IBM Atlas Suite
Version 6.0.1.4

IBM Atlas Suite V6.0.1 Fix Pack 4 Readme

IBM Atlas Suite
Version 6.0.1.4

IBM Atlas Suite V6.0.1 Fix Pack 4 Readme

Contents

Cumulative fix list (APARs)

The cumulative fix list contains all APARs that are fixed in version 6.0.1.4 of IBM Atlas Suite.

Important: For some APARs, such as security-related APARs, information about that APAR is not made available to customers to avoid compromising customer and product security. If an APAR is listed in the fix list but no information is available, the APAR might be a security APAR.

Table 1. Fix list for IBM Atlas Suite, Version 6.0.1.4

APAR	Description
HE11590	**From** field in Global Hold Reminder email contains incorrect user. The from field in Global Hold Reminder emails uses a paralegal or attorney email address. Because Global Hold Reminder emails can affect many matters and are handled by different paralegal or attorneys, the Global Hold Reminder emails should use a consistent from field. The fix is available from Fix Central in fix pack 6.0.1.4.
HE11594	CSV of exported interview results makes it impossible to differentiate between people with the same name. When exporting the interview results to a CSV file by using the Export function, the resulting data contains only the targets' names. The fix is available from Fix Central in fix pack 6.0.1.4.
HE11606	Matter is not updated with the user name of the last person to modify it. The matter MODIFIEDBY value is not properly set when the matter is updated. The fix is available from Fix Central in fix pack 6.0.1.4.
HE11622	$Recipients placeholder expansion is enhanced for improved reliability. When a notice is published by using the $Recipients placeholder, not all of the recipients show up in the emails. The fix is available from Fix Central in fix pack 6.0.1.4.
HE11626	Hold Notices with Virtual Interviews allow users to respond multiple times. With IBM Atlas Suite V6.0.1, hold with interview notices enable people to respond to the interview multiple times. In the past, only one response was allowed. The fix is available from Fix Central in fix pack 6.0.1.4.
HE11630	Unable to confirm on behalf of another user for a hold notice. This issue is specific to upgraded notices before V6.0. In IBM Atlas Suite V6.0.1.2, legal personnel are unable to Confirm On Behalf Of recipients. When going to the Notices Sent page and clicking on the list of specific notice recipients, the check box that normally appears to allow for legal to confirm is not available. The fix is available from Fix Central in fix pack 6.0.1.4.

Table 1. Fix list for IBM Atlas Suite, Version 6.0.1.4 (continued)

APAR	Description
HE11631	Clicking an interview notice URL in an IBM® Lotus® Notes® email message starts the notice in the Notes web browser rather than an external web browser. When a notice recipient tries to respond to an interview notice email by clicking on a $interviewurl link, the IBM Atlas Suite interview page should be displayed in a browser. If IBM Lotus Notes is the email client application, the IBM Atlas Suite interview page is displayed inside of the IBM Lotus Notes web browser instead of the default web browser for the workstation. The fix is available from Fix Central in fix pack 6.0.1.4.
HE11632	**Send Me** button does not work for suspended notices. When a notice is suspended, the **Send Me** button does not work on IBM Atlas Suite V6.x. The fix is available from Fix Central in fix pack 6.0.1.4.
HE11635	When saving a hold notice that contains a Virtual Interview without a Notice Questionnaire and that notice does not contain $NoticeResponseURL in the text of the notice, users receive the error `$NoticeResponseURL is required for Interview notice`. The substitution string $NoticeResponseURL is incorrectly required if the following configuration options are set: • A hold notice template is created of the type Rules • **Include Virtual Interview** is selected The fix is available from Fix Central in fix pack 6.0.1.4.

Known problems, restrictions, and solutions

Known problems, restrictions, and solutions that affect administration and usage of fix packs are documented as techdocs in the product support knowledge base.

You can find information about known problems, restrictions, and solutions that affect the administration and usage of fix packs by reviewing the following technical support documents. As problems are discovered and resolved and as other helpful information is developed, the IBM Software Support team updates the knowledge base. By searching the knowledge base, you can find workarounds or solutions to problems and useful tips that could help you with product administration or usage.

To review all known problems, restrictions, and solutions that affect all fix packs for version 6.0.1.4, use the following link to query the product support knowledge base: http://www.ibm.com/support/search.wss?rs=86&tc=SSRS7Z&atrn=SWVersion&atrv=8.4&atrn1=SWVersion&atrv1=8.4.0.1&rankprofile=8&dc=DA430&dtm.

At the time of publication of this fix pack readme file, the following problems, restrictions, and solutions were known:

- Known issue: When a person is deleted from an organization, the global notice is not sent to the user even though the user is still part of the notice and has not been released.
- Known issue: User names are not displayed correctly after users respond to questionnaires
- Known issue: Content in file attached to hold notice is not visible
- Known issue: Users cannot view a Schedule to Data Source Mapping Exceptions report
- Known issue: Multiple Global Hold Reminders sent after the application server is stopped and restarted
- Known issue: If a notice approver is using Firefox 10.0.5, that user can reject a notice without entering the required comments
- Known issue: When a hold notice containing the $interviewurl variable is sent to a user with an invalid email address, the virtual interview details report will incorrectly report that the user has replied to the notice
- Known issue: Global hold reminder fails with HTTP status of 302

Configuring SSL for your Java application server

You should enable SSL on your Java application server to encrypt web activity in the IBM Atlas Suite.

About this task

To ensure secure communication between a web browser and IBM Atlas Suite, you should enable SSL on the Java application server that hosts IBM Atlas Suite. If you do not enable SSL, confidential information such as passwords will be visible to all users.

See the documentation for your Java application server to enable SSL and encrypt the information on your server.

Protecting the ACA web service password

The ACA web service password is used by a connector to authenticate a caller (Atlas or Emulator), which calls the connector using the ACA Web Services. Today, this password is stored in an unprotected format in a connector property file. In IBM Atlas Suite V6.0.1 Fix Pack 4 the options are:

- Store the password in a WebSphere® J2C profile
- Store a password as an SHA1 digest in the connector's `auth.properties` file

Storing the ACA web service password in a WebSphere J2C profile

Store the ACA web access password in a J2C profile to secure it.

Procedure

1. Log in to the WebSphere administration application.
2. Go to **Security** > **Secure administration, applications, and infrastructure** > **Java Authentication and Authorization Service** > **J2C authentication data**
3. Create a J2C profile named `ACA_WS` (stands for Atlas Compliance Automation Web Service), providing a web service password. The ACA framework does not require user name, so you can provide any user name.
4. Save the master configuration.

Results

Now all ACA connectors that are deployed on this node share this password.

Important: All profile names are case-sensitive. They must be all uppercase.

Storing a password as an SHA1 digest in the auth.properties file

Store the ACA web access password as an SHA1 digest in the `auth.properties` file to secure it.

About this task

This method can be used if the connector runs on an application server other than WebSphere or the administrator does not want to configure a J2C profile.

Procedure

1. During the connector setup, select a password and configure it as an SHA1 digest using the password encoding form available on the connector main page.
2. Update the **`ACHP_PASSWORD`** parameter in the connector's `auth.properties` file:

   `ACHP_PASSWORD``=wLE3/i15JFnyb/djzORFdKW1qwM=`Note that the default password is *welcome*.
3. Restart the application server.

Results

In subsequent SOAP calls, the connector will:

- SHA1-encode the incoming password
- Compare the encoded incoming password with the password digest stored in the properties file
- Consider the client authenticated if digests match

Important: These mechanisms are implemented on the **achp_framework_base** level and are shared by all connectors including sample synchronous and asynchronous connectors.

Protecting Connector-to-Datasource passwords

The difference between the passwords that are described here (J2C and non-encrypted) and ACA Web Service passwords is that the connector must be able to retrieve the actual password as opposed to using an SHA1 digest (SHA1 is a one-way function). Therefore, the connector cannot store the password as a digest.

There are two options:

- J2C (passwords are stored in an authentication profile in WebSphere)
- Non-encrypted (passwords are stored in a property file)

Both options are implemented. If you do not want to store unencrypted data source password, you must use the WebSphere J2C feature. However, it is easier to use non-encrypted passwords for demonstration and proof-of-concept purposes.

About the IBM eDiscovery Manager Legal Hold connector

The IBM eDiscovery Manager Legal Hold connector stores:

- The ACA Web Service password either using the J2C **ACA_WS** profile or as an SHA1 digest in a property file
- EDM credentials either in the J2C **ACA_EDM_API** profile or unencrypted in a property file
- FileNet credentials either in the J2C **ACA_EDM_FILENET** profile or unencrypted in a property file
- Alternatively, you can define the J2C **ACA_EDM_ALL** profile, if the EDM API and Filenet share authentication credentials
- Alternatively, passwords can be stored unencrypted in a property file

If the connector does not find an API-specific profile, it tries to find the **ACA_EDM_ALL** profile. If it fails, it uses unencrypted passwords.

The **ACA_OPTIM_ALL** profile applies only to "connector-to-Optim" communication but not to "Atlas-to-connector" communication.

About the InfoSphere Optim connector

The InfoSphere Optim connector stores:

- The ACA Web Service password either using the J2C **ACA_WS** profile or as an SHA1 digest in the `auth.properties` file

- Optim connection passwords are either stored in the J2C profiles, **ACA_OPTIM_ALL** or **ACA_OPTIM_[TEMPLATE ID]_[SOURCE | HOLD]**

If the connector does not find a specific profile, it tries to find the **ACA_OPTIM_ALL** profile. If it does not find the **ACA_OPTIM_ALL** profile, it uses unencrypted passwords.

An example of a specific profile is the **ACA_OPTIM_ORDERS_SOURCE** profile. In this profile the template ID is "orders" and the password applies to only source archive files.

Protecting the Policy Distribution connector password

The Policy Distribution connector password can be protected in either a WebSphere J2C profile or stored as an SHA1 digest in the connector's `auth.properties` file.

The two options for protecting the Policy Distribution connector password are:

- Store the password in a WebSphere J2C profile
- Store a password as an SHA1 digest in the connector's `auth.properties` file

Storing the Policy Distribution connector password in a WebSphere J2C profile

Store the Policy Distribution connector password in a J2C profile to secure it.

Procedure

1. Log in to the WebSphere administration application.
2. Go to **Security** > **Secure administration, applications, and infrastructure** > **Java Authentication and Authorization Service** > **J2C authentication data**
3. Create a J2C profile named `PD_WS` (stands for stands for Policy Distribution Web Service), providing a web service user name and password.
4. Save the master configuration.

Results

Now all PD connectors that are deployed on this node share this password.

Storing the Policy Distribution connector password as an SHA1 digest in the auth.properties file

Store the Policy Distribution connector password as an SHA1 digest in the `auth.properties` file to secure it.

About this task

This method can be used if the connector runs on an application server other than WebSphere or the administrator does not want to configure a J2C profile.

Procedure

1. During the connector setup, select a password and configure it as an SHA1 digest using the password encoding form available on the connector main page.
2. Update the **password** parameter in the connector's `auth.properties` file:

password=wLE3/i15JFnyb/djzORFdKW1qwM=Note that the default password is *welcome*.

3. Restart the application server.

Results

In subsequent SOAP calls, the connector will:

- SHA1-encode the incoming password
- Compare the encoded incoming password with the password digest stored in the properties file
- Consider the client authenticated if digests match

Important: All profile names are case sensitive. They must be all upper case.

Protecting connector-to-datasource passwords

Currently, existing connectors do not need additional connector-to-data source passwords. Once the need arises, mechanisms similar to ACA will be implemented.

Installing IBM Atlas Suite, Version 6.0.1 Fix Pack 4 (V6.0.1.4)

To install Fix Pack 4 for IBM Atlas Suite, V6.0.1, you must first install or upgrade to IBM Atlas Suite, V6.0.1. For V6.0.1 installation instructions, see IBM Atlas Suite V6.0.1 Deployment Guide; for upgrades from previous Atlas releases, see IBM Atlas Suite V6.0.1 Upgrade Guide.

Important: If you uninstall your IBM Atlas Suite deployment, ensure that you delete this file: `ATLAS/Properties/Licenses/Atlas_Suite.6.0.1.swtag`. `ATLAS` is the IBM Atlas Suite home directory.

System requirements

System requirements for IBM Atlas Suite, V6.0.1 Fix Pack 4 must be met before installation.

The system requirements for IBM Atlas Suite, V6.0.1.x are listed here: http://www.ibm.com/support/docview.wss?uid=swg27023564.

Database upgrade summary

Before you upgrade to V6.0.1 Fix Pack 4, you must upgrade the Oracle database. To upgrade the database, you must have Oracle SYSDBA privileges.

Important: Before you apply IBM Atlas Suite, V6.0.1 Fix Pack 4, create a backup copy of your database.

Before you begin, you must collect the following Atlas database information:

- The host name (or IP address) and port of your database server, referred to as **DBHost** and **DBPort**.
- The TNS name of the database instance or net service that you want to connect to (**TNSName**)
- The literal, non-TNS database SID, or net service name (**DBName**)
- The name and password of a SYSDBA account (**SYS/SYSPWD**)
- The name and password of the Atlas schema owner (**PSSAPL/PSSAPLPWD**)
- The name and password of the Atlas web user account (**PSSWEBUSER/ PSSWEBUSERPWD**)
- The name and password of the Atlas Reports user account (**PSSRPTUSER/ PSSRPTUSERPWD**)
- The names of the table spaces that were created for Atlas (**PSS_USER** and **PSS_TEMP**)

  The database schema includes an optional **Monitor Job** that sends a red flag email if the Legal Notice or Alert system is not working properly. If you use the **Monitor Job** and you have upgraded your database, you will need:
  - The host name and port number of your SMTP server (**MailHost, MailPort**)
  - The email address of the person who receives the email (**MailTo**)
  - The email address that is used as the From: address in the email (**MailFrom**)
- If you do not have this information during initial deployment, you can set it later. See the *IBM Atlas Suite Administrators Guide: System Configuration*.

To use the **Monitor Job**, your database server must be able to access your SMTP server.

Important: Before you apply IBM Atlas Suite, V6.0.1 Fix Pack 4, create a backup copy of your database.

Preparing to upgrade

Procedure

To prepare to upgrade:

1. Log in to the database client machine and create the Atlas home directory (referred to as **ATLAS** in these instructions). If you are using the same database client machine that you used to install IBM Atlas Suite, V6.0.1, you should already have an Atlas home directory. If you do, first move the directory to a new location. For example, enter these commands:

   ```
   $ mv ATLAS c:/ATLAS6.0.1
   $ mkdir ATLAS
   ```

2. Open the IBM Atlas Suite, V6.0.1.4 archive and copy `/Atlas/Schema` into the Atlas home directory to create an `ATLAS/Schema` directory.
3. Open the database configuration file in a text editor:

   `ATLAS/Schema/Deploy/smf/db/etc/oracle/smf_properties.ini`

4. Look for the **[Connection]** section and replace the value placeholders (in italics) with actual values.

   ```
   ; Connection properties
   [Connection]
   DATABASE_USER          = PSSAPL
   DATABASE_USER_PASSWORD = PSSAPLPWD
   DATABASE_NAME          = TNSName
   DATABASE_URL           = jdbc:oracle:thin:@DBHost:DBPort:DBName
         --or--
   DATABASE_URL           = jdbc:oracle:thin:@//DBHost:DBPort/DBName
   DATABASE_JAVA_PRIV     = N
   ER_ENABLED             = N
   ```

   - If you are connecting directly to a database instance, use the first form of the **DATABASE_URL** value. If you are connecting through a net service, use the second form. The **DBName** value must be the real, non-TNS database SID, or net service name.
   - If you are using an External Repository, change the **ER_ENABLED** and **DATABASE_JAVA_PRIV** flags to Y. If you are not using an External Repository, leave them both as the default (N). To enable the External Repository after you deploy the database, see *IBM Atlas Suite Administrators Guide: System Configuration*.

5. If you want to use the Atlas Monitor Job, look for the **[MailServer]** section and replace the value placeholders with actual values:

   ```
   ; Mail Server properties
   [MailServer]
   MAIL_HOST              = MailHost
   MAIL_FROM              = MailFrom
   MAIL_TO                = MailTo
   SMTP_PORT              = MailPort
   ```

   To configure the Monitor Job after you deploy the database, see *IBM Atlas Suite Administrators Guide: System Configuration*.

6. If you want to enforce unique *Person Identifier* values in the Person records, set **UNQ_PERSONIDENTIFIER** to Y. The default value is N.

```
; Data Integrity properties
[DI]
UNQ_PERSONIDENTIFIER   = Y
```

7. Save and close the `smf_properties.ini` file.
8. Start your Oracle database if it is not already running.
9. Stop all Oracle jobs that service IBM Atlas Suite. How you find and stop the Oracle jobs depends on your environment. The IBM Atlas Suite distribution does not include tools or instructions for stopping the jobs.
10. Stop all Atlas applications: Atlas, AtlasLink, and Atlas Reports.
11. In a command window, drop and then re-create the **PSSWEBUSER** and **PSSRPTUSER** users:

```
$ cd ATLAS/Schema/Deploy/smf/db/release/default/oracle/create/user/
$ sqlplus SYS/SYSPWD@DBName @drop_pa_user.sql PSSWEBUSER
$ sqlplus SYS/SYSPWD@DBNAME @drop_pa_user.sql PSSRPTUSER
$ sqlplus SYS/SYSPWD@DBName @create_paweb_user.sql PSSWEBUSER PSS_USER PSS_TEMP
$ sqlplus SYS/SYSPWD@DBName @create_parpt_user.sql PSSRPTUSER PSS_USER PSS_TEMP
```

   Important: Change the **PSSWEBUSER** and **PSSRPTUSER** passwords after you re-create the users. By default, the passwords are the same as the user names.
12. If you are using the Monitor Job and you upgraded your Oracle database, execute the `grant_acl_sendmail.sql` script, passing in the arguments shown below. This will give the Monitor Job sufficient privileges to send email:

```
$ sqlplus SYS/SYSPWD@DBName @grant_acl_sendmail.sql PSSAPL MailHost
MailPort
```

Running the upgrade script

Procedure

To run the upgrade script:

1. Change to the following directory by running this command: `$ cd ATLAS/Schema/Deploy/smf/db/etc/python`
2. Run the script that upgrades the schema:

Operating system	Script command
Sun Solaris or Red Hat Linux	`$ ./run-script.sh upgradeSchema.py -v oracle > install.log`
Windows	`$ run-script.bat upgradeSchema.py -v oracle > install.log`

After the upgrade

Procedure

1. After a successful schema upgrade, grant privileges to **PSSWEBUSER** and **PSSRPTUSER** by running the following commands:

```
$ cd ATLAS/Schema/Deploy/smf/db/release/default/oracle/create/user/
$ sqlplus PSSAPL/PSSAPLPWD@DBNAME @grant_paweb_syn_priv.sql PSSWEBUSER
$ sqlplus PSSAPL/PSSAPLPWD@DBNAME @grant_parpt_syn_priv.sql PSSRPTUSER
```

2. Restart the Oracle jobs that service IBM Atlas Suite.

Results

Now, you are ready to upgrade the IBM Atlas Suite applications.

Upgrading IBM Atlas Suite applications to V6.0.1.4

The following is a summary of tasks required to upgrade the IBM Atlas Suite applications to V6.0.1 Fix Pack 4.

Use this section to upgrade the IBM Atlas Suite applications to V6.0.1.4. This section should be used by an application server administrator. You must upgrade and start your database before you upgrade the Atlas applications.

To upgrade the applications, you must know the location of the IBM Atlas Suite home directory that you used in the V6.0.1 release. The examples in this section call the directory `ATLAS`.

Important: These instructions assume that you are using the same version of the application server that you used when you installed IBM Atlas Suite, V6.0.1. If you are using a new version, for example, if you upgraded from WebSphere Application Server, Version 6.1 to versions 7 or 8, you must reconfigure the application server as described in the *IBM Atlas Suite V6.0.1 Deployment Guide*.

Copying the IBM Atlas Suite files

Procedure

To copy the IBM Atlas Suite files:

1. Stop the Atlas applications in your application server.
2. Log in to the machine that hosts the application server.
3. Move your current `/Atlas` home directory to a new location and then re-create the home directory, for example:

   ```
   $ mv ATLAS c:/ATLAS6.0.1
   $ mkdir ATLAS
   ```

4. Open the IBM Atlas Suite, V6.0.1.4 archive and copy the contents of the `/Atlas` directory into the Atlas home directory.

Merging previous configuration changes

Merge configuration settings from the prior version of IBM Atlas Suite with the upgraded version to retain custom settings.

About this task

The `ATLAS/Properties` directory and subdirectories contain a number of files that are used to configure various aspects of Atlas. If you made any changes to these files when you configured your previous version of IBM Atlas Suite, you must merge the changes into the 6.0.1.4 versions of the files. This includes new icons that you might have added to the application, for example, to represent custom Data Source media types.

Most of the configuration files that you might have changed are in the `ATLAS/Properties` directory; however, make sure that you also check your old versions of the files in `ATLAS/Properties/defaultimpl/db`. These files configure the Puller Agents that are used by Atlas Extensions.

Clearing the application server cache

When you upgrade to a new version of IBM Atlas Suite, you must clear the data that the application server has cached for the Atlas applications. Clear the cache by removing directories that are contained in the **AtlasSuite** and **AtlasReports** domain or profile directories.

About this task

The directories that you must remove depend on the application server that you are using:

Application server	Directories to remove
WebLogic Server	• cache • tmp
WebSphere Application Server	• temp • wstemp
JBoss Application Server	• tmp • work/jboss.web/localhost/

Deploying the Atlas applications

Before you deploy the V6.0.1.4 Atlas applications in your application server, you must remove the current instances of the applications.

About this task

The V6.0.1.4 application archives are in the following directories:

Application	Location of archive
Atlas Suite	ATLAS/EAR/PolicyAtlas.ear
Atlas Extensions	ATLAS/WAR/AtlasExtensions.war orATLAS/WAR/AtlasExtensions.ear
Atlas Reports	ATLAS/WAR/AtlasReports.war orATLAS/EAR/AtlasReports.ear

The EAR files are wrappers around the respective WAR files. You can deploy either the EAR or the WAR file. If you are not sure how to deploy an application, see your application server documentation.

Integrating IBM Atlas Suite with Cognos Business Intelligence

IBM Atlas, V6.0.1.4 integrates with the reporting framework from IBM Cognos® Business Intelligence, which allows users to generate and display reports that are based on Atlas artifacts.

About this task

IBM Atlas, V6.0.1.4 contains sample Cognos reports administrators can use to configure Atlas to work with IBM Cognos Business Intelligence.

The process consists of:

- Validating system requirements
- Creating a dedicated user for reports
- Connecting to the data source
- Importing the package of embedded sample reports to IBM Cognos Business Intelligence
- Rendering the sample reports in IBM Cognos Business Intelligence
- Installing the custom authentication module in Atlas
- Configuring the integrated authentication module in Atlas
- Registering the sample reports in Atlas
- Rendering the sample reports in Atlas
- Modifying passwords in the configuration files

System requirements

IBM Atlas Suite integrates with IBM Cognos Business Intelligence V10.1. For the full IBM Cognos Business Intelligence V10.1 hardware and software requirements, see http://www-01.ibm.com/support/docview.wss?uid=swg27019126.

Specifically, for the IBM Atlas Suite integration with IBM Cognos Business Intelligence the following Cognos deployments are supported:

- 32-bit is supported on Windows and Linux
- 64-bit is supported on Windows only

Important: In an enterprise deployment, do not install IBM Atlas Suite and IBM Cognos Business Intelligence on the same server.

For general IBM Atlas Suite system requirements, see: http://www.ibm.com/support/docview.wss?uid=swg27023564

Creating the report user

To create Cognos reports, a dedicated user account named PSSRPTUSER is required.

About this task

Tip: If you enabled Business Intelligence and Reporting Tools (BIRT) reports in a previous version, and did not change the default PSSRPTUSER user account, you can continue to use that account.

Procedure

To create the PSSRPTUSER user account for Cognos reports:

1. On the server where Atlas is deployed, ensure that you are logged in as a SYSTEM user. You must be logged in as a SYSTEM user to create the PSSRPTUSER user.
2. Enter the following command to change to the directory where the script to create the user is located: `cd C:/ATLAS/Schema/Deploy/smf/db/release/6.0/oracle/create/user/`
3. Enter the following command to create the user: `sqlplus SYSTEM/SYSTEMPWD@DBName @create_parpt_user.sql PSSRPTUSER PSS_USER PSS_TEMP`

   Important: Change the PSSRPTUSER passwords after the users are created. By default, the passwords are the same as the user names.
4. Enter the following command to set the user privileges for the PSSRPTUSER report user: `sqlplus PSSAPL/PSSAPLPWD@DBName @grant_parpt_syn_priv.sql PSSRPTUSER`

Connecting to the data source

As part of the integration process, you must connect to the data source.

Before you begin

You must copy the sample package of embedded reports to your IBM Cognos Business Intelligence environment. Copy the `Sample Cognos Reports for Atlas.zip` file from the `\release\Atlas\AddOns\cognos\cognosreports` folder to your IBM Cognos Business Intelligence deployment folder. Typically this folder will be `C:\Program Files (x86)\IBM\cognos\c10\deployment`.

Procedure

To connect to the data source:

1. Start the Cognos portal by opening this URL in a browser: `http://YourCognosServer:YourCognosPort/ibmcognos/`.
2. Click the **My Home** link.
3. Click **Launch** > **IBM Cognos Administration** and then click the **Configuration** tab.
4. Click the **Data Source Connection** link and then click the **New Connections** icon.
5. In the **Name** field, enter the user name: `Atlas_rptuser` (this entry is case-sensitive). Then, click **Next**.
6. In the **Type**, list, select **Oracle**. Then, click **Next**.
7. In the **SQL *Net Connect String** field, enter the name of your ATLAS database as registered in Oracle TNS Names. See the file called `tnsnames.ora` in the following directory:<*ORACLE install*>`\products\ 11.1.0\db_1\NETWORK\ADMIN .`

8. In the **User ID** field, enter PSSRTPUSER.
9. In the **Password** field, enter the password for user PSSRTPUSER and click **Next**.
10. Click **Finish**.

Importing the sample package of reports

As part of the integration process, you must import the sample package of reports into the Cognos Business Intelligence environment.

Procedure

To import the sample package:

1. Click **Content Administration** and select **Sample Cognos report for Atlas**.
2. Click the **Data Source Connection** link and then click the **New Import** icon to import the package.
3. In the **Name** field, enter the user name Atlas_rptuser. The name is case sensitive.
4. Click **Next** and then click **Next** again.
5. Select **SampleReportsForAtlas** and click **Next**.
6. Click **Next** in the next several windows.
7. Click **Save and run once** and then click **Finish** .

Rendering the sample reports in IBM Cognos Business Intelligence

Render the sample reports in IBM Cognos Business Intelligence to validate the configuration in the Cognos environment.

Procedure

To render the sample reports:

1. Click the **Home** icon and then click the **Public Folders** tab.
2. Click the public folder named **SampleReportsForAtlas**. Two reports are displayed: Sample Organization Details Report and Sample Person Organization Details Report.
3. Click **Sample Organization Details Report** to render the sample report.

Installing the custom authentication module

By using the custom authentication module, users can access Cognos reports from Atlas and report designers can design Cognos reports with Cognos modules.

Procedure

To install the authentication module:

1. Open the IBM Cognos Business Intelligence Configuration window by clicking **Start** > **All Programs** > **IBM Cognos 10** > **IBM Cognos Configuration**.
2. Expand the **Security** option in the left window. Then, under **Authentication**, select **Cognos**.
3. Set the value for **Allow anonymous access** to **False**.
4. Configure a namespace that is called propertyFileAuthentication by right-clicking **Authentication** and selecting **New resource** > **Namespace**.

5. In the **Name** field, enter `propertyFileAuthentication`.
6. Select **Custom Java Provider** for the **Type** and click **OK**.
7. Click the **propertyFileAuthentication** namespace and ensure that you use the following values:

Name	Value
NamespaceID	propertyFileAuthentication
Java class name	com.ibm.atlas.cognos.util.CognosPropertyFileAuthentication
Selectable for authentication?	True

   Use this namespace to log in directly to Cognos services by using following credentials:
   - **Userid**: `atlas`
   - **password**: `atlas`
8. Click the **PAReports** namespace and ensure that you use the following values:

Name	Value
NamespaceID	PAReports
Java class name	com.ibm.atlas.cognos.util.CognosTrustedSignOnHelper
Selectable for authentication?	True

9. Click **Actions** > **Stop** to stop the Cognos server. Then, close the IBM Cognos Business Intelligence Configuration window.
10. Copy the `\release\Atlas\AddOns\cognos\Jarfile\AtlasCognosAuthentication.jar` files to the `\ibm\cognos\c10\webapps\p2pd\WEB-INF\lib` folder.
11. Copy the `\release\Atlas\AddOns\cognos\properties\authenticationthrufile.txt` file to the `\ibm\cognos\c10\configuration` folder.
12. Copy the `\release\Atlas\AddOns\cognos\properties\cognos_access_credentials.properties` file to the `\ibm\cognos\c10\webapps\p2pd\WEB-INF\lib` folder.
13. Edit these parameters in the `cognos_access_credentials.properties` file with your policyAtlas server name and port:
    - **`SESSION_VALIDATION_URL`**=`http://`*policyAtlas_servername*:*policyAtlas_port*`/PolicyAtlas/srsbs?oper=SessionAndReportInformation`
14. Edit the `cognos_access_credential.properties` file to change the runtime mode to *Standalone*.
    - **`REPORT_RUNTIME_MODE`**=*Standalone*

    Standalone and Integration are the two supported modes. Integrated mode requires a valid session of PolicyAtlas to view the report although Standalone does not require a valid session.
15. Open the Cognos configuration by clicking **Start** > **All Programs** > **IBM Cognos 10** > **IBM Cognos Configuration**.
16. Click **Actions** > **Start** to start the Cognos server.
17. When the Cognos server starts, note the green check mark next to the messages, for example:

```
Testing "propertyFileAuthentication" namespace.
Testing "PAReports" namespace.
```

Configuring Atlas for Cognos reporting

This configuration will capture the Cognos setup details to invoke Cognos reports from Atlas.

About this task

Configure Atlas to connect to your Cognos deployment.

Procedure

To configure the integrated authentication mode:

1. Start the Policy Atlas interface at `http://your server:port/PolicyAtlas`.
2. Click the **Admin** link to enter the administrative user interface.
3. Under **Configuration**, click the **Components** link.
4. In the **Title** field, enter `COGNOS_REPORTING` and click **Search**.
5. Click the **COGNOS_REPORTING** component link.
6. Click **Edit** the populate **Parameter** fields to match the values in the table:

Parameter	Value
BASE_URL	Enter the URL for your Cognos server: `http://your cognos server:your cognos port/ibmcognos/cgi-bin/cognos.cgi`.
NAMESPACE	PAReports

7. Click **Save and Close**.

Registering the reports

As part of the integration process, register the sample reports in Atlas.

Procedure

1. Start the Policy Atlas interface at `http://your server:port/PolicyAtlas`.
2. Click the **Admin** link to enter the administrative user interface.
3. Under **Reports**, click the **Manage Reports** link.
4. On the **Reports** page, click **New Report**.
5. On the **Create Report** page, populate the fields with the values in the following table.

Field	Value
Report Name	`Sample Organization Details Report` **Important:** The name must be the exact name of the report as configured in Cognos.
Group Name	`Leave at default`
Security Role	`Leave at default`
Status	`Active`
Report Type	`COGNOS`
Report Formats	`HTML`
Report Class Name	`Sample Organization Details Report`
Source Type	`Package`

Field	Value
Source	`SampleReportsForAtlas` **Important:** The name must be the exact name of the package as configured in Cognos.

For the source type, note the following conditions:

- If the Source Type for the report is a folder, select the **Folder** radio button and specify `F1/F2/F3` as the path of the report.
- If the report is configured under a package that is called P1 but under folders `F1/F2/F3`, select the **Package** radio button for the Source Type and specify `P1/F1/F2/F3` as the path of the report.
- If the report is configured under a package that is named `P1` but under another package named `P2` and under folders `F1/F2/F3`, select the **Package** radio button for the Source Type and specify `P1//P2/F1/F2/F3` as the path of the report.
- Use a forward slash (`/`) to represent a folder and two forward slashes (`//`) to represent a package.
- You do not need to specify a forward slash (`/`) or two forward slashes (`//`) at the beginning of the path. The selection for the source type is sufficient.

6. Click **Save and Close**.
7. Repeat the previous steps but enter `Sample Person Organization Details Report` in the **Report Name** field. Leave all other fields the same as for the first report that you created.

Rendering the reports in Atlas

To validate the integration and view the sample reports, render a report in Atlas.

Procedure

To render the reports:

1. Click the **Reports** tab. See the two new reports under the **Cognos Reports** heading.
2. Click the **Sample Organization Details Report**.
3. Click **View Now** to render the sample report.
4. Go back to the **Reports** tab and click **Sample Person Organization Details Report** to render the sample report.

   Tip: To create a report in Cognos Report Studio, see this document and supporting information in the IBM Cognos Business Intelligence Information Center: Example - Create a Report.

Modifying passwords in the configuration files

About this task

To ensure secure access to the sample package and reports from the Cognos user interface, a namespace that is called **propertyFileAuthentication** is configured in the chapter that is titled, *Installing the custom authentication module*. During the login process, this namespace prompts for a user ID and password to log in to the

Cognos administration interface. By default the user name and password is *atlas* and *atlas* respectively. The passwords are encrypted and stored in the following configuration files:

- `authenticationthrufile.txt`
- `cognos_access_credentials.properties`

A utility is included in this Fix Pack to generate a new encrypted password to replace the default password. After the new encrypted password is generated, you must manually edit the `authenticationthrufile.txt` and `cognos_access_credentials.properties` files to replace the default password.

Procedure

1. `cd` to the folder `..\release\Atlas\AddOns\cognos\properties`
2. Run the batch file with the **<new password>** parameter to generate a new encrypted password: `GenerateEncyptedText.bat` **<new password>**

   The output from the utility when it is generating a new password "test" looks similar to this output:

   ```
   Encrypted text of the string
   [test] is [$2$fChqs5SjwH8~$tOrgZRxcIYAwOWPTduBYPUVslmSdjT_mhdTnXsKmmfA~]
   "Manually populate the encrypted password in the two property files
   (authenticationthrufile.txt and cognos_access_credentials.properties)."
   ```

   The new encrypted password is `$2$fChqs5SjwH8~$tOrgZRxcIYAwOWPTduBYPUVslmSdjT_mhdTnXsKmmfA~`
3. Edit the `...\ibm\cognos\c10\configuration\authenticationthrufile.txt` file and replace the default password with the new password

   Refer to the line that corresponds to the user and replace the existing encrypted password with the one generated utility.In this example it is the line,

   ```
   user:60:Atlas:User:atlas@us.ib.com:atlas:
   ```

   ```
   // User Database for single organization CJAP
   //

   // Users
   //
   // For Adding a New User:
   // (1) At least one role should be assigned to make the user visible and function correctly
   // (2) Add the user to the 'Users' folder below

   user:40:Test:User A:usera@us.ibm.com:usera:usera
   user:50:Test:User B:userb@us.ibm.com:userb:userb
   user:60:Atlas:User:atlas@us.ib.com:atlas:$2$fChqs5SjwH8~$tOrgZRxcIYAwOWPTduBYPUVslmSdj
   T_mhdTnXsKmmfA~
   ```
4. Edit the `...\ibm\cognos\c10\webapps\p2pd\WEB-INF\lib\cognos_access_credentials.properties` file and replace the default password with the new password.

   Refer to the line that corresponds to the user and replace the existing encrypted password with the one generated by the utility. In this example it is the line,

   ```
   PASSWORD=$2$fChqs5SjwH8~$tOrgZRxcIYAwOWPTduBYPUVslmSdjT_mhdTnXsKmmfA~
   ```

   ```
   # property authentication details
   USER_NAME=atlas
   PASSWORD=$2$fChqs5SjwH8~$tOrgZRxcIYAwOWPTduBYPUVslmSdjT_mhdTnXsKmmfA~
   USER_AUTHENTICATION_NAMESPACE=propertyFileAuthentication
   ```
5. When the property files are updated and saved, restart the Cognos server.

6. Verify the password change by logging in to the Cognos user interface at `http://cognos_server/ibmcognos/`, selecting the namespace that is called **propertyFileAuthentication** and providing the user name and new password to authenticate.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2011.

Product Number: 5725-D75, 5725-D76, 5725-D77