IBM Security Identity Manager v6.0.0 Fix Pack 4 Installation and Configuration

Before you begin

Before you install the fix pack, note the following changes.

If you have installed fix pack 3 already, the changes for fix pack 4 are in blue characters in this document.

IBM Security Identity Manager Service Center considerations

If you use the IBM Security Identity Manager Service Center that was shipped in Fix Pack 6.0.0.3 note that with the installation of Fix Pack 6.0.0.4, the Service Center will display only activities created after the installation of the 6.0.0.4 fix pack. If an activity was created prior to Fix Pack 6.0.0.4 and was still pending when you upgraded to Fix Pack 6.0.0.4, the activity will not appear in the IBM Security Identity Manager Service Center. To complete that activity, you must to log into the IBM Security Identity Manager Service Center or the IBM Security Identity Manager Administration Console.

Workflow Notification Properties update

You can use the Workflow Notification Properties page to manually add information about canceling a request to the email notification template. When you install the IBM Security Identity Manager Fix Pack 6.0.0.4, the email notification template content that includes information about canceling a request is not automatically applied.
The template changes that are available with Fix Pack 6.0.0.4 are not automatically applied to avoid having the installation process overwriting any custom changes that you might have made to the email templates. For information about manually updating the email notification template, see the IBM Knowledge Center.

Enterprise Business Asset properties considerations

If you previously installed the IBM Security Identity Manager v6.0 Identity Service Center for fix pack 3 and also customized the associated Enterprise Business Asset (also known as an eba), those changes are lost when you install fix pack 4.
For example, if you have an http server in place, you might have configured the Enterprise Business Asset to use the server. Map the Identity Service Center log to the WebSphere Application Server console with these steps:

1. In the task menu, click **Applications > Application Types > Business level applications**.
2. In the applications list, click **IdentityServiceCenterApplication**.
3. Click **com.ibm.isim_CU.eba**.
4. On the next panel, click **Modify Targets**.
   a) Select the appropriate Web server from the available box.
   b) Click the arrow icon to add the Web server to the selected box.
   c) Click **OK**.
   d) In the message box, click **Save configuration**.

Installing the fix pack replaces the Enterprise Business Asset and removes the changes in the previous example. To prevent the loss:

1. Make a record of any customizations that you had made to the Enterprise Business Asset prior to installing the fix pack.

2. Reapply the changes after you install the fix pack.

Oracle, Sun and other operating system considerations

If you select to install the IBM Security Identity Manager v6.0 Identity Service Center, on your Oracle/Sun supporting operating system, you must install the IBM Security Identity Manager v6.0 fix pack 4. During deployment of the new Identity Service Center Enterprise Business Asset (for example, WebSphere EBA), you might experience an abnormally long wait and eventual time out or out right failure during the time the EBA is deployed. This happens due to insufficient memory in the WebSphere Application Server. Check the application server logs for the following error:

java.lang.OutOfMemoryError: PermGen space

To correct this issue, change the properties of the WebSphere Application Server startup profile to increase the MaxPermSize. Oracle and Sun environments, require a value of at least 512m. If it fails to prevent the problem, you can increase the value in increments of 256m, depending upon system resources, until the problem no longer occurs. To increase the memory limit in WebSphere Application Server, follow these steps:

- In the WebSphere Application Server administrative console, navigate to **WebSphere application servers > server_name > Java and Process Management > Process definition > Java Virtual Machines**.
- In the **Generic JVM arguments** field, append the following parameter: -XX:MaxPermSize=512m
- Save your changes and restart the WebSphere Application Server instance.
- For clustered installations, repeat these changes for each node in the cluster.

Service Center functionality does not support Oracle 10gR2

The Request Access function in the Service Center UI does not work with Oracle 10gR2. If you use Oracle 10gR2 errors such as the following are displayed in the logs:

> ORA-32036: unsupported case for inlining of query name in WITH clause. If you are using Oracle as your database, ensure you are running with 11gR2 prior to installing the Service Center functionality. Please note that Oracle has dropped support of 10gR2 as of July 2013.

Cluster node considerations

Before starting fix pack Installation on cluster:

- Ensure that Business Level Application “IdentityServiceCenterApplication” is in a stopped state.
- Ensure that all node agents are running and can communicate with the Network Deployment Manager.
- Ensure that each IBM Security Identity Manager cluster is stopped.
  - Application cluster
  - Messaging cluster
- If the Deployment Manager node and a cluster member are in the same host, perform this procedure only once. Stop WebSphere using your normal procedures, For example,

  ```
  $WAS_HOME/profiles/AppSrv01/bin/stopServer.sh server1
  ```

  or, if you want to submit userid and password when WAS admin security is used:

  ```
  $WAS_HOME/profiles/AppSrv01/bin/stopServer.sh server1 -username xxxx -password yyyy
  ```

then proceed to next step, only after the stop confirmation is displayed.

- **Note**: Perform the procedure first on the NDM and then on every node in the cluster.

Cognos Reporting

This fix pack installs new Cognos Reports and Models which can be found in the following locations. To use these new reports and models, see the supplied Cognos Reporting documentation.

You can find the models and reports specific to Security Identity Manager are located at:

- <itim_home>/extensions/6.0/Cognos/Model/ISIMReportingModel_6.0 – ISIM model files
- <itim_home>/extensions/6.0/Cognos/Reports/ISIMReportingPackage_6.0.0.FP#.zip – ISIM report files. Where, FP# is the number of the fix pack.

This fix pack provides the following additional support:

- New User Access reports
- Enhancement to the IBM Security Identity Manager dashboard

If Shared Access Enablement is enabled for IBM Privileged Security Identity Manager, the models and reports are no longer delivered with IBM Security Identity Manager fix packs. Support for Shared Access Reports will be made available to the customer with the IBM Privileged Security Identity Manager Reporting package from Passport Advantage.

Customizable File considerations

The following file considerations regarding customizations to files in the <ITIM_HOME>/data directory are noted.

XML files that are now automatically merged

If the user has made modifications to files in the <ITIM_HOME>/data directory, this fix pack preserves the following additional xml settings during the upgrade process:

- workflowDataSyntax.xml
- workflowextensions.xml

Properties file updates requiring manual intervention

In this fix pack, manual updates are required to the following files for the product to function properly:

- **enroleHiddenAttributes.properties**
  - the current GA value of the key 'allowed' has the following value:

    # Attributes not protected by ACIs (to allow read by public API)

    allowed=erparent,erhistoricalpassword,erpersonstatus,eraccountstatus,erorgstatus,erbporgstatus,eraccountcompliance,erservice,erowner,erscope,erglobalid,objectclass,ernoncomplianceaction,erdraft,eraccessname,erobjectprofilename,erlastrecertificationaction,erlastrecertificationactiondate,eraccesslastcertifieddate,eraccessrecertificationlastaction,eraccessrecertificationlastactiondate,errolerecertificationlastaction,errolerecertificationlastactiondate,eraccountownershiptype,eraccount,ercvcatalog,erlessee,ercredentialpooldn,erleasestatus

- Add the new values that are highlighted in red.

  # Attributes not protected by ACIs (to allow read by public API)

  allowed=erparent,erhistoricalpassword,erpersonstatus,eraccountstatus,erorgstatus,erbporgstatus,eraccountcompliance,erservice,erowner,erscope,erglobalid,objectclass,ernoncomplianceaction,erdraft,eraccessname,erobjectprofilename,erlastrecertificationaction,erlastrecertificationactiondate,eraccesslastcertifieddate,eraccessrecertificationlastaction,eraccessrecertificationlastactiondate,errolerecertificationlastaction,errolerecertificationlastactiondate,eraccountownershiptype,eraccount,ercvcatalog,erlessee,ercredentialpooldn,erleasestatus,***ercvserviceuri,eraccesscategory,eraccesstag,eradditionalinformation,erbadge,erimageuri,erserviceinfo,ercheckpolicy***

Setting the SOAP timeout interval before fix pack installation

Installing fix packs requires a sufficient time interval to avoid time out exceptions. If you will install the Identity Service Center then this section overrides the same section in the on-line documentation.

Before you begin

To avoid timeout exception errors during fix pack installation, before every fix pack installation, set the SOAP timeout interval to at least 15 minutes (900 seconds).

Note: If you are going to install the Identity Service Center or the aforementioned setting does not work, you might have to set the value to 0, to specify an unlimited timeout interval, and reinstall the fix pack.

Procedure

1. Edit the soap.client.props file. This file is in the WAS_HOME\profiles\profile_name\properties directory.
2. Set the com.ibm.SOAP.requestTimeout property to 0. For example,

   com.ibm.SOAP.requestTimeout=0
3. Save the changes to the file.

What to do next

Install the fix pack if applicable.

Fix pack Installation

Before you begin

You must use the WebSphere Update Installer Version v7.0.0.27 or newer. You can download the latest version and get more information about the WebSphere Update Installer at:
http://www.ibm.com/support/docview.wss?rs=180&uid=swg24020212

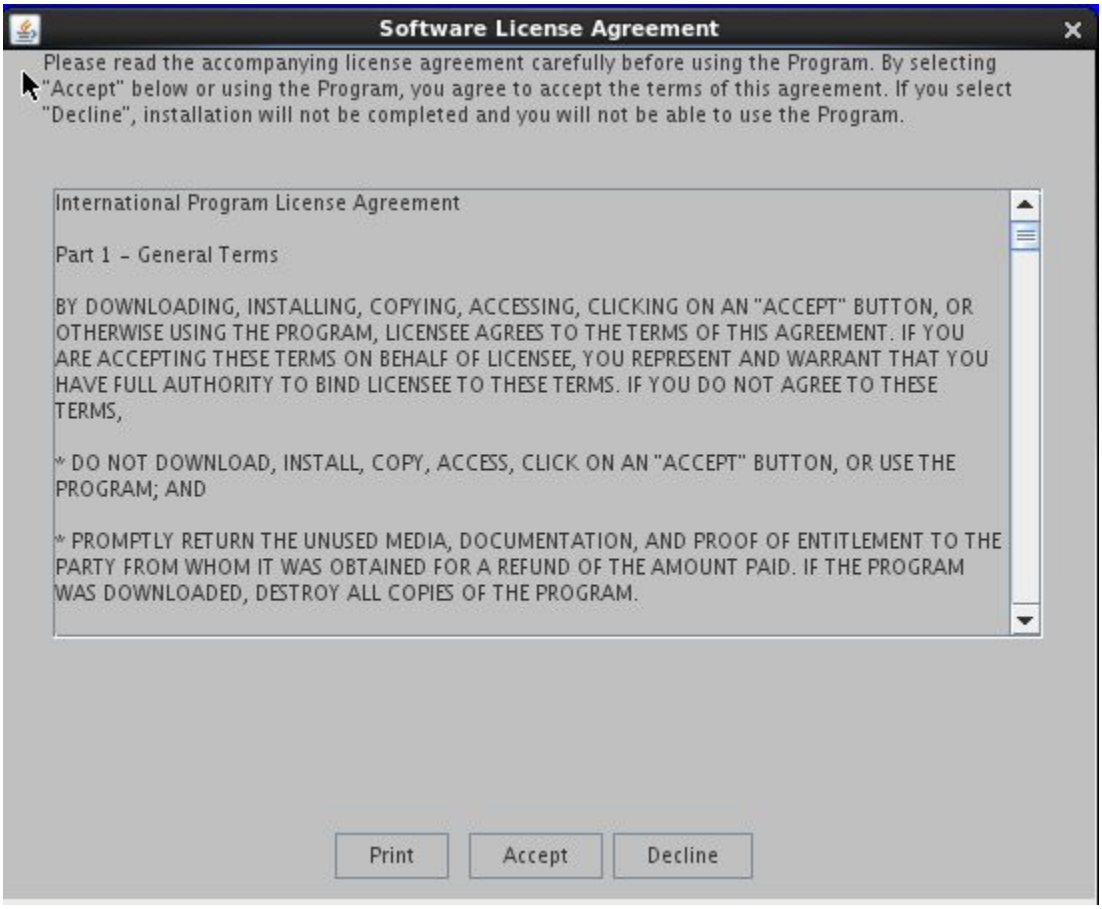
Procedure

To start the WebSphere Update Installation for the IBM Security Identity Manager, follow these steps:

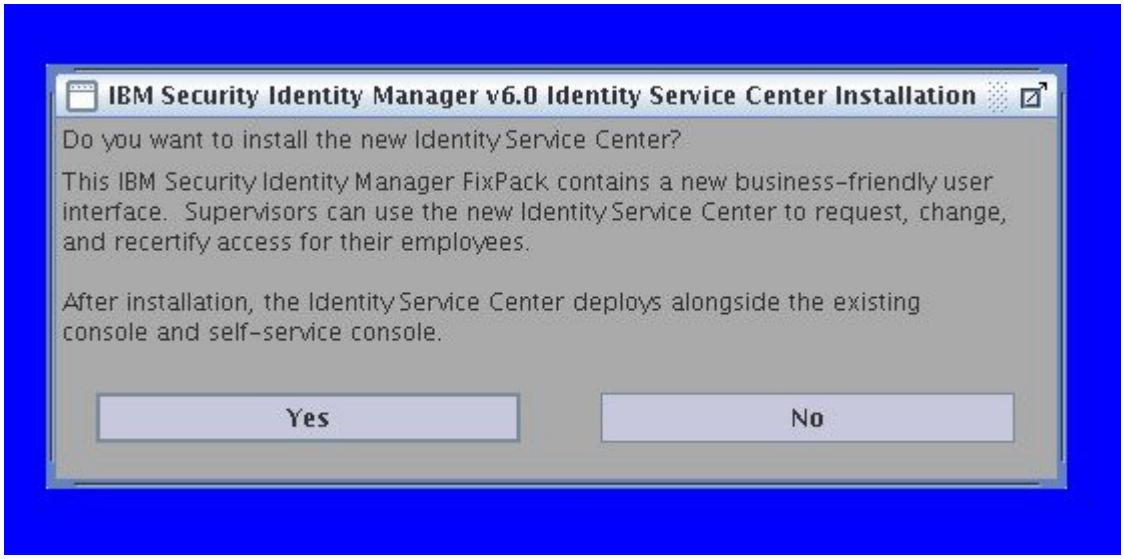
1. Run the WebSphere Update Installer. For example,
   On UNIX or Linus operating systems:
   /opt/IBM/WebSphere/UpdateInstaller/update.sh
   On Windows operating systems:
   C:\Program Files\IBM\WebSphere\UpdateInstaller\update.bat

2. When the update installer asks for Product Selection, specify your ISIM_HOME directory, typically
   On UNIX or Linus operating systems:
   /opt/IBM/isim
   On Windows operating systems:
   C:\Program Files\IBM\isim

3. Enter the directory path or click **Browse** to navigate to the ISIM installation directory. Then click **Next**.
4. The update installer asks for the Maintenance Operation Selection. Select **Install Maintenance Package.** and click Next
5. The update installer prompts for the Maintenance Package Directory Selection. This is the directory that you downloaded the *.pak file to. Enter the directory or click **Browse** to navigate to the ISIM installation directory. Click **Next**.
6. The update installer locates the available maintenance packages and automatically selects the most appropriate one to install. Click **Next**.
7. The update installer performs some basic prerequisite checks. For example, it checks to ensure that the WebSphere Application Server is stopped. If it is not stopped, the installer displays a warning message. When all checks are complete, click **Next**.
8. The update installer displays an installation summary panel, click next to continue.
9. The update installer displays some status information about what steps it is performing during the installation.
10. A new license agreement is displayed. By accepting the new license the product update continues and the fix pack is installed. By not accepting the new license terms you are prompted to acknowledge your decision, Click **Yes** to terminate the update process, Click **No** to return you to the previous panel to change your answer.

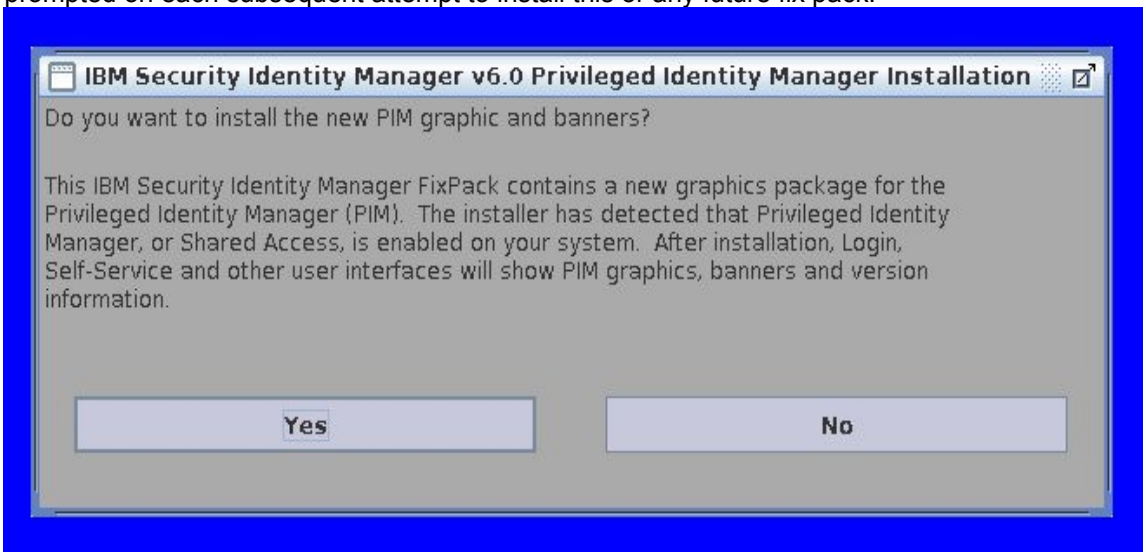


11. If you accept the license, or accepted it during a previous install attempt, then you are prompted to install the Identity Service Center function. Click **Yes** to install and enable the function. If you click **No**, you will be prompted on each subsequent attempt to install this or any future fix pack.



Note: The Identity Service Center does not support Microsoft SQL Server database. If you are using this database product you do not see this prompt or dialog. Use a DB2 database or an Oracle database instead.

12. The installation continues and the installer checks whether Shared Access (Privileged Identity Manager or PIM) is installed and enabled. If you do,the installer prompts you to install the new Privileged Identity Manager graphic package and logos. Whether you choose to install them or not, you will not be re-prompted on each subsequent attempt to install this or any future fix pack.



13. After the Maintenance Installation is complete, you may exit the Update Installer.
14. A WebSphere Single Server environment is automatically restarted during the update process. For a clustered environment use normal startup procedures to restart the clusters.

Fix pack Post Installation

Merge customization files

After the installation of the Fix Pack, you must merge new and existing customization files. See the instructions for " Merging new and existing customized configuration files" in the IBM Knowledge Center at http://www.ibm.com/support/knowledgecenter/SSRMWJ_6.0.0.4/com.ibm.isim.doc_6.0.0.4/configuring/tsk/tsk_ui_merge_custom_config_files.htm

Utility for access catalog data synchronization

The access catalog data synchronization utility is a separately installed utility that synchronizes data and access control items between the LDAP server and the IBM Security Identity Manager database. The synchronized data is used to search an existing access catalog and to resynchronize data between LDAP and the database.

Note:

- The fix pack installer installs the utility only if you select to enable the Identity Service Center during fix pack installation.
- You must run this utility after you select to enable the Identity Service Center during fix pack installation.
- In a Single Server configuration
  - You must run the utility on the server containing the IBM Security Identity Manager.
- In a Clustered Server configuration
  - You must run this utility on the server containing the Deployment Manager.

Running the access catalog data synchronization utility

You can start the access catalog data synchronization process.

Before you begin

Before you run the utility command, stop Identify Manager applications.

From WebSphere Administrative Console

- Click **Applications>Application Types>Business level applications.**
- Select **ITIM** and **IdentityServiceCenterApplication.**
- Click **Stop.**

You must also set required variables in the syncISIMData script.

Set values for required variables ITIM_HOME, JAVA_HOME and JDBC_DRIVER. For example:

On Unix and Linux operating systems

```
export ITIM_HOME=/opt/IBM/isim
export JAVA_HOME=/opt/IBM/WebSphere/AppServer/java
export JDBC_DRIVER=/opt/IBM/isim/lib/db2jcc.jar
```

On Windows operating systems

At a command prompt in the drive:\IBM\isim\bin\win directory:

```
set ITIM_HOME=C:\IBM\isim
```

set JAVA_HOME=C:\IBM\WebSphere\AppServer\java
set JDBC_DRIVER=C:\IBM\isim\lib\ojdbc.jar;C:\IBM\isim\lib\sqljdbc.jar
Note:

- The JDBC_DRIVER path in this example is for Oracle.
- The JDBC_DRIVER environment variable is the full-path to database driver installed for the IBM Identity Security Manager. If you are not sure what the full-path is ask your WebSphere Administrator for the value of the ITIM_DB_JDBC_DRIVER_PATH environment variable setting. This path will contain the db2jcc.jar for DB2 or the ojdbc.jar for Oracle.
- For DB2, the driver path includes several different files. For example, a JDBC_DRIVER statement might be:
  set
  JDBC_DRIVER=C:\IBM\isim\lib\db2jcc.jar;C:\IBM\isim\lib\db2jcc_license_cu.jar;C:\IBM\isim\lib\db2jcc_license_cisuz.jar
- You can locate the JAR files in the /lib directory in the IBM Security Identity Manager installation home directory.
- To specify a directory that contains spaces, enclose the path in double quotation marks. For example:

  set JAVA_HOME="c:\program files (x86)\ibm\websphere\appserver\java"

Where

ITIM_HOME
: Specifies the IBM Security Identity Manager installation home directory.

JAVA_HOME
: Java home directory

JDBC_DRIVER
: The JDBC driver path that the data synchronization utility uses to access the IBM Security Identity Manager database.

Procedure

1. Navigate to one of these directories:

   On UNIX and Linux operating systems
   ISIM_HOME/bin/unix

   On Windows operating systems
   ISIM_HOME\bin\win

2. Run one of the following commands:

   On UNIX and Linux operating systems
   syncISIMData.sh [-syncOption value] [-dataType value]
   For example,
   syncISIMData.sh -syncOption Maintenance -dataType AccessCatalog

   On Windows operating systems
   syncISIMData.cmd [-syncOption value] [-dataType value]
   For example,
   syncISIMData.cmd -syncOption Maintenance -dataType AccessCatalog

   Where:

   -syncOption
   Required. Values are: Upgrade or Maintenance.
   Upgrade

Specify this option when you have existing data on IBM Security Identity Manager version 6.0, you apply the fix pack, and you enable the Identity Service Center.

Maintenance

Select this option to resynchronize data when the connection to the database is lost during a data transaction.

Examples of loss can occur because of network failure, WebSphere Application Server failure, or an unavailable database.

-dataType

Required. Values are ConfigData , AccessCatalog , or ALL.

ConfigData

Default configuration data such as group profiles, organization, service (ISIM service), provisioning policy, and global settings.

AccessCatalog

Access catalog data such as role access, group access, service, and provisioning policy.

ALL

Data that is described by ConfigData , AccessCatalog values.

What to do next

Start Identify Manager applications. From the WebSphere Administrative Console

- Click Applications>Application Types>Business level applications
- Select ITIM and IdentityServiceCenterApplication
- Click Start.

If you encounter a problem when you run the report data synchronization utility, see the syncISIMData.log file. This log file is in the ISIM_HOME directory.

Note: Additional, ignorable messages can occur in sysout. No action is required on your part. For example:

Oct 2, 2013 2:35:58 PM com.ibm.ws.util.ImplFactory

WARNING: WSVR0072W

Oct 2, 2013 2:35:59 PM com.ibm.ws.ssl.config.SSLConfigManager

INFO: ssl.disable.url.hostname.verification.CWPKI0027I

Oct 2, 2013 2:36:01 PM com.ibm.ws.security.config.SecurityObjectLocator

INFO: Client code attempting to load security configuration

Oct 2, 2013 2:36:01 PM com.ibm.ws.security.config.ConfigURLProperties

SEVERE: security.JSAS1480I

Oct 2, 2013 2:36:02 PM com.ibm.ws.security.config.SecurityObjectLocator

INFO: Client code attempting to load security configuration

Utility for changing system cipher

There is a modification to the change Cipher command that must be made before the command can be run successfully. The scripts that were shipped with the GA version of the product omit a setting for ITIM_HOME, that must be added.

Before you begin

Before you run the utility command, you must set a required variable in the changeCipher script.

Set the proper value for the required variable ITIM_HOME. For example:

On UNIX and Linux operating systems

1. Edit the <ITIM_HOME>/bin/unix/changeCipher.sh file
2. Add a line containing the following before the JAVA_HOME setting:
   ITIM_HOME=/opt/IBM/isim

On Windowsoperating systems

1. Edit the <ITIM_HOME>\bin\win\changeCipher.sh file
2. Add a line containing the following before the JAVA_HOME setting: ITIM_HOME=/opt/IBM/isim

   ITIM_HOME=C:\Program Files (x86)\IBM\isim

The change looks something like the following example on a Linux system.

ITIM_LIB Shared Library

The ITIM_LIB Shared Library for IBM Security Identity Manager must be updated before using the product to ensure that the license function within the product performs correctly. Perform one of the following tasks. It is suggested that you manually add the Jar file by using the WebSphere Console, because re-running the configuration utility might take a long time.

1. To manually add the license_metric_logger_1.0.0.201310151701.jar file to the ITIM_LIB shared lib path using the WebSphere Console do the following.
   (a) Open the WebSphere Console
   (b) On the left hand Task Panel find and click **Environment** to expand the menu.
   (c) Click **Shared Libraries.** The Shared Libraries panel is displayed.
   (d) On the Shared Libraries page, click **ITIM_LIB**. The Configuration, General Properties panel for ITIM_LIB is displayed.
   (e) In the **Classpath** field add ${ITIM_HOME}/lib/license_metric_logger_1.0.0.201310151701.jar to the end of the list.
   (f) Click **Apply**.
   (g) Click **OK**.
   (h) You are returned to the Shared Libraries page.
   (i) At top of page, click **Save**.
   (j) Restart WebSphere.

2. Run the **runConfig** utility to automatically add the jar file to the ITIM_LIB shared lib path.
   (a) Go to <ISIM_HOME>/bin directory.
   (b) Run the **runConfig** utility with the installation option. This process might take a long time.
      - On UNIX or Linux operating systems:
        # runConfig install

(c) On the configuration tool pop-up window, you can either verify your configuration or continue to the next step.
(d) Click **OK**.
(e) Wait for the utility to finish.
(f) Restart WebSphere.

Context Root For Form Login

For those installations that are using custom domains or global security, the user must manually enter the security property, com.ibm.websphere.security.setContextRootForFormLogin. For your specific configuration this property must be set to 'true',

If you are using the default ISIMSecurityDomain in WebSphere, then this property is automatically set to 'true' for you.

If you are using a Custom Security Domain or global security, then a pop-up dialog displays during the fix pack installation. This dialog indicates that the installer is unable to automatically set the property.

To manually set this property, follow these steps.

1. Open the WebSphere Application Server administrative console and expand the security tab.
2. If you have defined a custom security domain, click the security domains link then select your custom domain.
3. If you are using global security, click the global security link.
4. Click the custom properties link.
5. Click **New**.
6. Enter 'com.ibm.websphere.security.setContextRootForFormLogin' in the Name field and 'true' in the value field.
7. Click OK.
8. Restart your application server for changes to take effect.

Reinitialize authentication with an external user registry

If you have migrated your IBM Security Identity Manager Version 6.0 installation from WebSphere Application Server Version 7 to Version 8.5 by using the migration procedure that is described in the IBM Knowledge Center and had an external user registry configured, you must reinitialize it. After migrating your existing IBM Security Identity Manager Version 6.0 from WebSphere Version 7 to a WebSphere Version 8.5 environment, the external user registry is reset back to ISIM security. In order to reconfigure your system so that it uses the external user registry, you must re-run the procedure already documented in the IBM Knowledge Center **Security Products >IBM Security Identity Manager, Version 6.0>Installing>*Reconfiguration for authentication with an external user registry>Reconfiguration of a WebSphere security domain.***

Shared Account Workflow Extension

If you have "Shared Account workflow extension" which was added for Privileged Identity Manager, the fix pack installer will remove this custom update during the re-application of the ITIM.ear.

The problem may manifest itself around the ChangePasswordWithTAMESSO and when it tries to execute a library in encentuate.bridges.wfe.EncentuateCltAppExtension. An error will be thrown in the trace.log file indicating that ISIM could not find the EncentuateCltAppExtension. To correct this issue:

1. Navigate to:

   <*WEBSPHERE_HOME*>/AppServer/profiles/<*SERVER_NAME*>/installedApps/<*NODE_NAME*>/ITIM.ear/app_web.war/WEB-INF/

2. If there is no lib directory, create it.
3. Copy the workflow extension, from:

   <your_installer_directory>/adapter_isamesso_6.0.1/SAMESSOwfe.jar

   to the lib directory created in the previous step:

   <*WEBSPHERE_HOME*>/AppServer/profiles/<*SERVER_NAME*>/installedApps/<*NODE_NAME*>/ITIM.ear/app_web.war/WEB-INF/lib
4. Restart your WebSphere Application Server.

Integration between IBM Security Identity Manager and IBM Security Identity Governance

A connector is provided to allow access to IBM Security Identity Governance from IBM Security Identity Manager. The connector must be installed and configured separately. For instructions and further documentation, see technote 1688802 at http://www.ibm.com/support/docview.wss?uid=swg21688802.