute. This attribute identifies whether an LDAP directory entry is treated by the iProcess Engine as a user, group or role, or is ignored.
- *description* is the LDAP directory attribute which maps to the iProcess DESCRIPTION attribute.
- *language* is the LDAP directory attribute which maps to the iProcess LANGUAGE attribute.
- *sortmail* is the LDAP directory attribute which maps to the iProcess SORTMAIL attribute
- *new_attr* is an additional LDAP directory attribute to be used in the iProcess system. (This option should be repeated for each additional attribute that is required; any attributes that are already in use but which are not specified are cleared.)

Specifying the -x option without any parameters means that no additional LDAP directory attributes are to be used in iProcess; any that are already in use are cleared.

Example The following example sets up the attribute mappings between the LDAP directory and iProcess. It also defines two additional LDAP directory attributes, **email** and **telephone**, for use in iProcess.

```
LDAPCONF ATTRIB -user username -r urole -g ugroup -menu menuname -desc description
-lang language -sort sortmail -x email -x telephone
```

VIEW

View the current connection settings, search settings and attribute mappings. See Viewing Configuration Settings on page 36 for more information.

Syntax

```
ldapconf VIEW
```

Example

```
LDAPCONF VIEW

DIT                  = LDAP
GRP USERS FORMAT     = LDAP DN

CONNECTION :-
     hostname        = node1
     portno          = 329
     credentials     = cn=admin,o=aco,c=gb
     password        = *******
SEARCH :-
     base            = o=aco,c=gb
     filter          = cn=*

ATTRIBUTE MAPPINGS :-
     username        = sn
     Groupname       = groupname
     Rolename        = rolename
     description     = description
     language        = language
     menuname        = menuname
     sortmail        = sortmail
     groupusers      = groupusers
     roleuser        = roleuser
     Qsupervisors    = qsupervisors
     Userflags       = userflags

     extra [1]       = email
     extra [2]       = telephone
```

TEST

Test the current connection with the current search settings and attribute mappings. See Testing the Interface on page 37 for more information.

Syntax

```
ldapconf TEST [-f filename] [-s|l]
```

where:

- *filename* is the name of the file to send the output of the command to. If omitted, information is output to the screen.
- -**s** indicates that user, group, role and attribute information should be downloaded from the LDAP directory and displayed in iProcess format; -**l** indicates that it should be downloaded and displayed in LDAP format.

Example

The following example tests the connection and downloads user information from the LDAP directory, displaying it on the screen in iProcess format:

```
LDAPCONF TEST -s
Testing connection...
Connect successful.
Number of entries found : 1
     NAME            Jones
     DESCRIPTION     Senior Consultant
     LANGUAGE        english
     MENUNAME        PRODEF
     SORTMAIL        PROCEDURE
     GROUPUSERS
     ROLEUSER
     QSUPERVISORS
     USERFLAGS
     GROUPNAME
```

MOVESYSINFO

Performs partial or full synchronization of the iProcess user directory with the LDAP directory. See Synchronizing iProcess User Data with the LDAP directory on page 44 for more information.

The iProcess Engine must be set to operate in LDAP mode for this command to have any effect.

Syntax

```
ldapconf MOVESYSINFO -full|partial
```

where:

- **-full** requests the iProcess Engine to do a MoveSysInfo to perform a full synchronization with the LDAP directory.
- **-partial** requests the iProcess Engine to do a MoveSysInfo to perform a partial synchronization with the LDAP directory.

Example

The following example performs a full synchronization of the iProcess user directory with the LDAP directory.

```
LDAPCONF MOVESYSINFO -full
```