IdentityForge

Advanced Adapter Guide for IBM-i5

July 2013

Primary Author: Anna Hix

Contributing Authors: Martin Lightheart

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Identity Forge license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software—Restricted Rights (June 1987). Identity Forge , LLC. ., 5885 Cumming Hwy. Suite 108-350, Atlanta GA 30518.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

The Programs may provide links to Web sites and access to content, products, and services from third parties. IdF is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. IdF is not responsible for:
(a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. IdF is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface

This guide describes the procedure to deploy the IdF IBM-i5 Series Advanced Adapter.

Audience

This guide is intended for resource administrators and target system integration teams.

Related Documents

For more information, refer to the following documents in the IdF documentation library:

- IdF LDAP Gateway Release Notes
- IdF Advanced Adapter for i5 Series Release Notes
- IdF Glossary of Terms

Documentation Updates

IdF is committed to delivering the best and most recent information available.
For information about updates to IdF Advanced Adapter for i5 Series please visit:
http://www.identityforge.net/support

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	**Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.**
italic	*Italic type indicates book titles, emphasis, definition or placeholder variables for which you supply particular values.*
`monospace`	`Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.`

What's New in the Advanced Adapter for IBM-i5 Series?

This chapter provides an overview of the updates made to the software and documentation for the IdF Advanced Adapter for IBM-i5 Series.

See Also:

The earlier release of this guide for information about updates those were new for that release.

The updates discussed in this chapter are divided into the following categories:

- Software Updates

  This section describes updates made to the adapter software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

  See Also: IdF LDAP Gateway Release Notes

Software Updates

The following software updates have been made in this release of the adapter:

1. Java SDK 1.6 and above is now a requirement.
2. See i5 Series Release Notes for all new features, enhancements and bug fixes

Documentation-Specific Updates

The following is a documentation-specific update in this release of the guide:

1 About the Adapter

The IdF Advanced Adapter for IBM-iSeries (formerly AS400) provides a native interface between iSeries and any LDAPv3 supported product. The adapter functions as a trusted virtual administrator on the target system, performing tasks such as creating login IDs, suspending IDs, and changing passwords. In addition, it automates some of the functions that administrators usually perform manually.

The adapter enables provisioning and reconciliation with the IBM-i5 Series security facilities.

This chapter discusses the following topics:

- Certified Deployment Configurations
- Adapter Overview
- Features of the Adapter
- Roadmap for Deploying and Using the Adapter

Certified Deployment Configurations

Table 1-1 Certified Deployment Configurations

Item	Requirement
Target System Identity Repository	IBM-iSeries Versions supported include: • IBM i5/OS v5.4 up to 7.1 Note: The end-of-support date has passed for some of these i5/OS versions. Check with your IBM support contacts for more details.

Item	Requirement
Infrastructure Requirements: Message transport layer	JTOpen API
I5/OS Admin Account	Authorized account with privileges

Message Transport Layer Requirements

Between the LDAPv3 server and i5/OS uses JTOpen API.

Review Link Below for JTOpen Standard Ports for COMMAND CALL
http://www-03.ibm.com/systems/i/software/toolbox/faqports.html

Overview of the Adapter

The IBM-i5 Series Advanced Adapter includes the following components:

- LDAP Gateway: The LDAP Gateway is built on Java Technology and allows portability across various platforms and operating systems. The LDAP Gateway receives LDAPv3 protocol commands from distributed applications and translates them to native mainframe commands. After the commands are run, LDAPv3-formatted responses are returned to the requesting application.

- Voyager Reconciliation Agent: The IBM-i5 Series Advanced adapter provides the reconciliation functionality through the Voyager Reconciliation Agent. The Voyager Agent captures native i5/OS events by using exit technology. Exits are programs that are run after a system event in the OS are processed. The Voyager Agent captures in real time events occurring from logins, the command prompt, batch jobs, and other native events. The Voyager Agent stores these events into an encrypted file for use later from an LDAPv3 protocol query messages through the LDAP Gateway.

Note:

At some places in this guide, the Voyager Reconciliation Agent is referred to as the Reconciliation or Voyager Agent.

This component is only used with the Enterprise Edition of the software.

- **Message Transport Layer:** The message transport layer enables the exchange of messages between the LDAP Gateway and the Voyager Agent and Pioneer Agent. You can use any one of the following messaging protocols for the message transport layer:
    - TCP/IP with AES encryption is used for Agent File Change Events: This uses 1024-bit cryptographic keys. We provide our own internal Security Key Manager that generates 3 different key for encryption.
    - JTOpen API is used for all other commands and auth.
        - JTOpen API provides a password algorithm ensuring no password is every in clear text, including Non-SSL mode. *The IBM Toolbox never transmits or stores passwords in the clear (not even on the call stack).*

The architecture of the adapter can be explained in terms of the adapter operations it supports:

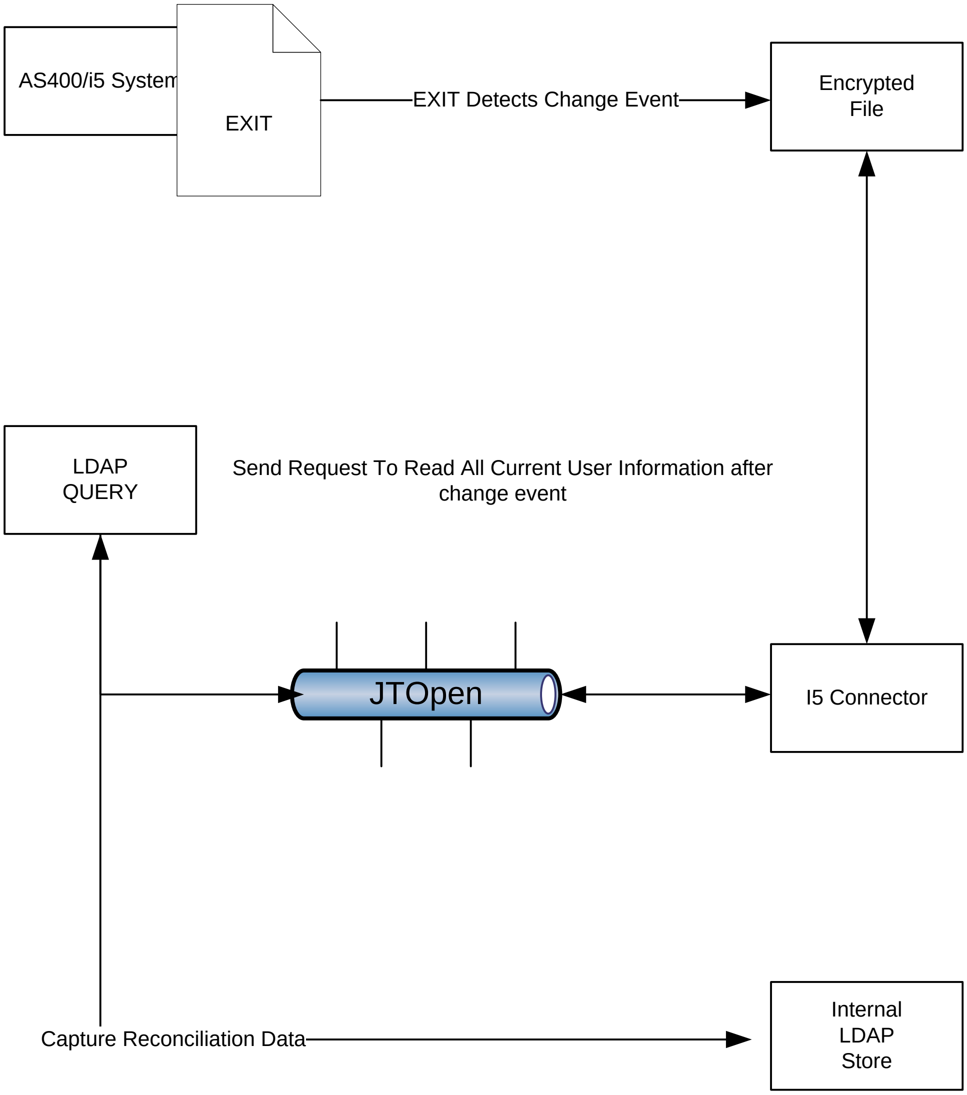
- **Reconciliation**
- **Provisioning**

See Also:

Appendix B, "Adapter Architecture" for more information about the adapter architecture and configuration of the message transport layer

Reconciliation

Figure 1-1 shows the flow of data during reconciliation.


AS400/i5 System
EXIT
EXIT Detects Change Event
Encrypted File
LDAP QUERY
Send Request To Read All Current User Information after change event
JTOpen
I5 Connector
Capture Reconciliation Data
Internal LDAP Store

Reconciliation involves the following steps: [Enterprise Edition Only]

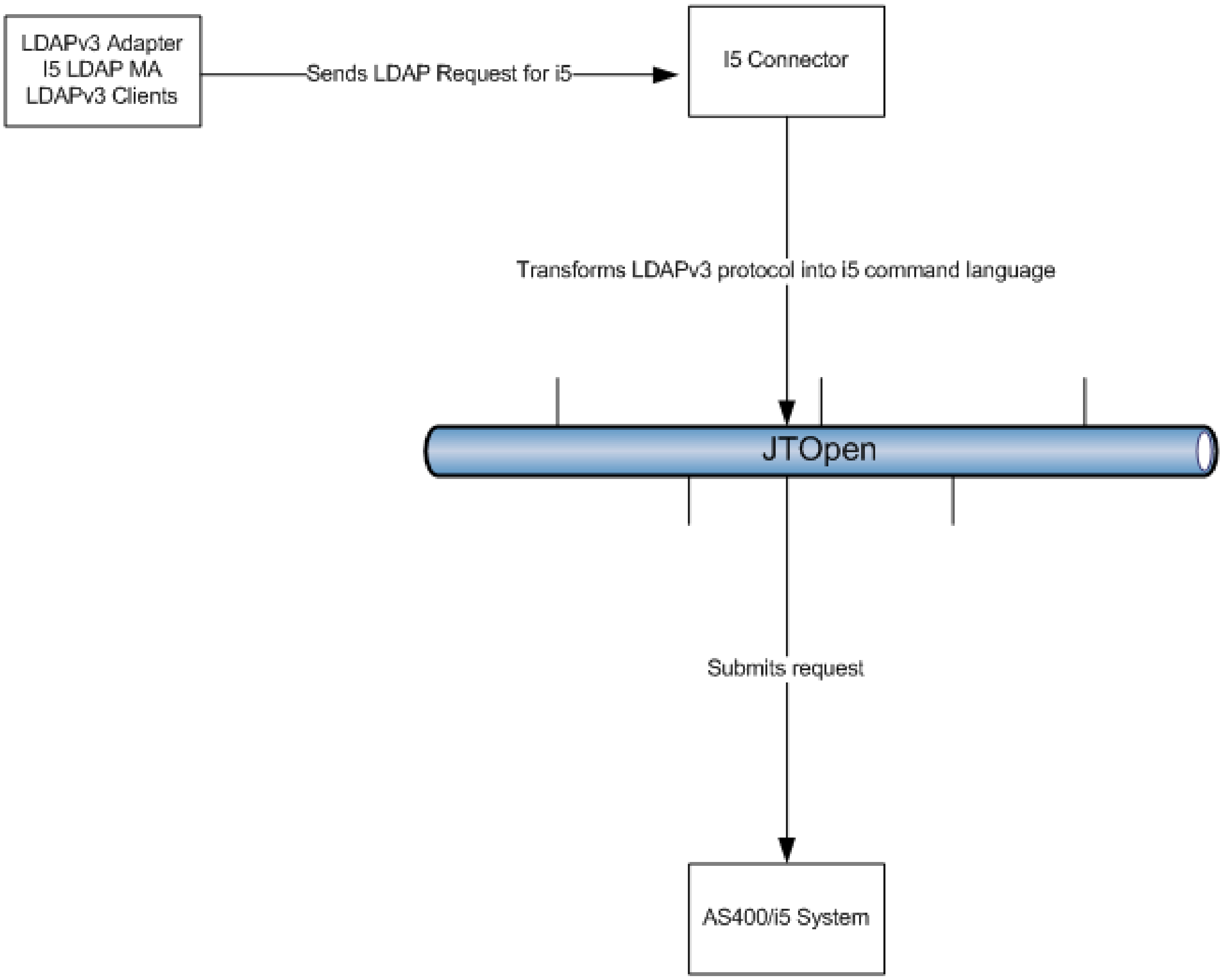
1. I5/OS identity and authorization events take place in the i5 target system. The i5/OS events are processed through appropriate exits.

Note: *Identity and authorization events in consist of capturing logon, running of a command, real-time password synchronization, creation or deletion of a user, or a change in the user attributes.*

2. The events are stored in an encrypted file
3. The LDAP Gateway queries the file from the Voyager Agent events
4. Data is sent to IDM system and/or stored in the Internal Meta Store of the LDAP.

Provisioning

Figure 1-1 shows the flow of data during Provisioning.



Provisioning involves the following steps:

1. A user is created, updated, or deleted and an LDAPv3 request is sent to the LDAP Gateway IBM-i5 Series Connector.

2. The LDAP Gateway translates the change request from the LDAP Gateway to i5/AS400 commands. The IBM-i5 Series Advanced adapter uses JTOpen API to send request to i5/AS400.

3. The adapter also updates the internal meta-store of the LDAP Gateway with the changes in user data. [Enterprise Version Only]

4. On the target system, the command is executed data, which is validated against the target system repository, and returns success or error messages back to the LDAP Gateway. When a success message is returned to the LDAP Gateway, the data is provisioned.

Features of the Adapter

This section discusses the following topics:

- Functionality Supported by the Pioneer Provisioning Agent
- Functionality Supported for Provisioning
- Functionality Supported by the Voyager Reconciliation Agent
- Functionality Supported for Reconciliation
- Target System Attributes Used for Reconciliation and Provisioning
- Adapter Architecture

Functionality Supported by the Pioneer Provisioning Agent

The Pioneer Provisioning Agent supports the following functions:

- Standard IBM-i5/OS user profile commands:
  - [`CRTUSRPRF`]: Creates a IBM-i5 user profile
  - [`CHGUSRPRF`]: Modifies a IBM-i5 user profile
  - [`DLTUSRPRF`]: Deletes a IBM-i5 user profile
- Standard IBM-i5/OS searching [DSPUSRPRF]
  - Search All IBM-i5 Users
  - Search by Change Date all IBM-i5 Users
  - Display IBM-i5 User Attribute Information
- Custom IBM-i5/OS Command Processing
  - Configurable Custom Commands
- Real-Time EXIT Capture
  - Change/Delta Based Query of all changed IBM-i5 Users

Functionality Supported for Provisioning

The functions supported by the Pioneer Agent are described in the following table:

Function	Description
Authenticate Users	Validates users LoginId and Password
Create Users	Adds new users IBM-i5.
Modify Users	Modifies user information in IBM-i5.
Change Passwords	Changes user passwords on IBM-i5 in response self-service change password.
Reset Passwords	Resets user passwords IBM-i5. The passwords are reset by the administrator.
Disable User Accounts	Disables users in IBM-i5.
Enable User Accounts	Enables users in IBM-i5.
Delete Users	Removes users from IBM-i5.
Add Users to Files	Add to IBM-i5 Files
Remove Users from Files	Remove from IBM-i5 Files
Search All Users	Retrieves all users and data from IBM-i5
Custom Command	Process custom commands

Functionality Supported by the Voyager Reconciliation Agent

The Voyager Reconciliation Agent supports reconciliation of changes that are made to user profiles by using commands such as CHGUSERPRF. These commands also contain users' passwords for reconciliation, if needed.

Functionality Supported for Reconciliation

The Voyager Agent supports the following functions:

- Change passwords
- Password resets
- Create user data
- Modify user data
- Disable users
- Delete users
- Enable users
- Audit information

Target System Attributes Used for Reconciliation and Provisioning

The following attributes are reconciled between IBM-i5 and any External Target:

- User Field Mapping

Roadmap for Deploying and Using the Adapter

The IBM-i5 Series Advanced adapter deployment involves deploying the LDAP Gateway, Voyager Agent.

- Chapter 2, "Adapter Deployment provides instructions for deploying the LDAP Gateway. Installing the LDAP Gateway and configuring the message transport layer.
- Chapter 3, “LDAP Gateway Deployment” describes installing and configuring the LDAP Gateway Server.
- Chapter 4, "Agent Adapter Deployment on IBM i5" describes the procedure to deploy the Voyager Agent. It is recommended that you perform this procedure with the assistance of the systems programmer or administrator.

- Chapter 5, "Troubleshooting" states the problem scenarios commonly associated with the adapter and the possible solutions to those problems. In addition, this chapter discusses some guidelines on using the adapter.
- Chapter 6, "Known Issues" lists the known issues associated with this release of the adapter.
- Appendix A, "Field Mapping between IBM-i5 Series and LDAP Gateway" describes the user field mapping between the LDAP Server and IBM-i5.

2 Adapter Deployment

The following sections of this chapter describe the procedure to deploy the LDAP Gateway:

- Files and Directories That Comprise the Adapter
- Copying the Adapter Files
- Installing and Configuring the LDAP Gateway

Files and Directories That Comprise the Adapter

Table 2-1 Files and Directories That Comprise the Adapter:

Files and Directories	Description
etc/LDAP Gateway/ldapgateway.zip	Files required for LDAP Gateway deployment
scripts/propertEncrypt.sh (bat)	Files required encrypting property file passwords
scripts/meta-population-adatper.jar	Jar file for reading EXIT file on OS and populating internal LDAP
scripts/meta-properties	Properties file containing all configurable information needed to run meta-import
scripts/run_initial_file.bat	Batch job to pre-populate Internal LDAP Store for use for Full Imports or Reconciliation
scripts/run_read_file.bat	Batch job you can use to run the read of the OS file at any time for change events.
etc/Provisioning and Reconciliation Adapter/Mainframe_AS400.zip	Files required for the installation of the Voyager Agent and Pioneer Agent on the target system

See Also:

- "Copying the Adapter Files"
- "Step 2: Deploying the Voyager Agent "

3 LDAP Gateway Deployment

To install and configure the LDAP Gateway:

1. Extract the contents of the ldapgateway.zip file to a directory on the same server as your Identity Manager. In this document, the location (and name) of the ldapgateway directory is referred to as LDAP_INSTALL_DIR.

2. **Download jtOpen (http://sourceforge.net/projects/jt400/) jar files jt400.jar and util400.jar and add them to the /ldapgateway/lib directory.**

3. SET JAVA HOME. In a text editor, open the following scripts from the `LDAP_INSTALL_DIR/bin` directory.

   Linux:

   - run.sh: Edit the following
     ```
     ##### SET ENVIRONMENT VARIABLES #######
     APP_HOME=/opt/ldapgateway
     TMPDIR=/opt/ldapgateway/temp

     # Get standard environment variables
     # Like JAVA_HOME, etc.
     if [ -r "$PRGDIR"/setenv_idf.sh ]; then
       . "$PRGDIR"/setenv_idf.sh
     else
       JAVA_HOME=/opt/j2sdk
       SECURE="false"
       SM=""
       DEBUG="false"
       DB=""
       JVM_OPTS=""
     Fi
     ```

   - setenv.sh: Edit the following
     ```
     JAVA_HOME=/opt/j2sdk
     ```

   Windows:

   SET JAVA_HOME=\software\java\j2sdk1.5_21

4. In a text editor, open the as400.properties file. This file is located in the LDAP_INSTALL_DIR/conf directory. In this file, specify information for the following properties of the message transport layer that you use

   Here is the description for each of the properties.

Parameter	Sample Value	Description
host	10.0.0.1	Target iSeries IP or Host address for the Reconciliation Agent to use
_isSSL	False	Set to true for SSL execution to iSeries
adminId	As400AdminID	Target i5 system administrator ID
adminPwd	As400Pwd	Target i5 system administrator password
agentHost	10.0.0.1	Target iSeries IP or Host address for the Reconciliation Agent to use
agentAdminId	As400AgentAdmin	Target i5 system reconciliation agent administrator ID
agentAdminPwd	As400AgentAdmPwd	Target i5 system reconciliation agent administrator password
agentLib	LSSUBURBAN	Target i5 library in which the reconciliation agent files are located
agentFile	QCSRC	Reconciliation agent file on the target IBM i5 system
agentMember	EUSRPWD	Reconciliation agent member file which contains the real time responses.
agentport	5490	Target LDAP Gateway port that the reconciliation agent will use
defaultDelete	Delete	This is used during disable user provisioning.
_ usePwdComplexLength _	True|false	USE IF YOU WANT TO CONTROL LENGTH OF PASSWORD
_ pwdMaxLength _	1-14	Length of Password

```
// USE INTERNAL META STORE [true|false] ENTERPRISE SET TO “true”
_internalEnt_=true

// USE INTERNAL META STORE DOMAIN OU – MUST MATCH suffix VALUE IN BEANS.XML
_domainOU_=as400

// FEATURE FOR TRIMMING VALUES ON OMVS UID ATTRIBUTE IN RACF //

# TRIM '0' BEGINNING FROM OMVSUID VALUE
trimOmvsUid=false
```

```
# HOW MANY ZERO's TO TRIM
trimNum=2

# NEW OMVS UID LDAP ATTRIBUTE NAME
newOmvsUidAttr=OmvsUidEmplNumber

# USED USERLIST ON CHANGE DATE
_useUserList_=false

# USED FOR DIFFERENT TIMESTAMP QUERY FOR NEW MA
useMAv2=false

# USE TO ADD ANY CHARACTER TO FRONT OF PASSWORD
usePwdReplaceCharacter=true

# ACTUAL CHARACTER TO ADD FOR PASSWORD
pwdCharacter=Q

# THROW ERROR IF PASSWORD CONTAINS A SPACE
isPwdSpace=true

# THROW ERROR IF PASSWORD CONTAINS THE UID
isPwdUID=true
```

5. In the as400.properties file, use the following property to specify whether you want to revoke access rights or delete users during Disable User provisioning operations:

    ```
    # DEFAULT ACTION WHEN DELETE FUNCTION USED
    ```

    - `_defaultDelete_=revoke`

    Set **revoke** as the value of this property if you want the user to be disabled on the target system as the outcome of a Delete User provisioning operation.

    Set **delete** as the value of this property if you want the user to be deleted from the target system as the outcome of a Delete User provisioning operation.

6. When clear text is not desirable for the passwords in the as400.properties file, optional password security is provided for the properties _adminPassword_ and _agentAdminPassword_ by using substitute properties and an encryption utility. The option property for _adminPassword_ is called _adminPasswordEncrypt_ and it is used in place of _adminPassword_. The optional property for _agentAdminPassword_ is called _agentAdminPasswordEncrypt_ and it is used in place of _agentAdminPassword_. Execution of the encryption utility is accomplished using a batch file for Windows and a shell script for Unix type operating systems. They are named propertyEncrypt.bat and propertyEncrypt.sh. They will be located in the directory where the distribution scripts are located.

The input you provide to the utility will be you password in the clear and the output will be an encrypted. The properties will look similar to this:

```
_adminPwdEncrypt_=098282D6EB11A6C30C101CCE4F7BC94B
_agentAdminPwdEncrypt_=098282D6EB11A6C30C101CCE4F7BC94B
```

7. To Edit either the Administrator credentials or Default Port From the `LDAP_INSTALL_DIR/dist/idfserver.jar` file, extract the `beans.xml` file, open it in an editor, and set values for the following:

    - Target system administrator credentials

    You must change the administrator credentials stored in the following lines of the beans.xml file:

    ```
    <bean name="as400" singleton="true"
    class="com.identityforge.idfserver.backend.as400.As400Module">

    <property name="adminUserDN"
    value="cn=idfAs400Admin,dc=as400,dc=com"/>

    <property name="adminUserPassword" value="idfAs400Pwd"/>
    ```

    Save the changes made to the beans.xml file, and then re-create the `idfserver.jar` file.

    Also for the new altAdminUserDN and altAdminUserPassword properties

3.1 Configure Custom i5 (AS400) Command Processing

1. Edit /ldapgateway/conf/as400.properties file and add the following paramters:

    ```
    # CHECK FOR CUSTOM COMMAND EXECUTION
    _isCustom_=true
    # CONFIGURE CUSTOM COMMAND EXECUTION
    _exeCustom_=WYNNE:RST400:USRPRF(rdn)PASSWORD(userpassword)|
    WYNNETRAN:RSTTRN USRPRF(rdn)|KRONOS:RSTKRN EMPNO(rdn)|
    ```

    - 'rdn' refers to beginning part of Full DN (ldap distinguishedName) that is passed in as part of the LDAP modify. It supports either 'cn' or 'uid'
    - Any other standard or support LDAP attribute can be passed in as part of the command. Like 'userpassword' above.
    - Each command is configured with OU:COMMAND (i.e., ou=WYNNE,dc=as400,dc=com)

3.2 Configuring Windows Service

Overview of the Windows Service for the LDAP Gateway:

The Windows Service for the LDAP Gateway is installed with a supplied IdentityForge batch file. The batch file for the windows service installer will have to be modified to change the JAVA_HOME and JVM variables which are used with the Java JDK. This batch file is a modified version of the batch file used to normally run the LDAP gateway. The windows service installer uses the Apache Procrun utility prunsrv.exe to create a fully managed Windows Service for the LDAP Gateway.

To install and configure the Windows Service for the LDAP Gateway:

- Copy the **IDF-Win-Service.bat** batch file from the IdentityForge /win_service directory of the release package to the <LDAP_INSTALL_DIR>/ldapgateway/win_service directory. If the directory does not exist, create it and copy the batch file there.

- Locate the service install utility from the IdentityForge/win_service directory of the release package. Your system requirements will determine whether you need the 32bit or 64bit version. The 32bit version of the utility is named **prunsrv_win32.exe**. The 64bit version of the utility for systems running AMD processors is named **prunsrv_amd64.exe**. The 64bit version of the utility for systems running INTEL processors is named **prunsrv_intel64.exe**. Copy the utility that is for your system to the <LDAP_INSTALL_DIR>/ldapgateway/win_service directory.

- Rename the install utility you just copied to **IdentityForgeService.exe**. Renaming this file is necessary since the batch file will be expecting it to be named like that. It also lets you better recognize the running process and associates that it belongs to IdentityForge.

- Copy the **prunmgr.exe** file from the IdentityForge /win_service directory of the release package to the <LDAP_INSTALL_DIR>/ldapgateway/win_service directory. This file does not have to be renamed. It is used by the batch file also.

- In a text editor, open the **IDF-Win-Service.bat** file in the <LDAP_INSTALL_DIR>/ldapgateway/win_service directory. If the JAVA_HOME and JVM directory in your installation is different that what is specified in the batch file, then modify the JAVA_HOME and JVM directory to match your installed location. Here is the as depicted in the following example:

```
 set JAVA_HOME=C:\software\Java\jdk1.6.0_16
 set JVM=C:\software\Java\jdk1.6.0_16\jre\bin\server\jvm.dll
```

- After saving the file, execute the following command from a console from the <LDAP_INSTALL_DIR>/ldapgateway/win_service directory to install the service.

```
> IDF_Win_Service install
```

If there are any problems with the installation of the service from the batch file, you may need to check the JAVA_HOME and JVM variables to make sure they are accurate. If any modifications need to be made, it is best to uninstall the service, make the modifications and re-install the service until it installs and runs correctly. To uninstall the service, execute the following command from the <LDAP_INSTALL_DIR>/ldapgateway/win_service directory:

```
> IDF_Win_Service remove
```

- Once the service is installed, you can start, stop, and restart it from the standard Windows Services manager.

3.3 Configuring SSL for the Connector

This section describes how to configure Secure Sockets Layer (SSL) for the AS400 connector.

In summary, you must fetch the SSL certificate from the OS/400 target system and then import the certificate

Before you begin, consider these requirements:

- For the JDK requirements, set your JAVA_HOME environment variable to point to your specific JDK installation.
- SSL must be configured and enabled on the OS/400 server, and the Digital Certificate Manager must be started. For more information, see the IBM manual at the following location:

  `http://www-912.ibm.com/s_dir/slkbase.NSF/DocNumber/28604514`

To configure SSL for the AS400 connector, follow these steps:

1. Fetch the SSL certificate from the OS/400 target system:
   1. In a web browser, go to the Digital Certificate Manager on http://OS400domain:2001, where OS400domain is the OS/400 target system. Use the same user account and password that you use to access the target OS/400 system.
   2. In the left panel, select Create Certificate Authority.

      Or, if the Create Certificate Authority is not an option, select Install Local CA Certificate on Your PC.

   3. Select Install Certificate, and copy the certificate to a text file. For example: cert.txt
2. Determine the SSL keystore location on the server you are using.
3. Use the keytool -importcert command to add the certificate from Step 1 to the keystore for the specific AS400 LDAP connector server.

   For example,:

   ```
   keytool -importcert -file path-to-certificate -alias arbitrary-alias -
   keystore <JAVA_HOME>/jre/lib/security/cacerts
   ```

   where:

   - path-to-certificate is the path to the certificate file you obtained in Step 1.
   - arbitrary-alias is a user-defined alias for identification of the certificate in the certificate store.

To verify presence of the certificate in the certificate store, use the `keytool -list -keystore` command.

3.3 Configuring LDAP Gateway with Multiple Connectors

Multiple LPAR Support via Virtual Directory:

1. Open the beans.xml file located inside the /ldapgateway/dist/idfserver.jar
2. Copy/Paste the current <beans name=as400> inside the file and rename it to something else (example: <beans name=***as400LPAR2***>.
3. Edit the following properties that are included in the new <beans name> that was just pasted above (note all below that are in BOLD need to be changed).

```
<bean name=”as400LPAR2" singleton="true"
class="com.identityforge.idfserver.backend.as400.As400Modul
e">

          <property name="suffix" value="dc=as400,dc=com"/>
          <property name="workingDirectory"
          value="../as400"/>
          <property name="adminUserDN"
          value="cn=idfAs400Admin, dc=as400,dc=com"/>
          <property name="adminUserPassword"
          value="idfAs400Pwd"/>
          <property name="allowAnonymous" value="true"/>
          <property name="entryCacheSize" value="1000"/>
          <property name="defaultUacc" value="read"/>
          <property name="searchUsersType" value="user"/>

          <property name="schema" ref="schemas"/>
          <property name="metaBackend"><ref
          bean="hpbe2"/></property>

          <property name="configLocation"
          value="../conf/as400.properties"/>

          <property name="agent" value="true"/>
          <property name="agentAdapters">
               <list>

          <value>com.thortech.xl.as400.recon.As400AgentReco
          nImpl</value>
               </list>
          </property>
     </bean>
```

4. Create a new folder under the /ldapgateway install directory that matches the value used above for the “workingDirectory” property.

5. Create a new as400.properties file using a different name that you configured above for the “configLocation” property and copy/paste all the data from the as400.properties to your new file. Once copied, edit the _host, _port properties in the file to match the LPAR/Pioneer Agent that it will send provisioning request too.
6. For Each new suffix created (ie. dc=as4001,dc=com) create the following XML section after each <bean name=as400LPAR2> Change the BOLD values below…make sure that when changing the name that the last value is numeric and that the constructor argument matches the number.

```
<bean name="be5"
class="com.identityforge.idfserver.backend.BackendEntry">
     <constructor-arg value="as400"/>
     <constructor-arg value="5"/>
     <constructor-arg value="dc=as400,dc=com"/>
</bean>
```

7. Add each new <bean name=**as400LPAR2**> to the NEXUS bean for processing commands. Add to the following section.

```
<property name="backends">
     <list>
          <ref bean="hpbe2"/>
          <!-- <ref bean="racf"/> -->
          <ref bean="as400"/>
          <!-- <ref bean="acf2"/> -->
          <!-- <ref bean="tops"/> -->
          <ref bean=”as400LPAR2”/>
     </list>
</property>
```

8. Save beans.xml file and re-jar the idfserver.jar release distribution.

3.4 Configuring Meta Population Script for initial population of LDAP META

This functionality is used to query the iSeries for all users and initially populate the META internal LDAP store.

Edit meta-properties file and set values to your LDAP environment.

```
ldapUrl:ldap://localhost:6389
ldapAdminDn:cn=idfAs400Admin, dc=as400,dc=com
ldapAdminPwd:idfAs400Pwd
rootDn:dc=as400,dc=com
domainOU:as400
metaAdminDn:cn=Directory Manager, dc=system,dc=backend
metaAdminPwd:testpass
```

```
metaBaseDn:dc=system,dc=backend
```

Run.
Run_initial_file.bat which will process all user to store internally in the LDAP Store.

3.5 Configuring Meta Population Script for reading EXIT file on iSeries

This functionality is used to read the Change Events stored on the iSeries Encrypted File created by the EXITS

Edit meta-properties file and set values to your LDAP environment.

```
ldapUrl:ldap://localhost:6389
ldapAdminDn:cn=idfAs400Admin, dc=as400,dc=com
ldapAdminPwd:idfAs400Pwd
rootDn:dc=as400,dc=com
domainOU:as400
metaAdminDn:cn=Directory Manager, dc=system,dc=backend
metaAdminPwd:testpass
metaBaseDn:dc=system,dc=backend
```

Run.
Run_read_file.bat which will process data stored in the file captured by the EXIT changes and stored internally in the domanOu property internally in the LDAP Store.

4 i5/OS Agent Adapter Deployment

NOTE: This is installed and configure ONLY if you have the Enterprise Edition of the IBM-i5 Series Advanced Adapter.

Overview:

When the exit program XUSRPWD is triggered by any of the exit points it has been registered to, it collects data specific to the exit that called it. This data is encrypted and appended to the file EUSRPWD. The design of the AS400 allows the exits to append data without having contention issues.

When the data is collected, the IDF gateway renames the EUSRPWD file to EDZ + threadnumber (4 digits) + .BU (example EDZ0004.BU). This is done to allow the exits to continue collecting data if they are called during the time the IDF gateway is processing the data.

Only the reconciliation agent (Voyager-EXITS) needs to be installed on the target i5 system. The provisioning agent (Pioneer) is part of the base LDAP Gateway install. The reconciliation agent installation is provided as an i5 save file (savef). Once the agent is downloaded from the IDF website then it has to be unzipped with either PKZIP or WINZIP. The save file is named IDFEX.SAVF. This file is uploaded to the i5 system by using a 5250 emulator or FTP. Once uploaded to the i5, the uploaded file must be restored using the RSTOBJ (restore objects) command.

Assumptions:

- Installer has working knowledge of i5 systems Programming
- A 5250 emulator on Desktop system with access to target i5 system.
- Access to the Internet for download of software.

How software is packaged:

- I5 save file

1. Transmit or FTP the /etc/Provisioning and Reconciliation Connector/IDFEX.SAVF file to any desired directory on the i5.

Note: For this set of instructions, the directory to which this file is transmitted will be referred to as LSVALGAARD.

2. To view the contents of the TLIBEX.SAVF file, run the DSPSAVF command as shown.

   DSPSAVF   FILE(SAMPLIB/IDFEX)

   The following is the output of the DSPSAVF command:

```
==============================================================================
                  Display Saved Objects - Save File          ,

Library saved  . . . :     ORIGLIB            Release level  . . . :
V4R5M0
ASP  . . . . . . . . :         1                   Data compressed  . . :   No
Save file  . . . . . :         IDFEX               Objects displayed  . :    3
Library  . . . . . .  :        ORIGLIB             Objects saved  . . . :     3
Records  . . . . . . :         688                 Access paths . . . . :     0
Save command . . . . :  SAVOBJ
Save active  . . . . :      *NO
Save date/time . . . :      01/20/07   01:28:35

Type options, press Enter.

  5=Display saved data base file members

Opt  Object          Type     Attribute     Owner        Size (K)   Data
    XUSRPWD        *PGM     CLE          ORIGLIB           236   YES
    NOTIFY         *PGM     CLE          ORIGLIB            68   YES
    QCSRC           *FILE    PF            ORIGLIB            24   YES

F3=Exit       F12=Cancel

==============================================================================
```

3. Restore the objects in the IDFEX.SAVF file by running the RSTOBJ (restore object) command. The following is the syntax for this command:

```
RSTOBJ OBJ(*ALL) SAVLIB(ORIGLIB) DEV(*SAVF) SAVF(SAMPLIB/IDFEX)
RSTLIB(NEWLIB)
```

The RSTOBJ command saves the restored objects in a new target library. In the command:

4. The SAVLIB parameter takes the original library name as input. In the command, replace ORIGLIB with the original library name.
5. DEV(*SAVF) indicates that a savefile is used.
6. The SAVF parameter takes the directory name and file name of the savefile.
7. The RSTLIB parameter takes the new library in which you restore the save file objects. In the command, replace NEWLIB with the name of the new library.

If required, specify the general public library (QGPL) as the new target library. The QGPL is an existing library on IBM i5/OS than can be used by the system or a user.

Installation of the exits for Reconciliation agent (Voyager)

After copying the connector save file to the directory of choice, you install the exits for the Reconciliation Agent. As mentioned earlier, the connector exits are engineered to be the last exits called in sequence, allowing existing exits to function normally. To install the exits for the Reconciliation Agent:

> Note:
>
> The Reconciliation Agent can be installed in either a menu-driven or a command-driven installation protocol. The following instructions assume the use of the menu-driven protocol.

1. Log in to the i5 system as a system administrator.
2. Ensure that the connector library files and objects are present in the LSVALGAARD directory.
3. Start the WRKREGINF User Exit Registration program, as shown:

```
 Parameters or command
===> WRKREGINF
```

   In IBM i5/OS, exit programs are called dynamically. This means that if an exit program is registered with the system, then you can replace the program with a new version, without the need to register the exit.

4. You must register the exit points that are required for the Reconciliation Agent with IBM i5/OS.

   DO NOT USE NOTIFY EXIT

   From the menu that is displayed when you run the WRKREGINF program, select option 8 for the exit points that you want to register, either as a group or one at a time. The following exits are registered.

QIBM_QSY_CHG_PROFILE	CHGP0100	*YES	Change User Profile
QIBM_QSY_CRT_PROFILE	CRTP0100	*YES	Create User Profile

QIBM_QSY_DLT_PROFILE	DLTP0200	*YES	Delete User Profile - before
QIBM_QSY_RST_PROFILE	RSTP0100	*YES	Restore User Profile
QIBM_QSY_VLD_PASSWRD	VLDP0100	*YES	Validate Password

Each exit point has an exit point format associated with it. The format that is passed to the exit program determines the format of the other information passed to it.

The CHG_PROFILE (change), CRT_PROFILE (create), DLT_PROFILE (delete), and RST_PROFILE (restore) exit points are used to change, create, delete, and restore user profiles. The VLD_PASSWRD is called when the password is changed by the user.

Notes:

Deleting a user profile can take a long time because a user may own multiple objects, and therefore, be present on many lists and internal tables. After a user is deleted, cleaning up all the entries for the user takes a long time to process. Therefore, you can use a batch job to run the cleanup process. There are two delete points: before the start of the cleanup job and at the end of the cleanup job. This means that in the process of deleting the user profile, there are only two times when actions are monitored. The Reconciliation Agent monitors only the delete point before the clean-up job.

The RST_PROFILE exit point is not called when a user profile is created with the initial password or when the security administrator changes the password for a user. This IBM design limitation has been fixed in IBM i5 V5R4 by introducing another exit point called QIBM_QSY_CHK_PASSWRD.

XUSRPWD is the exit program that must be registered with your exit points as the first exit program. However for the exit point QIBM_QSY_CHG_PROFILE you might find that there is an existing exit program registered for this point. In the following code snippet, this is QGLDPUEXIT in the main system library QSYS, which implies that the i5 system itself uses this exit point to extend its functionality.

Do not do anything with this existing exit program.

```
                Exit
              Program       Exit
Opt          Number       Program            Library
1                         XUSRPWD          "CUSTOMERS LIBRARY"
2147483647                QGLDPUEXIT     QSYS
```

You must also consider the Exit Program Number, which determines the order in which the exit programs run. The system exit program is typically the last to run in the processing order, and therefore, has a very large Exit Program Number (2147483647). Enter the IDF custom user exit program and the library for it, and select option 1 for adding the exit program.

5. Press the Enter key. The Add screen is displayed with the following values:

```
Exit point . . . . . . . . .  > QIBM_QSY_CHG_PROFILE
Exit point format  . . . . . > CHGP0100            Name
Program number . . . . . . > 1                       1-2147483647, *LOW, *HIGH
Program  . . . . . . . . . . . . > XUSRPWD           Name
Library  . . . . . . . . . . . . . >   "CUSTOMERS LIBRARY"  Name, *CURLIB
Threadsafe . . . . . . . . .   *UNKNOWN           *UNKNOWN, *NO, *YES
Multithreaded job action . .   *SYSVAL          *SYSVAL, *RUN, *MSG, *NORUN
Text 'description' . . . . .   *BLANK
```

Press the Enter key to add the program, and then the F5 key to refresh the system to display the result.

Note:

An exit program runs in the environment (called an activation group) of the job or user issuing the command that causes the exit program to be called. Therefore, the current library (*CURLIB) value changes often and the system might not be able to locate the exit program. The library from which the system can find the exit program is usually hard coded into the exit program registration, as shown in the screen output.

6. Register the exit points as shown in the following screen output:

```
          Program     Exit
Opt        Number    Program            Library

                1    XUSRPWD            LSVALGAARD
       2147483647    QGLDPUEXIT         QSYS
```

```
Exit point:   QIBM_QSY_CHG_PROFILE     Format:   CHGP0100

Exit point:   QIBM_QSY_CRT_PROFILE     Format:   CRTP0100

Exit point:   QIBM_QSY_DLT_PROFILE     Format:   DLTP0200

Exit point:   QIBM_QSY_RST_PROFILE     Format:   RSTP0100

Exit point:   QIBM_QSY_VLD_PASSWRD     Format:   VLDP0100
```

Note:

On IBM i5 V5R4 and up, you also register the CHK_PASSWRD exit point.

7. Enter the WRKSYSVAL command and scroll down to the following line:

```
QPWDVLDPGM  *SEC     Password validation program
```

The WRKSYSVAL command allows you to change the system values that control most of the system configuration.

8. Select option 2 for QPWDVLDPGM. The value should be *REGFAC. Specifying a validation program here is obsolete. The calling format is different from that of registered programs and is no longer found in recent IBM documentation.

This completes the installation of the reconciliation agent exits.

Notes:

- Do not specify an exit program instead of *REGFAC because this will interfere with an existing validation program. This way of specifying a validation program is no longer valid. The IBM i5 Advanced connector code does not support the obsolete validation program.
- The QSECURITY system value determines the security level of the system. The highest (most secure) level is level 50. The IBM i5 Advanced connector is designed for and has been successfully tested on level 50.
- Before the General Registration Facility was introduced, a password validation program was used. This was handled through the system value settings.

5 Troubleshooting

This chapter discusses the following topics:

- Troubleshooting
- Guidelines for using the Connector

Table 5-1 Troubleshooting

Problem Description	**Solution**
Cannot establish a connection to the IBM-i5/OS server.	• Ensure that the i5 server is up and running. • Check that the necessary ports are working. (See http://www-03.ibm.com/systems/i/software/toolbox/faqports.html). • View the Gateway logs to determine if messages are being sent or received. <install-directory>/ldapgateway/logs • Examine the as400.properties configuration to verify that the IP address, admin ID, and admin password are correct. •
A particular use case does not appear to be functioning.	• Check for the use case event in question on the Gateway Server Log. Then check for the event in the specific log assigned to that Advanced Connector. • If the event does not register in either of these two logs, then investigate the connection between i5 and the connector Gateway. • If the event is in the log but the command failed to make the intended change on a iSeries user profile, and then check for configuration and connections between the Gateway and the i5.

5.1 Guidelines on Using the Connector

Apply the following guidelines while using the connector:

- Passwords used on the i5 must conform to stringent rules. These passwords are also subject to restrictions imposed by corporate policies and rules about i5 passwords. While creating user accounts for target systems on the i5, you must take these requirements into account before assigning passwords for these accounts.

6 Known Issues

The following are known issues associated with this release of the connector:

- Currently the connector does not support deleting Group Profiles

APPENDIX A: User Field Mappings

User Field Mappings

Table A-1 User Field Mapping

LDAP Attribute	IBM i5 Field	Description
uid	USER	User login ID
cn	NAME	User full name
sn	NAME	User last name
givenName	NAME	User first name
userPassword	PASSWORD	Password used to login
revoke	NA	Value 'Y' if user is revoked or 'N' if user is resumed
status	STATUS	*ENABLED | *DISABLED
text	TEXT	Text description free form field
spcaut	SPCAUT	Special authority
usrcls	USRCLS	User class
inlmnu	INLMNU	Initial Menu
uidNumber	UID	UID
gidNumber	GID	GID
homeDir	HOMEDIR	HOME Directory
locale	LOCALE	Locale
grpprf	GRPPRF	Group profile
supgrpprf	SUPGRPPRF	Suplemental Group Profiles
lmtcpb	LMTCPB	Limit capabilities
inlpgm	INLPGM	Initial program
jobd	jobD	Job Decription
noPassword	PASSWORD	*NONE (LDAP attribute returns true|false)
changeDate	CHANGE_DATE	ObjectDefinition CHANGE_DATE
lastUsedDate	LAST_USED_DATE	ObjectDefinition LAST_USED_DATE
creationDate	CREATION_DATE	ObjectDefinition CREATION_DATE