Oracle® Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety

Installation Guide for On-Premise Deployment

Release 1.0.2

E49877-01

December 2013

ORACLE®

Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Installation Guide for On-Premise Deployment, Release 1.0.2

E49877-01

Contents

Preface

This guide provides information on how to install the Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety (Adverse Event: InForm and Argus Safety).

Audience

The audience for this installation guide is database administrators (DBAs) and system administrators installing the integration. If you want assistance with your installation, engage Oracle Consulting.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documentation sets:

Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety

- *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Installation Guide Release 1.0.2 [this document]*
- *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Implementation Guide Release 1.0.2*
- *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Security Guide Release 1.0.2*

Oracle Application Integration Architecture

- *Oracle Fusion Middleware Concepts and Technologies Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6)*

- *Oracle Fusion Middleware Developer's Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6)*
- *Oracle Fusion Middleware Getting Started and Demo Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6)*
- *Oracle Fusion Middleware Infrastructure Components and Utilities User's Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6)*
- *Oracle Fusion Middleware Installation and Upgrade Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6)*
- *Oracle Fusion Middleware Reference Process Models User's Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6)*
- *Oracle Fusion Middleware Product to Guide Index for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6)*
- *Oracle Fusion Middleware Migration Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6)*

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, 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.

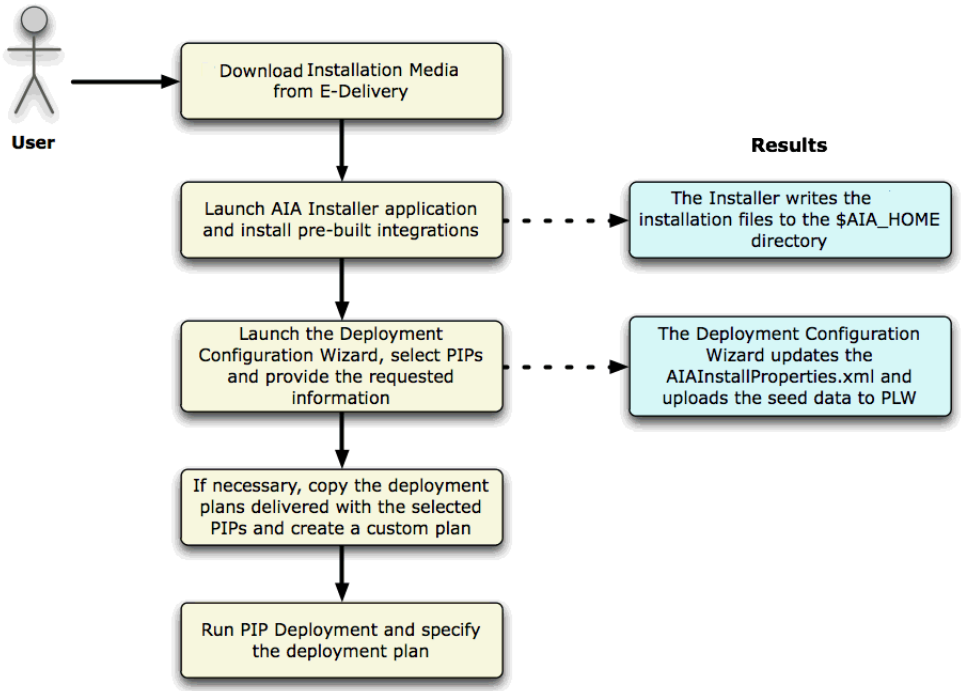
1

Pre-built Integration Installation

The Adverse Event: InForm and Argus Safety integration installation consists of three stages:

- Installation
- Configuration
- Deployment

Figure 1–1 Illustrates the Flow of the Pre-built Integration Installation



The installer is built on Oracle Universal Installer (OUI). You use the installer to install and uninstall the integration. The installer is platform independent.

For information about system requirements and supported platforms for Oracle Application Integration Architecture Foundation Pack 11gR1, search for System Requirements and Supported Platforms for Oracle Application Integration Architecture Foundation Pack 11gR1 on http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html and download the xls file.

The Deployment Configuration Wizard (DCW) defines the configurations needed for each pre-built integration and guides you through the configuration. When you launch the DCW, you select the individual pre-built integrations to configure and enter the information required for the configuration.

For details about the DCW, see Chapter 2.

When your pre-built integration is configured, you run the pre-built integrations deployment and specify the deployment plan.

For more details about deployment, see Chapter 3.

2

Pre-built Integration Configuration

The integration Deployment Configuration Wizard (DCW) helps you configure the integration by prompting you for integration-specific information. This section discusses configuration options and the DCW screens.

- When you configure the integration over an existing configuration that has one or more integrations, if the new integration you select for configuration shares one or more participating applications with existing pre-built integrations, the common application information that is captured is shown to you. You can choose to change the captured information or keep it the same.

  For example, when the first run of the DCW configures integration1 and the second run tries to configure integration2, if integration2 shares a participating application (such as Argus Safety) with integration1, DCW shows the captured details and asks whether to overwrite them. If you choose not to overwrite, the details previously provided are retained.

2.1 Routing Rules Configuration in Enterprise Business Services

Every pre-built integration has its own set of routing rules. These routing rules are delivered when you install the integration. However, implementation of the routing rules can differ depending on the installation scenario.

When you deploy a single pre-built integration, the Enterprise Business Services (EBS) for that integration is deployed with the default routing rules.

For more information about using and extending routing rules, see *Oracle Enterprise Service Bus Developer's Guide*.

The routing rules for the InForm and Argus Safety integration are available in `AIA_HOME/pips/AEInFormandArgus/EBS`. The install log provides information about the EBS for which you need to configure routing rules.

For more information about how to use the default routing rules to design and implement your own integration routing rules and the associated integration configuration properties, see *Oracle Fusion Middleware Developer's Guide for Oracle Application Integration Architecture Foundation Pack*.

2.2 Installation, Configuration, and Deployment Topologies

Several installation and deployment topologies are possible using the installer. Choose the installation that best suits your needs. For details, see the AIA Installation and Deployment - Strategies, Topologies, and Flexibilities White Paper on `http://www.oracle.com/index.html`.

Only one instance of each participating application can participate in any direct or process integration when installed through the installer. However, after installing using the installer, you can configure pre-built integrations to connect to multiple instances. For details, see *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Implementation Guide*.

3

Pre-built Integration Deployment

The pre-built integration ships a main deployment plan, a supplementary deployment plan (optional), and a conditional policy file (optional). These files are passed as parameters to the AIA Install Driver (AID) for deployment.

In addition, AIAInstallProperties.xml is passed as a parameter to the AID for deployment.

You use the configuration wizard to configure AIAInstallProperties.xml with the pre-built integrations server details. The AID does not perform any checks to validate that AIAInstallProperties.xml has been configured with the corresponding pre-built integrations server details.

The AID retrieves the required property values from the install properties file and deploys the pre-built integrations.

3.1 Pre-built Integration Codeployment

Codeployment is also available among PIPs or Direct Integrations (DIs) when neither is part of a pre-built integration group. Before you install multiple PIPs or DIs on a single Service Oriented Architecture (SOA) instance, refer to My Oracle Support note 881206.1 to review the integration PIP Codeployment Matrix and check whether your PIP or DI combination is supported on a single instance.

To install multiple PIPs that do not support codeployment, you must install each PIP or DI on a separate SOA instance. Installing unsupported PIP or DI combinations on a single SOA instance may require custom changes to accommodate any resulting impact on common PIP or DI components, such as common routing rules.

3.2 Pre-built Integration Undeployment

PIPs are undeployed using undeployment plans. The undeployment plan and the configured AIAInstallProperties.xml file are passed as parameters to the AID for undeployment.

4

Prerequisites

Before you start the installation process, ensure the following:

SOA Patch:

- SOA Suite patch 14137846 and 14630316 are installed.

AIA Foundation Pack Installation:

- Install AIA Foundation Pack 11.1.1.6.0 before you install the Adverse Event: InForm and Argus Safety integration.

  For more information on how to install the AIA Foundation Pack, search for *Oracle® Fusion Middleware Installation and Upgrade Guide for Oracle Application Integration Architecture Foundation Pack* on the Oracle Technology Network (OTN) at `http://www.oracle.com/technetwork/middleware/foundation-pack/documentation/index.html` and download the latest version. This guide is constantly updated and bug fixed.

Back up Customizations:

- Take a backup of any customizations before installing the patch. If you do not take a backup, your customizations will be overwritten.

  For more information about backing up your customizations, see the section "Creating Backups of Your Customizations".

AIA Foundation Pack Patch:

- Install patch 17423167 on top of AIA Foundation Pack 11.1.1.6.

Argus File Structure:

- Create a file structure on the Argus Interchange server to enable file sharing.

  The following example provides information to create the folders and assign permissions to the folders to enable file sharing:

  Create a folder on the Argus ESM Server (for example, C:\ INF-ARG-INTEGRATION). The parent folder should have three sub folders named in, out, and ack-archive. The *in* folder is the parent folder for all E2B+ files. The *out* folder is the parent folder of all acknowledgement files. The *ack-archive* folder is the parent folder for the processed acknowledgement files.

  For a single-tenant Argus installation, you do not have to create a specific folder for each enterprise. The file structure is as follows:

  C: \INF-ARG-INTEGRATION

  - in
  - out

- ack-archive

For a multi-tenant Argus installation, there are sub-directories for each enterprise within each directory, as shown in the following example. In the example, ent<n> represents the enterprise short name. This value will also be entered in the HS_TRIAL_SAFETY_CONFIG DVM. For more information about HS_TRIAL_SAFETY_CONFIG DVM, see *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Implementation Guide*.

The file structure is as follows:

C: \INF-ARG-INTEGRATION

- in
  - ent1
  - ent2
  - ent3
- out
  - ent1
  - ent2
  - ent3
- ack-archive
  - ent1
  - ent2
  - ent3

- Create a mount point between the parent directory (for example, C:\INF-ARG-INTEGRATION) and SOA_Server. This allows file adapters on SOA_Server to exchange files with the Argus Safety system. The SOA server must be able to access the in, out, and ack-archive directories of the Argus Interchange (Argus ESM) server.
- Create a folder for archiving the files. For example, C:\INF-ARG-INTEGRATION\Archive.
- The Argus Interchange Server user needs read and write permissions to the folders. Assign read and write permissions to these folders:
  - C:\INF-ARG-INTEGRATION\in
  - C:\INF-ARG-INTEGRATION\out
  - C:\INF-ARG-INTEGRATION\ack-archive

  The following is the sample folder structure if the SOA server is in a Linux environment:

  Create a folder on the SOA server. For example, the Argus Interchange server can be mounted to the following parent folder:

  /home/user/ArgusSafety

  The Write File Adapter writes an E2B+ file with 660 permissions to this folder on the SOA server. The directory is a file mount between the Argus Interchange server and the SOA server. This destination directory is secured by operating system (OS) level security. On the Argus Interchange server, only the owner and

the group (administrator) have read and write access to the file. The user who logs in and shares the folder should have local administrator rights.

4.1 Enabling SSL on the SOA Server

You must enable SSL on the SOA server for the following reasons:

- Because patient data is sent in the messages from InForm Publisher to the SOA server, Oracle recommends that you use https to send the data.
- The default SOA server endpoint has a global policy that requires SAML or user name token authentication. InForm Publisher sends the user name token in the SOAP header. To pass the user name token in the SOAP header, InForm Publisher requires the SOA server endpoint to be SSL-enabled.

To enable SSL, see *Oracle® Fusion Middleware Securing Oracle WebLogic Server 11g Release 1 (10.3.6)*.

4.2 Configuring the SOA Server to Invoke InForm Adapter Over HTTPS

To invoke InForm Adapter in secure mode, follow this procedure.

The https certificate to access InForm Adapter must be loaded into the trusted keystore on the SOA server. You need the certificate that is installed on the InForm Adapter server.

1. Add the certificate to the WebLogic trust keystore. The following example shows how to add the certificate to DemoTrust.jks.

   The following link provides algorithm for locating trust store by WebLogic:

   http://docs.oracle.com/cd/E11035_01/wls100/secmanage/identity_trust.html#wp1183754

   Based on this, you can add the downloaded certificate to any trust keystore.

   a. Ensure that the SOA server can access the certificate. If the SOA server is on a different machine, copy the certificate to a folder on the SOA server machine.

      For example, copy the InForm Adapter certificate to the SOA server folder <Oracle Home>/<certs>/folder.

   b. Navigate to the location of the trust keystore. For example, if you are adding certificate to DemoTrust.jks, navigate to `<Middleware_Home>/wlserver_10.3/server/lib`.

   c. Execute the following command:

      ```
      keytool -import -trustcacerts -v -keystore DemoTrust.jks -file
      <Oracle Home>/<certs>/<cert_name> -alias InFormAdapterCert
      ```

   d. Enter the password when prompted.

   e. Enter **Yes** when prompted "Trust this certificate? [no]:".

   f. Execute the following command to ensure that the certificate is added:

      ```
      keytool -v -list -keystore DemoTrust.jks -storepass <password for
      keystore>
      ```

   g. Modify the startWebLogic.sh script in `<MIDDLEWARE_HOME>/user_projects/domains/soa_domain/bin/startWebLogic.sh` as follows:

      a. Open the startWebLogic.sh script.

b. Modify the line `JAVA_OPTIONS="${SAVE_JAVA_OPTIONS}"` to `JAVA_OPTIONS="${SAVE_JAVA_OPTIONS} -Djavax.net.ssl.trustStore=<full path to keystore>"`.

Note: You must modify this script because startWebLogic.sh requires the location of the custom trust keystore.

---

h. Restart the SOA server, Admin server, and Node manager.

2. Create a key in the credential store for InForm Adapter authentication credentials.

InForm Adapter authentication credentials are defined at the trial level when InForm Adapter is invoked over an https connection. If your company uses the same authentication user for all trials, you must perform the following steps to create a key in the SOA server keystore. The name of this key will be entered on a screen in the Configuration Wizard.

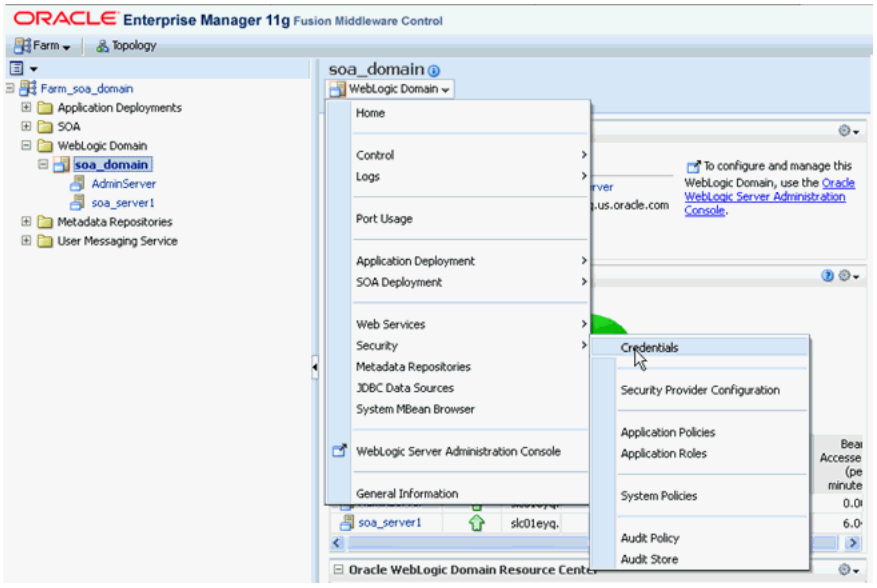
If you use a different user for each trial, follow the instructions in *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Implementation Guide* for setting up a trial for this integration.

a. Open Enterprise Manager.

b. Navigate to **Farm_soa_domain > WebLogic Domain > soa_domain**.

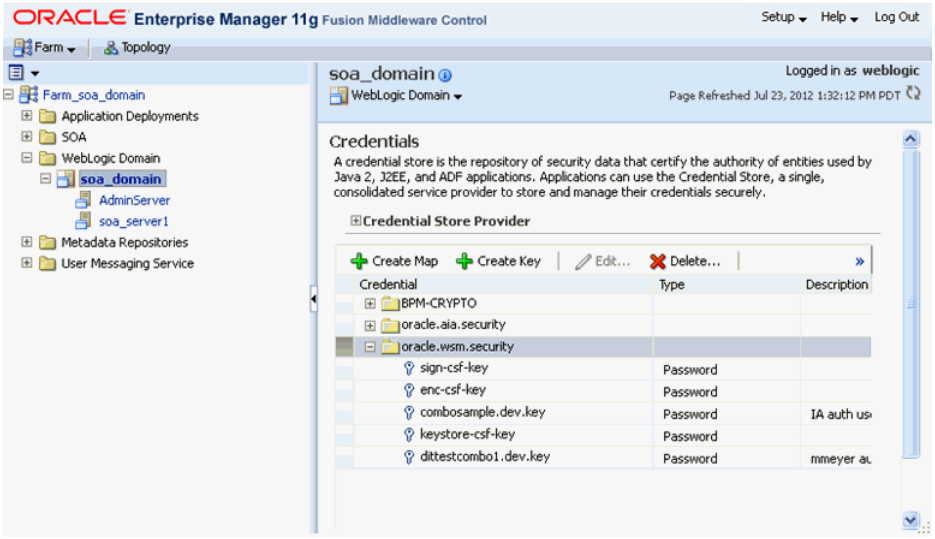
c. Click on the WebLogic Domain drop-down box and select **Security > Credentials**.

Figure 4–1 WebLogic Domain



d. In the Credential Store Provider screen, select **oracle.wsm.security** and expand it.

Figure 4–2 Credential Store Provider



If the **oracle.wsm.security** map does not exist, create the credential map using the following steps:

a. Open the Oracle Enterprise Manager 11g Fusion Middleware Control.

b. From the navigation pane, expand WebLogic Domain.

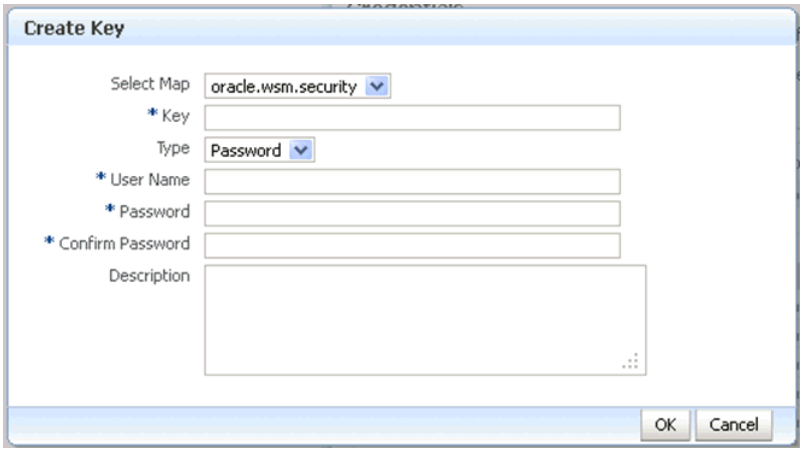
c. Right-click the domain name, click **Security**, then **Credentials**.

d. On the Credentials page, click **Create Map** and name it **oracle.wsm.security**.

e. Click **OK**.

e. Click **Create Key**. The Create Key screen is displayed.

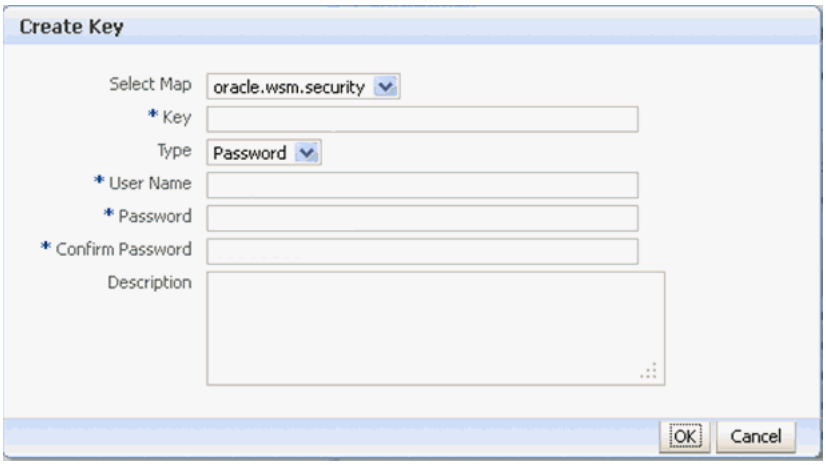
Figure 4–3 Create Key



f. In the Key field, enter a value (for example, alltrials.auth.key) and enter the user name and password for InForm Adapter authentication.

Note: Contact the InForm system administrator to obtain these values.

Figure 4–4 Entering a Value in the Key Field



g. Click **OK**.

The new key will appear in the list of keys under the oracle.wsm.security group. This key value will be provided either in configuration wizard screens or in HS_TRIAL_SAFETY_CONFIG.dvm.

The integration pack first checks HS_TRIAL_SAFETY_CONFIG.dvm for authentication parameters for a given trial. If the value is not found, it reads the value in the AIAConfigurationProperties.xml file, which is applicable to all trials on the SOA server.

The integration pack obtains credential information from the credential store through the key value. The credentials are then passed to the SOAP header when InForm Adapter is invoked in secure mode.

4.3 Verifying a Wildcard Hostname

If you are using a wildcard certificate for https communication, perform the following steps to enable verifying wildcard hostnames on the SOA server:

1. Navigate to the Admin console.
2. For each server in the cluster:
   a. Click the **SSL** tab.
   b. Click **Advanced**.
   c. Find **Hostname Verification**.
   d. Select **Custom Hostname Verifier** from the drop-down list.
   e. Find **Custom Hostname Verifier** and enter **weblogic.security.utils.SSLWLSWildcardHostnameVerifier** in the corresponding text box.
3. Click **Save**.

4.4 Creating Backups of Your Customizations

This section discusses the key tasks that you must perform before you install the media pack or when you apply patches to your existing PIPs:

- **Back up custom extensible style sheet language transformations (XSLTs)**: These are the extensions performed on the AIA Transformation style sheet. The Oracle AIA does not contain any XSLTs for its components and utilities. Because the process content is delivered only in PIPs, you must manually back up any XSLTs you developed for custom integrations, and reapply them as a post-installation step.
- **Back up custom routing rules in the EBS**: If you defined routing rules on any EBS that is available as part of the PIP, you must manually take a backup of the EBS and then merge the EBS manually as a post-installation step.
- **Back up the AIAConfigurationProperties.xml file**: This file is located in the `$AIA_INSTANCE/AIAMetaData/config` folder. Merge custom inclusions in the CONFIG file and change properties as required after installation.

Note: Ensure that you check My Oracle Support for the most current list of patches.

4.5 Creating a User in the Oracle WebLogic Server

InForm Publisher sends user name and password credentials to the SOA server. The user name and password that you create here must be entered as the endpoint user name and password in the InForm Publisher configuration screen. For more information, see *InForm Publisher Installation Guide*.

To create a user, perform the following steps:

1. Navigate to the WebLogic console.
2. Under the Domain Structure of **soa_domain**, select **Security Realms**, then select **myrealm**.
3. Select the **Users and Groups** tab, then select the **Users** tab.
4. Click **New**.
5. In the **Name** field, enter the user name that InForm Publisher sends.
6. In the **Password** field, enter the password.
7. In the **Provider** list, select the default authentication provider for the user.
8. Click **OK**.

5

Software Requirements

The Adverse Event: InForm and Argus Safety integration requires:

- Oracle® Health Sciences InForm Release 4.6 (SP2 and above), 5.5, or 6.0

  Note: Trials must be designed with Central Designer 1.4 or above.

- Oracle® Argus Safety Release 6.0.7 (including Argus J), 7.0.1, 7.0.2, or 7.0.3 (including Argus J).
- Oracle® Application Integration Architecture (AIA) Foundation Pack Release 11.1.1.6, and Service-Oriented Architecture (SOA) Suite with patches 14137846 and 14630316

  Roll-up Patch (RUP) 17423167
- InForm Publisher 1.0.3
- InForm Adapter 1.3.6.1 and above (Optional)

  InForm Adapter's safety web service is used to update case status information on the InForm Safety Event form. If it is not available, case information such as, status, case ID, and rejection reason (only for rejected cases) will not be updated.
- Central Designer 1.4 or above with plug-in installed

6 Configuration Wizard

The configuration wizard prompts you to enter the data that is required for successful configuration of the Adverse Event: InForm and Argus Safety integration. For faster, error-free configuration, enter the details of the Adverse Event: InForm and Argus Safety integration in the following tables, and then print the tables and enter that information into the screens in the configuration wizard.

6.1 Pre-Built Integration Server Details Screen

Table 6–1 describes the fields in the Pre-Built Integration Server Details screen.

Table 6–1 Pre-Built Integration Server Details Screen Fields

Field	Description
Admin Host Name	Where the admin server resides. This can be a remote server or the same system where the installer is launched. For example, `server1.company.com`. The Admin Host Name is _____
Admin Port	The port number on which the WebLogic admin server is started. To find this value, contact the WebLogic administrator. For example, `7001`. The Admin Port is _____
Domain Name	The WebLogic server domain where SOA server is created. For example, `domain1` The Domain Name is _____
Admin User	The WebLogic admin user name. To find this value, contact your WebLogic administrator. The Admin Username is _____
Admin Password	The WebLogic admin password. To find this value, contact your WebLogic administrator. The password is _____
Managed Server	After you enter the Admin Host Name, Admin Port, and Admin User, this field is populated with the managed servers for the domain. Select the managed server from the list. If you are deploying the integration to a SOA cluster, select the cluster name. The Managed Server is _____
Managed Port	This field is automatically updated after you select the managed server. If you have configured a SOA cluster, the SOA cluster port appears.

6.2 Argus Safety Details Screen

Table 6–2 describes the fields in the Argus Safety Details screen.

Table 6–2 Argus Safety Details Screen Fields

Field	Description
Is Argus Hosted by Oracle?	Indicates whether the Argus Safety application is hosted. If this check box is selected, Argus Safety is hosted by Oracle.
Interchange Files Root Directory Path	The directory path on the Argus server where the case files will be written and acknowledgment files will be read. This is configured in Argus Interchange and must be accessible to the SOA server. The Interchange directory path is _____
DTD Directory Path	The full file path of E2B+ DTDs on the Argus server. The DTD Directory Path is _____
Argus Database ID	A unique identifier for the Argus Safety database. The Argus Database ID is _____

6.3 InForm and InForm Adapter Details Screen

Table 6–3 describes the fields displayed in the InForm and InForm Adapter Details screen.

Table 6–3 InForm and InForm Adapter Details Screen Fields

Field	Description
Is InForm hosted by Oracle?	Indicates whether the InForm application is hosted. If this check box is selected, InForm is hosted by Oracle.
InForm Internet Protocol	For example: `https://`
InForm Hostname	The fully-qualified machine name of the InForm host. Enter this value if all trials use the same URL up to the trial name. The InForm host name is _____
InForm Port	The InForm port. Enter this value if all trials use the same URL up to the trial name. The InForm port number is _____
InForm Adapter Internet Protocol	For example: `https://` The protocol field must end with `://`
InForm Adapter Server Hostname	The fully qualified machine name of the InForm Adapter Server host. Enter this value if all trials use the same URL to access the InForm Adapter. The InForm Adapter Server host name is _____
InForm Adapter Server Port	The InForm Adapter port. Enter this value if all trials use the same URL to access InForm Adapter. The InForm Adapter Server port number is _____
InForm Adapter Server Path	The path to the InForm Adapter Web service. Enter this value if all trials use the same URL to access InForm Adapter. For example, if the URL for the InForm Adapter Server Path is `http://<hostname:port>/informadapter/safety/safety.svc`, the InForm Adapter Server Path refers to the text after `<hostname:port>`, which is `informadapter` in this example. The InForm Adapter Server Path is _____

Table 6–3 (Cont.) InForm and InForm Adapter Details Screen Fields

Field	Description
InForm Adapter Authentication Key	The key that used by the integration code to obtain the InForm Adapter authentication user name and password from the credential keystore. The user name and password are added to the SOAP header when InForm Adapter is invoked over SSL (https). Enter this value if all trials have the same authentication user name and password. The InForm Adapter authentication key is _____
InForm Adapter Transaction User	InForm Adapter passes this value to the InForm API for updating the InForm database. The transaction user must have two InForm rights - **Enter data into a CRF** and **Edit data on a CRF**. The transaction user name is placed in the audit trail in InForm for all update transactions. For example, the transaction user for InForm Adapter is `safetyintegration`. The InForm Adapter Transaction User is _____
Sender Company Abbreviation Code	Unique abbreviation code for the company, which is used as the sender of serious adverse event information. The Sender Company Abbreviation Code is _____

7

Installing the Adverse Event: InForm and Argus Safety Integration

This chapter contains the following topics:

7.1 Installing the Adverse Event: InForm and Argus Safety Integration

To install the Adverse Event: InForm and Argus Safety integration, perform the following steps:

1. Download Oracle® Health Sciences InForm and Oracle Argus Safety Integration Release 1.0 from the edelivery page.
2. Unzip aia-inform_argus-pip.zip to any location on the server.
3. Navigate to **inform_argus-pip** > **Disk1**.
4. Execute the following commands, based on your platform.

Table 7–1 Launching the Adverse Event: InForm and Argus Safety Installer

Field	Description
Linux x86 (64-bit) Solaris SPARC (64-bit)	At the command line prompt, enter: `./runInstaller -invPtrLoc <soa_Home>/oraInst.loc -jreloc <location of the jre specific to your operating system. This directory should have /bin/java>`
Microsoft Windows (32-bit or 64-bit)	Double-click **setup.exe**.

The Welcome screen is displayed, listing prerequisites and information about how to begin the installation process.

5. Click **Next**.
6. Wait for the following prerequisite checks to complete:

- Operating system certification
- Recommended operating system packages
- Kernal parameters
- Recommended gilbc version
- Physical memory

7. When the prerequisite checks are complete, click **Next**.

   The Installation location screen is displayed.

8. Select the AIA Home where the Foundation Pack is installed.
9. Click **Next**.

   The Installation Summary screen is displayed.

10. Review the installation summary. To save the Response file, click **Save.**

    The Response file stores the values that you previously entered and are on the summary page.

    If you want to install again, you can run a command and the installer performs a silent install with inputs from the Response file instead of using the wizard. The following is an example of the command. Note the `-silent` and `-response` arguments.

    ```
    ./runInstaller -invPtrLoc <SOA_Home>/oraInst.loc -jreLoc <location of the jre
    for your operating system> -silent -response <Oracle Home>/11.1_Installer_
    response.xml
    ```

    Note: he location of the jre for your operating system should have the format /bin/java. Do not use a hard coded value for java dir.

11. Click **Install**.

    A warning message is displayed indicating that any customizations will be overwritten.

12. Click **Yes** to proceed with the installation.

    Alternatively, if you click **No**, you can go back to the previous screen. For more information on how to back up AIA_HOME and preserve customizations, see Section 4.4.

13. Click **Next**.

    The Installation Progress screen is displayed.

14. Click **Next**.

    The Installation Complete screen is displayed.

15. Click **Finish**.

    The installation is complete.

7.2 Configuring Pre-deployment Security for the InForm-Argus Safety Integration

The Adverse Event: InForm and Argus Safety integration stores messages containing patient data in a JMS Queue on the SOA server. The JMS Queue must reside in an encrypted tablespace in the SOA database.

To configure pre-deployment security, perform the following steps:

1. Create or open the sqlnet.ora file from $ORACLE_HOME/network/admin.

   For example:

   `<Oracle Home>/db11g/product/11.2.0/dbhome_1/network/admin`.

2. To create a wallet that is used by the TDE encryption, follow the instructions in *Oracle® Database Advanced Security Administrator's Guide 11g Release 2 (11.2)*.

   Ensure that the following line is present in the sqlnet.ora file. If it is not present, add it at the end of the file.

   ```
   ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_
   DATA=(DIRECTORY=<ORACLE_BASE >/admin/<ORACLE_SID >/wallet/)))
   ```

   For example:

   ```
   ENCRYPTION_WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_
   DATA=(DIRECTORY=<Oracle Home>/db11g/admin/phrmdev2/wallet/)))
   ```

3. Save the sqlnet.ora file.

4. Navigate to `<AIA_HOME>/data/AEInFormandArgus/sql/JMSEncryption`.

5. Open **CreateSecureTableSpace.sql** in an editor.

6. Locate the string <ORACLE_HOME>/db11g/admin/<ORACLE_SID>/secure01.dbf in CreateSecureTableSpace.sql and replace it with the appropriate location on your database server. Change any parameters for the tablespace to suit your environment.

   For example:

   `/slot/machinename/xxxx.dbf`

7. Save CreateSecureTableSpace.sql.

8. Using SQL*Plus, connect to the database as a user with the SYSDBA role.

   For example:

   `sqlplus <username> as sysdba`

   Press **Enter**.

   Enter `<password>`.

9. Execute `CreateSecureTableSpace.sql`.

   For example:

   ```
   SQL> @ /<AIA_HOME>/data/AEInFormandArgus/sql/
   JMSEncryption/CreateSecureTableSpace.sql
   ```

   The SQL script prompts for the wallet password. Enter the wallet password provided during wallet creation. When the script executes successfully, a secure tablespace is created.

10. Exit SQL*Plus.
11. Using SQL*Plus, connect to the database as a user with the <AIA_INSTANCE>_JMSUSER role.

    For example:

    ```
    sqlplus <username>@<db sid>
    ```

    Press **Enter**.

    Enter `<password>`.

    Note: The script CreateSecureTable.sql can only be run once. If you run it second time, it deletes the existing table before creating a new one.

12. Execute `CreateSecureTable.sql`.

    For example:

    ```
    SQL> @ <AIA_HOME>/data/AEInFormandArgus/sql/
    JMSEncryption/CreateSecureTable.sql
    ```

    When the script executes successfully, a secure tablespace is created in the <AIA_INSTANCE>_JMSUSER schema.
13. Exit SQL*Plus.

7.3 Configuring the Adverse Event: InForm and Argus Safety Integration

The configuration wizard screens prompt you to enter the data that is required for successful configuration of the Adverse Event: InForm and Argus Safety integration. Complete the worksheets for the screens before you launch the configuration wizard. For more information, see Chapter 6.

To configure the Adverse Event: InForm and Argus Safety integration:

1. Navigate to <AIA_Instance>/bin and run the following command, as appropriate for your platform, to configure the installation environment:
   - Linux: `source aiaenv.sh`
   - Windows: `aiaenv.bat`
2. Navigate to <AIA_HOME>/bin and run the following command, as appropriate for your platform, to launch the AIA Configuration Wizard:
   - Linux: `./aiaconfig.sh`
   - Windows: `aiaconfig.bat`
3. Click **Next**.
4. Expand **Core Process Integration Packs** in the navigation tree.
5. Select **Adverse Event: InForm and Argus Safety Version 1.0**.
6. Click **Next**.

7.3.1 Specify Pre-Built Integration Server Details

To specify Pre-Built Integration Server details:

1. Enter information for your server in the Pre-built Integration Server Details screen.
2. Click **Next**.

7.3.2 Specify Argus Safety Details

To specify Argus Safety details:

1. Enter information about your Oracle Argus Safety server instance in the Argus Safety Details screen.
2. Click **Next**.

7.3.3 Specify InForm and InForm Adapter Details

To specify InForm and InForm Adapter details:

1. Enter information about your InForm server in the InForm and InForm Adapter Details screen.
2. Click **Next**.

7.3.4 Complete Configuration

To complete configuration:

1. Review the configuration information in the Configuration Summary screen.

   If you want change the configuration before starting the installation, use the navigation pane on the left and select the topic to edit.

   You can also create a response file based on the input provided and use it for future silent installations and deployments.
2. Click **Configure** to accept the configuration and begin the installation.

   The system displays progress in the Configuration Progress screen.

   Warnings or errors are displayed as necessary. You can review the configuration log for additional details. The configuration log location is displayed in the Configuration Progress screen.
3. Click **Next**.

   When the configuration process completes without errors, the Configuration Complete screen is displayed.
4. Click **Finish** to close the configuration wizard.
5. AIAInstallProperties.xml is updated. This file is located in the `<AIA_HOME>/aia_instances/<AIA_instance_name>/config` folder. Use this file for deploying the integration pack on the SOA server.

7.4 Configuring the Adverse Event: InForm and Argus Safety Integration Using a Response File

To configure the Adverse Event: InForm and Argus Safety integration using a response file, perform the following steps:

1. Open the response file.

   When you create a response file through the Oracle Universal Installer (OUI), passwords are stored as <SECURE>.

2. Replace the password fields with actual passwords in the response file.
3. Navigate to <AIA_Instance>/bin and run the following command, as appropriate for your platform, to configure the environment:
   - Linux: `source aiaenv.sh`
   - Windows: `aiaenv.bat`
4. Navigate to <AIA_HOME>/bin and run the following command, as appropriate for your platform:
   - Linux: `./aiaconfig.sh <Response File Location and Name>`
   - Windows: `aiaconfig.bat <Response File Location and Name>`

7.5 Deploying the Adverse Event: InForm and Argus Safety Integration

You deploy the Adverse Event: InForm and Argus Safety components on the SOA server as part of the post-installation configurations.

To deploy the integration to the SOA server, run the following commands, as appropriate for your platform.

1. Navigate to `<AIA_HOME/aia_instances/<AIA_instance_name>/bin` and enter the following:
   - Linux: `source aiaenv.sh`
   - Windows: `aiaenv.bat`

Table 7–2 Deployment commands for the InForm - Argus Safety Integration

Platform	Deployment Command
Linux Solaris SPARC	`ant -f $AIA_HOME/Infrastructure/Install/AID/AIAInstallDriver.xml -DPropertiesFile=$AIA_HOME/aia_instances/<instance_name>/config/AIAInstallProperties.xml -DDeploymentPlan=$AIA_HOME/pips/AEInFormandArgus/DeploymentPlans/AEInFormandArgusDP.xml -DSupplementaryDeploymentPlan=$AIA_HOME/pips/AEInFormandArgus/DeploymentPlans/AEInFormandArgusSupplementaryDP.xml -l $AIA_HOME/pips/AEInFormandArgus/DeploymentPlans/AEInFormandArgus.log`
Microsoft Windows	`ant -f %AIA_HOME%\Infrastructure\Install\AID\AIAInstallDriver.xml -DPropertiesFile=%AIA_HOME%\aia_instances\<instance_name>\config\AIAInstallProperties.xml -DDeploymentPlan=%AIA_HOME%\pips\AEInFormandArgus\DeploymentPlans\AEInFormandArgusDP.xml -DSupplementaryDeploymentPlan=%AIA_HOME%\pips\AEInFormandArgus\DeploymentPlans\AEInFormandArgusSupplementaryDP.xml -l %AIA_HOME%\pips\AEInFormandArgus\DeploymentPlans\AEInFormandArgus.log`

AIA ships a few artifacts in AIA Lifecycle Workbench that can be used in your integrations. You can modify these native artifacts, or you can add new, natively supported artifacts using AIA Lifecycle Workbench and then generate a BOM.xml file.

AIA Foundation Pack also supports the deployment of custom artifacts. These artifact types are beyond what is natively supported by Project Lifecycle Workbench and AIA Harvester. For example, you can deploy third party technology artifacts that constitute part of integration landscape in addition to those provided by AIA.

For more information on deploying artifacts, see *Oracle® Fusion Middleware Developer's Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6.0).*

8

Performing Post-Installation Configurations

This section discusses post-installation configurations for the Adverse Event: InForm and Argus Safety integration, including:

Note: Before you use the integration for a trial, follow the trial setup steps provided in *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Implementation Guide*.

Note: Be sure to install patch set 1.0.2 for the integration. You can download it from MOS as patch 16949125.

8.1 Creating a File Adapter Control Directory in Oracle WebLogic Server

When a Read File Adapter is deployed on multiple SOA servers, multiple composite instances are created for a single file. A control directory for File Adapter high availability must be created when the integration SOA server is clustered. This control directory ensures that all Read File Adapters do not read the same file simultaneously.

For example, when ReportDrugSafetyReportReadFileAdapter is deployed on a two-node SOA server cluster, the control directory ensures that there is only one composite instance per incoming file.

1. Log into the Oracle WebLogic Server Administration Console.

   To access the console, navigate to `http://servername:portnumber/console`.

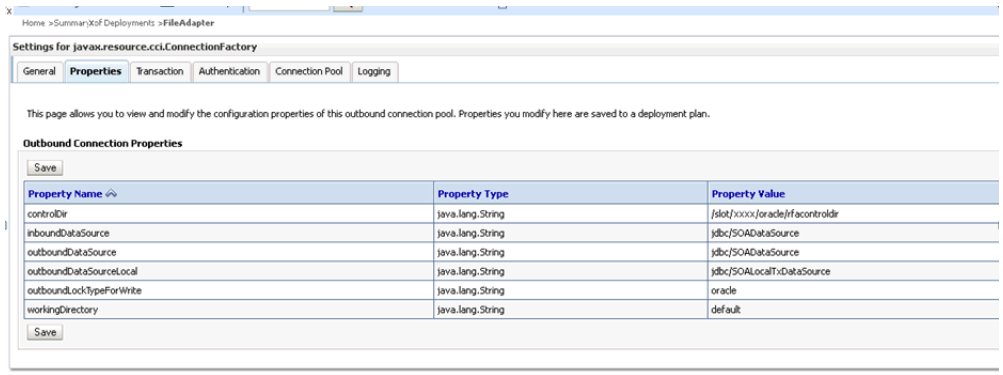
2. Click **Deployments** in the left pane for Domain Structure.
3. Click **File Adapter** under Summary of Deployments on the right pane.

4. Click the **Configuration** tab.
5. Click the **Outbound Connection Pools** tab, and expand **javax.resource.cci.ConnectionFactory** to view the configured connection factories.
6. Click **eis/HAFileAdapter**.

   The Outbound Connection Properties screen for the connection factory corresponding to high availability is displayed.
7. Update the **controlDir** property as follows:
   - Set the property to the directory structure where the control files can be stored.

     If multiple WebLogic Server instances run in a cluster, this must be a shared location. The directory specified must be write accessible to all WebLogic server instances.
   - Specify the directory path in the controlDir property.
   - Press **Enter**.

Figure 8–1 Outbound Connection Properties



8. Click **Save**.

   The Save Deployment Plan screen is displayed.
9. Click **OK** to save the deployment plan.

For more information, see *Oracle® Fusion Middleware User Guide for Technology Adapters 11g Release 1*.

8.2 Enabling Customization

For information about enabling customization, see *Oracle® Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Implementation Guide*.

8.3 Installing the Patch Set

You must install patch set 16949125 for the integration before proceeding with post-installation steps. The patch is available on My Oracle Support (https://support.oracle.com). For information on how to install the patch set, see *Oracle® Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety 1.0.2 Patch Set Readme*.

For questions or problems, contact Oracle Support for AIA.

8.4 Setting Up Argus Safety for Integration

To install the integration in Argus, perform the following steps:

- Section 8.4.1, "Configuring a Custom Package for Encoding Products with Investigational Licenses"
- Section 8.4.2, "Setting Up an Argus E2B Extension Profile"
- Section 8.4.3, "Turning Off PMDA Validations for the PMDA PIP Profile in the Argus ESM_PKG"
- Section 8.4.4, "Configuring Post-Save Functionality in Argus Safety"

8.4.1 Configuring a Custom Package for Encoding Products with Investigational Licenses

If you do not have the Argus 7.0.3.1 patch set installed, run this procedure to set the E2B import logic to encode products correctly. Perform this procedure before you create integration profiles.

1. Copy the folder `<AIA_HOME>\data\AEInFormandArgus\sql\ArgusCustomImpUtl` to the Argus Interchange server. This folder contains the SQL script to use in this procedure.
2. Connect to the Argus database using SQL*PLUS as the esm_owner.
3. Run **ArgusCustomImpUtl**<*Argus Version*>**\custom_esm_imp_utl_<Argus Version>.plb**. *Argus_Version* must be 607, 701, 702, or 703, depending on the version of Argus Safety that is installed.
4. You will be prompted for the esm_user database user twice. Each time you are prompted, enter the esm owner username (for example, esm_owner).

8.4.2 Setting Up an Argus E2B Extension Profile

You set up Argus E2B profiles on the Argus Interchange server. The profile you create depends on the version of Argus Safety you are using and whether you are creating a profile for the FDA or PMDA.

If you are using the multi-tenant feature of Argus Safety:

- Create one reporting destination for each enterprise.
- Create in, out, and ack archive directories to hold E2B+ and acknowledgement files. Within each of these directories, create a sub-directory for each enterprise.

  For information about these directories, see Chapter 4.

> **Note:** You must install the Adverse Event: InForm and Argus Safety integration patch set 1.0.2 (patch # 16949125) before you set up an Argus E2B profile. The patch is available on MOS.

This section contains instructions for:

- Section 8.4.2.1, "Setting Up an FDA-based Extension Profile"
- Section 8.4.2.2, "Setting Up a PMDA-based Extension Profile"
- Section 8.4.2.3, "Updating an Existing Argus FDA Profile"

Note: If you create a profile and then run a second profile creation script, the following message displays:

```
ORA-00001: unique constraint (ESM_OWNER.PK_LM_ESM_ARGUS_
MAPPING) violated
```

You may ignore this error. It occurs because some data that is shared between profiles is inserted in a database table when the first profile is created and, since the data exists, when subsequent profiles are created a unique constraint violation occurs.

8.4.2.1 Setting Up an FDA-based Extension Profile

Use one of the following procedures, as appropriate for the version of Argus Safety in use, to set up an FDA extension profile.

For Argus 6.0.7:

1. Navigate to the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile/FDA/6.0` and copy the **ich-icsr-v2.1-FDA-PIP.dtd** file to the Interchange server folder `<Oracle_Home>\Argus\ESMService\DTDFiles\`.
2. Copy all the files from the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile/FDA/6.0` to a folder on the Argus ESM server (for example, `C:\Temp_config_folder`).
3. On the Argus Interchange server, open a command prompt and navigate to the folder where you copied the scripts in step 2.

Note: You must install the Adverse Event: InForm and Argus Safety integration patch set 1.0.2 (patch # 16949125) before you set up an Argus E2B profile. The patch is available on MOS.

The Argus DTD will be updated to include additional fields to support custom extension fields, non-custom extension fields, and non-E2B extension fields.

4. Run **Setup_Safety_Integration_Profile.bat**. The scripts in this batch file import the custom extension fields, non-custom extension fields, and non-E2B extension fields that need to be added to the integration-specific DTD.
5. Enter the database name, ESM owner's username (for example, esm_owner), password, and log file path (C:\Temp_config_folder\profilecreationoutput.log).
6. Press **Enter**.

For Argus 7.0.1, 7.0.2, and 7.0.3:

1. Navigate to the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile/FDA/7.0` and copy the **ich-icsr-v2.1-FDA-PIP.dtd** file to the Interchange server folder `<Oracle_Home>\Argus\InterchangeService\DTDFiles\`.
2. Copy all the files from the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile/FDA/7.0` to a folder on the Argus Interchange server (for example, `C:\Temp_config_folder`).
3. On the Argus Interchange server, open a command prompt and navigate to the folder where you copied the scripts in step 2.

> **Note:** You must install the Adverse Event: InForm and Argus Safety integration patch set 1.0.2 (patch # 16949125) before you set up an Argus E2B profile. The patch is available on MOS.
>
> The Argus DTD will be updated to include additional fields to support custom extension fields, non-custom extension fields, and non-E2B extension fields.

4. Run **Setup_Safety_Integration_Profile.bat**. The scripts in this batch file import the custom extension fields, non-custom extension fields, and non-E2B extension fields that need to be added to the integration-specific DTD.

> **Note:** Run Setup_Safety_Integration_Profile.bat for each enterprise separately.

5. Enter the database name, enterprise short name, ESM owner's username (for example, esm_owner), password, and log file path (C:\Temp_config_folder\profilecreationoutput.log).

> **Note:** If Argus Safety is installed in single-tenant mode, do not provide an enterprise short name. Instead, press **Enter**.

6. Press **Enter**.

8.4.2.2 Setting Up a PMDA-based Extension Profile

Use one of the following procedures, as appropriate for the version of Argus Safety in use, to set up an PMDA extension profile.

For Argus 6.0.7:

1. Navigate to the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile/PMDA/6.0` and copy the **ich-icsr-v2.1_PMDA_PIP.dtd** and **ichicsr-sjis-PIP.dcl** files to the Interchange server folder `<Oracle_Home>\Argus\ESMService\DTDFiles\`.
2. Copy all the files from the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile/PMDA/6.0` to a folder on the Argus ESM server (for example, `C:\Temp_config_folder`).
3. On the Argus Interchange server, open a command prompt and navigate to the folder where you copied the scripts in step 2.

> **Note:** You must install the Adverse Event: InForm and Argus Safety integration patch set 1.0.2 (patch # 16949125) before you set up an Argus E2B profile. The patch is available on MOS.
>
> The Argus DTD will be updated to include additional fields to support custom extension fields, non-custom extension fields, and non-E2B extension fields.

4. Run **Setup_Safety_Integration_Profile.bat**. The scripts in this batch file import the custom extension fields, non-custom extension fields, and non-E2B extension fields that need to be added to the integration-specific DTD.
5. Enter the database name, ESM owner's username (for example, esm_owner), password, and log file path (C:\Temp_config_folder\profilecreationoutput.log).
6. Press **Enter**.

For Argus 7.0.3:

1. Navigate to the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile/PMDA/7.0` and copy the **ich-icsr-v2.1_PMDA_PIP.dtd** and **ichicsr-sjis-PIP.dcl** files to the Interchange server folder `<Oracle_Home>\Argus\InterchangeService\DTDFiles\`.
2. Copy all the files from the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile/PMDA/7.0` to a folder on the Argus Interchange server (for example, `C:\Temp_config_folder`).
3. On the Argus Interchange server, open a command prompt and navigate to the folder where you copied the scripts in step 2.

> **Note:** You must install the Adverse Event: InForm and Argus Safety integration patch set 1.0.2 (patch # 16949125) before you set up an Argus E2B profile. The patch is available on MOS.
>
> The Argus DTD will be updated to include additional fields to support custom extension fields, non-custom extension fields, and non-E2B extension fields.

4. Run **Setup_Safety_Integration_Profile.bat**. The scripts in this batch file import the custom extension fields, non-custom extension fields, and non-E2B extension fields that need to be added to the integration-specific DTD.

> **Note:** Run Setup_Safety_Integration_Profile.bat for each enterprise separately.

5. Enter the database name, enterprise short name, ESM owner's username (for example, esm_owner), password, and log file path (C:\Temp_config_folder\profilecreationoutput.log).

> **Note:** If Argus Safety is installed in single-tenant mode, do not provide an enterprise short name. Instead, press **Enter**.

6. Press **Enter**.

8.4.2.3 Updating an Existing Argus FDA Profile

You must update the ICH-ICSR V2.1 MESSAGE TEMPLATE - FDA PIP Argus profile if you:

- Created an Argus profile before applying the patch set

- Had an FDA Profile from Device and Drug Adverse Event: Siebel AECM and Argus Safety integration pack on your Argus 6.0 environment before applying the patch set
- Upgraded Argus Safety from 7.0.1 to a higher version after applying the patch set

To update an existing Argus profile, follow these steps:

1. Navigate to the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile/FDA/<version>` (where version is 6.0 or 7.0, depending on your version of Argus).
2. Copy the `ich-icsr-v2.1-FDA-PIP.dtd` file to the Interchange server folder `<Oracle_Home>\Argus\ESMService\DTDFiles\`.
3. After the patch set is successfully installed on the SOA server, copy all Argus profile creation SQL scripts from `$AIA_HOME/data/AEInFormandArgus/sql/ArgusProfile/FDA/<version>` (where version is 6.0 or 7.0, depending upon your version of Argus) to a temporary directory on the Argus Interchange server.
4. On the Argus Interchange Server, open the ESM Mapping Utility.

   You must select a specific enterprise name if you are using multi-tenant Argus.
5. Select `Profile - ICH-ICSR V2.1 MESSAGE TEMPLATE - FDA PIP` from the Profile drop-down list.
6. Select **Administrator**, then select **Delete Profile**.

   Note: If the Delete Profile option appears to be disabled, expand the profile element (for example, SAFETYREPORT[A.1]) and click any child node (for example, SAFETYREPORTVERSION). Navigate to **Administrator**, then select **Delete Profile**.
7. Click **Yes**.

   If you are using Argus Safety version 7.0.2 or lower, the following error message is displayed on the ESM Mapping Utility:

   ```
   Unhandled exception has occurred in your application. If you click
   Continue, the application will ignore this error and attempt to
   continue. If you click Quit, the application will close immediately.
   Contact your System Administrator - Continue, Quit.
   ```

   If you are using Argus Safety version 7.0.3 or higher, the following error message is displayed on the ESM Mapping Utility:

   ```
   Profile ICH-ICSR V2.1 MESSAGE TEMPLATE - PFA PIP cannot be deleted, as
   it is being used in Reporting Destination.
   ```
8. Click **Continue**. You can ignore the message because you are deleting the profile that is referred to in the reporting destination configuration on the Argus Console. The profile will be created in the steps that follow.
9. Open the command prompt and navigate to the temporary directory where the profile creation scripts are copied.
10. Run **Setup_Safety_Integration_Profile.bat**.

    These scripts import the custom extension fields, non-custom extension fields, and non-E2B extension fields that are added to the integration-specific DTD.

11. Enter the database name, enterprise short name (for Argus 7.0 and later), ESM owner's user name (for example, esm_owner), password, and log file path (for example, C:\Temp_config_ folder\profilecreationoutput.log).

    Note: For single-tenant Argus, do not provide an enterprise short name. Instead, press **Enter**.

12. When the script runs, it generates unique constraint violation errors as follows:
    - ORA-00001: unique constraint (ESM_OWNER.PK_CFG_PROFILE) violated
    - ORA-00001: unique constraint (ESM_OWNER.PK_LM_ESM_ARGUS_ MAPPING) violated

    These errors occur if a profile with the same name exists. While deleting the profile in step 4, data from LM_ESM_ARGUS_MAPPING and CFG_PROFILE tables are not deleted. However, you can ignore these errors because the profile scripts insert the same data into these tables.

13. After the script completes, the profile is updated for the E2B import process specific to the Argus Safety version in use.

8.4.3 Turning Off PMDA Validations for the PMDA PIP Profile in the Argus ESM_PKG

If you have Argus J enabled and do not have the Argus 7.0.3.1 patch set installed, follow this procedure to turn off PMDA validations for the Argus PMDA PIP profile.

1. The folder `<AIA_HOME>\data\AEInFormandArgus\sql\ArgusESMPkg` has sub-directories for Argus versions 6.0 and 7.0. Each sub-directory contains the version-specific SQL scripts used in this procedure. Copy the contents of the folder for your version of Argus Safety to the Argus Interchange server.
2. Connect to the Argus database using SQL*PLUS as the ESM_OWNER user.
3. Run **esm_pkg_h.plb**.
4. When prompted for esm_user database user, enter the username of the esm owner database (for example, esm_owner).
5. Run **esm_pkg.plb**.
6. When prompted again for esm_user database user, enter the username of the esm owner database (for example, esm_owner).

8.4.4 Configuring Post-Save Functionality in Argus Safety

After creating integration profiles, perform the following procedure to enable post-save functionality in Argus Safety.

1. Copy the folder `<AIA_HOME>\data\AEInFormandArgus\sql\ArgusPostSave` to the Argus Interchange server. This folder contains the SQL scripts to use in this procedure.
2. Connect to the Argus database using SQL*PLUS as the esm_owner.
3. Run **Custom_AutopsyResults_PIP.sql**.

   Run **GrantAutopsyResults_PIP.SQL**.
4. Log into the ESM Mapping Utility.

5. Select integration profile **ICH-ICSR V2.1 MESSAGE TEMPLATE - FDA PIP** from the drop down list.
6. Navigate to **ICHICSR->SAFETYREPORT->PATIENT->PATIENTDEATH->PATIENTAUTOPSYYESNO**.
7. On the right side, select the **Enable Post-Save** check box.
8. Click **Save**.
9. If you are using Argus 6.0.7 or Argus 7.0.3, Argus J is enabled, and an integration-specific PMDA profile was created, select integration profile **ICH-ICSR V2.1 MESSAGE TEMPLATE - PMDA PIP** from the drop down list and repeat steps 6 through 8.
10. Open the Argus Safety Web application. For multi-tenant Argus, select the enterprise and navigate to the Argus Safety application for that enterprise.
11. Open Argus Console and select **System Configuration**, then **System Management** (common profile switches) screen, and then **Case Form Configuration** in the navigation on the left side of the screen.
12. On the right side of the screen, select the **Custom Routine after Commit** check box (under Custom Routine).
13. In the text box next to Custom Routine after the Commit check box, specify the PL/SQL function name as **ESM_OWNER.Custom_AutopsyResults_PIP**.

    If a different custom routine is already configured in the text box, you must edit that custom routine to invoke ESM_OWNER.Custom_AutopsyResults_PIP.
14. Click **Table Config**.
15. Add **CASE_DEATH** table to the list of selected tables.
16. Save the case form configuration.

8.5 Configuring Argus Safety to Use Extension Profiles

8.5.1 Configuring Argus Safety to Use the FDA Extension Profile

To configure Argus Safety for use with the FDA extension profile, perform the following steps:

1. Open the Argus Console.
2. From the browser, navigate to the **Reporting Destination** folder.
3. Click **Add New** to create new agency details to serve as a reporting destination.
4. Enter the agency information in the **Agency Information** pane. Table 8–1 provides field description and example values.

Table 8–1 Agency Information Tab Field Descriptions for FDA

Fields	Description
Agency Name	Enter INFORM-ARGUS-INTEGRATION. This agency is for the integration only and should not be used for sending reports to regulatory agencies. The E2B files received by this agency use a format that is different from the standard E2B format that can be sent to regulatory authorities such as FDA. For example, the positions of companynumb element and primarysourcecountry element have been swapped to ensure that the companynumb element is in all acknowledgement files that are auto-generated by Argus due to M2 validation failure.
Report for Marketed Licenses	Contains the default value **Always**.
Report for Investigational Licenses	Contains the default value **Always**.

5. Click the **Local Company Contact** tab and enter the contact details. Table 8–2 provides the field description and an example value.

Table 8–2 Local Company Contact Tab Field Description for FDA

Fields	Description
Company Name	Enter the company name. This is a mandatory field. For example, INTEGRATIONS.

6. Click the **EDI** tab and enter values in the fields. Table 8–3 provides field description and example values.

Table 8–3 EDI Tab Field Description for FDA

Fields	Description
SGML or XML	Select **XML**. This field represents the format of incoming E2B files and outgoing acknowledgement files.
Agency Identifier	Enter **INFORM_01**. This value should match the sender identifier in the E2B file.
Company Identifier	Enter **ARGUS_01**. This value should match the receiver identifier in the E2B file.
Method	Select **E2B-XML transmission**.
Message Profile	Select the ICH ICSR V2.1 MESSAGE - TEMPLATE - FDA PIP extension profile from the Message Profile list.
ACK Profile	Select the ICH-ICSR V 1.1 ACKNOWLEDGMENT TEMPLATE - FDA acknowledgment profile from the ACK Profile list.
File Name	Enter Safety######.xml as the file name pattern of the incoming file.
URL of Message DTD	Enter the extension DTD file path. For example, `C:\Program Files\Oracle\Argus\InterchangeService\DTDFiles\ich-icsr-v2.1-FDA-PIP.dtd`
URL of ACK DTD	Enter the acknowledgment DTD file path. For example, `C:\Program Files\Oracle\Argus\InterchangeService\DTDFiles\FDA-icsrack-v1.1.dtd`

7. Click **Save**. The Argus Console dialog box is displayed.
8. Click **OK**. Oracle Argus Safety is configured for the E2B extension for the selected agency.

Note: In multi-tenant Argus Safety, different enterprises can have the same agency and company identifier values. For configuring the E2B folder, see "Configuring Folders for XML File Sharing".

8.5.2 Configuring Argus Safety to Use the PMDA Extension Profile

If you have Argus J enabled, follow this procedure to configure Argus Safety for use with the PMDA extension profile. You must have the Argus J privilege to enter data into J fields.

1. Open the Argus Console.
2. From the browser, navigate to the **Reporting Destination** folder.
3. Click **Add New** to create new agency details to serve as a reporting destination.
4. Enter the agency information in the **Agency Information** pane. Table 8–4 provides field description and example values.

Table 8–4 Agency Information Tab Field Descriptions for PMDA

Fields	Description
Agency Name	Enter INFORM-ARGUS-INTEGRATION-JAPAN. This agency is for the integration only and should not be used for sending reports to regulatory agencies. The E2B files received by this agency use a format that is different from the standard E2B format that can be sent to regulatory authorities such as PMDA. For example, the positions of companynumb element and primarysourcecountr element have been swapped to ensure that the companynumb element is in all acknowledgement files that are auto-generated by Argus due to M2 validation failure.
Agency Name J	Enter INFORM-ARGUS-INTEGRATION-JAPAN. This agency is for the integration only and should not be used for sending reports to regulatory agencies. The E2B files received by this agency use a format that is different from the standard E2B format that can be sent to regulatory authorities such as PMDA. For example, the positions of companynumb element and primarysourcecountr element have been swapped to ensure that the companynumb element is in all acknowledgement files that are auto-generated by Argus due to M2 validation failure.
Report for Marketed Licenses	Contains the default value **Always**.
Report for Investigational Licenses	Contains the default value **Always**.

5. Click the **Local Company Contact** tab and enter the contact details. Table 8–2 provides the field description and an example value.

Table 8–5 Local Company Contact Tab Field Description for PMDA

Fields	Description
Company Name	Enter the company name. This is a mandatory field. For example, INTEGRATIONS.
Company Name J	Enter the company name for the Japanese view. This is a mandatory field. For example, INTEGRATIONS-J.

6. Click the **EDI** tab and enter values in the fields. Table 8–3 provides field description and example values.

Table 8–6 EDI Tab Field Description for PMDA

Fields	Description
SGML or XML	Select **SGML**. This field represents the format of incoming E2B files and outgoing acknowledgement files.
Agency Identifier	Enter **INFORM_01J**. This value should match the sender identifier in the E2B file.
Company Identifier	Enter **ARGUS_01J**. This value should match the receiver identifier in the E2B file.
Method	Select **E2B-Binary transmission**.
Message Profile	Select the ICH ICSR V2.1 MESSAGE - TEMPLATE - PMDA PIP extension profile from the Message Profile list.
Message Profile 2	Select the ICH ICSR V2.1 MESSAGE - TEMPLATE - PMDA J extension profile from the Message Profile list.
ACK Profile	Select the ICH-ICSR V 1.1 ACKNOWLEDGMENT TEMPLATE - PMDA acknowledgment profile from the ACK Profile list.
File Name	Enter Safety######.sgm as the file name pattern of the incoming file.
SGML Declaration File	Select ichicsr-sjis-PIP.dcl. This field represents the control file used by the SGML parser to parse incoming files.
Encoding	Enter UTF-8.
URL of Message DTD	After you complete the other fields in the table, this field is disabled.
URL of ACK DTD	After you complete the other fields in the table, this field is disabled.

7. Click **Save**. The Argus Console dialog box is displayed.
8. Click **OK**. Oracle Argus Safety is configured for the E2B extension for the selected agency.

Note: In multi-tenant Argus Safety, different enterprises can have the same agency and company identifier values. For configuring the E2B folder, see "Configuring Folders for XML File Sharing".

8.6 Configuring Folders for XML File Sharing

To exchange E2B and acknowledgement files between Argus Safety and the SOA server, you must create folders and configure them. For folder details, see Chapter 4.

> **Note:** If you are using multi-tenant Argus Safety, you need to create folders and configure each enterprise separately.

To configure the folders, perform the following steps:

1. On the Argus ESM server, open the ESM Mapping Utility as follows: click **Start**, select **All Programs**, select **Oracle**, then select **ESM Mapping**.
2. Enter the user name, password, and database name to run the mapping tool.
3. For a multi-tenant Argus Safety installation, select the enterprise name from the drop-down list.
4. In the ESM Mapping Utility, navigate to Administrator, and select **setup.ini**.
5. In the **Multiple Database** section, double-click on the database name to set up system directories for E2B exchange.

   The Service DB Setup screen displays.

   > **Note:** If the Argus database is new, you may not see a database name. To create a database, select **Add New Process** and double click. This opens the Service DB Setup screen.
   >
   > For entering the values in the **Service DB Setup** screen, see Table 8–7.

6. In the System Directories pane, select **INFORM-ARGUS-INTEGRATION** from the list.

   The fields that appear in the System Directories pane depend on the version of Argus in use.

Table 8–7 Field Descriptions for the Service DB Setup Screen

Fields	Description
Database Section	
Database Name	Enter the database name (for example, AS70xx).
Unique Database ID	Enter unique database ID (for example, 123).
User ID	Enter the database user name.
Password	Enter the database password.
Process	For Argus 6.0.x, enter `C:\Program files\Oracle\Argus\ESMService\EsmProc.exe`. For Argus 7.0.x, enter `C:\Program Files\Oracle\Argus\InterchangeService\EsmProc.exe`.
Receive Process	For Argus 6.0.x, enter `C:\Program files\Oracle\Argus\ESMService\E2BReceive.exe`. For Argus 7.0.x, enter `C:\Program Files\Oracle\Argus\InterchangeService\E2BReceive.exe`.

Table 8–7 (Cont.) Field Descriptions for the Service DB Setup Screen

Fields	Description
Archive Folder	Select the folder for archiving the files (for example, `C:\INF-ARG-INTEGRATION\Archive`. You created this folder as one of the Prerequisites.
Receive Processes	Enter the value `1`.
Process Elapse Time	Enter the value `1 minute`.
Time Out Section	
EDI Transmit Time Out value (File is not picked up by Gateway)	Enter the value `10 minutes`.
Physical Media Transmit Time Out value (File is not picked up manually)	Enter the value `10 minutes`.
Receive ACK Time Out value (ACK is due for transmitted reports)	Enter the value `10 minutes`.
Processing Time Out value (E2B Report not Processed by User)	Enter the value `10 minutes`.
XML Transmit Time Out value (File is not picked up by Gateway)	Enter the value `10 minutes`.
Binary Transmit Time Out value (File is not picked up by Gateway)	Enter the value `10 minutes`.
MDN Time Out Value (For E2B Reports which have received Bus ACK)	Enter the value `0 hours`.
System Directories Section (for Argus 7.0.x)	
Enterprise Short Name	Select the enterprise short name (for example, ent1).
Agency Name	Select INFORM-ARGUS INTEGRATION agency configured in the Argus Console, Reporting Destination.
Local Company	The value displayed is based on the Reporting Destination Configuration.

Incoming Folder	Specify the folder path for incoming files. The path is the same for FDA and PMDA extension profiles.
	You created this folder as one of the Prerequisites.
	For multi-tenant Argus, agencies from two different enterprises cannot share the same folder for incoming E2B files. Therefore, the following folder structure is required:
	`C:\<FILE_EXCHANGE_DIR_ROOT>\in\<enterprise_name_1>`
	`C:\<FILE_EXCHANGE_DIR_ROOT>\in\<enterprise_name_2>`
	For single-tenant Argus, the folder structure is as follows:
	`C:\<FILE_EXCHANGE_DIR_ROOT>\in`

Outgoing Folder	Specify the folder path for outgoing files. The path is the same for outgoing acknowledgements for FDA and PMDA extension profiles.
	You created this folder as one of the Prerequisites.
	For multi-tenant Argus, the folder structure is as follows:
	`C:\<FILE_EXCHANGE_DIR_ROOT>\out\<enterprise_name_1>`
	`C:\<FILE_EXCHANGE_DIR_ROOT>\out\<enterprise_name_2>`
	For single-tenant Argus, the folder structure is as follows:
	`C:\<FILE_EXCHANGE_DIR_ROOT>\out`

Table 8–7 (Cont.) Field Descriptions for the Service DB Setup Screen

Fields	Description
System Directories Section (for Argus 6.0.x)	
Agency Name	Select INFORM-ARGUS-INTEGRATION-JAPAN agency configured in the Argus Console, Reporting Destination.
Local Company	The value displayed is based on the Reporting Destination Configuration.
XML Incoming Folder	Specify the folder path from the FDA extension profile for incoming files. You created this folder as one of the Prerequisites. The folder structure is as follows: `C:\<FILE_EXCHANGE_DIR_ROOT>\in`
XML Outgoing Folder	Specify the folder path from the FDA extension profile for outgoing files. You created this folder as one of the Prerequisites. The folder structure is as follows: `C:\<FILE_EXCHANGE_DIR_ROOT>\out`
Binary Incoming Folder	Specify the folder path from the PMDA extension profile for incoming files. You created this folder as one of the Prerequisites. The folder structure is as follows: `C:\<FILE_EXCHANGE_DIR_ROOT>\in`
Binary Outgoing Folder	Specify the folder path from the PMDA extension profile for outgoing files. You created this folder as one of the Prerequisites. The folder structure is as follows: `C:\<FILE_EXCHANGE_DIR_ROOT>\out`

7. Enter the values in the corresponding fields and click **Save**.
8. Click **OK**.
9. Click **OK** on the **Service INI File** Setup screen.

8.7 Changing Parameters on the SOA Server

8.7.1 Changing Parameters to Increase Performance

To change parameters on the SOA server to increase the performance of the integration, perform the following steps:

1. Navigate to the Enterprise Manager (EM) Console:

   http://<server name>:<port number>/em/
2. Navigate to farm_soa_domain, select **SOA**, then right-click **soa-infra**.
3. Select **SOA Administration**, then select **Mediator Properties**.
4. Change the default value of ResequencerLockerThreadSleep from 10 to 1.

8.7.2 Changing the Default Values of Transaction Timeouts

To change the transaction timeout values on the SOA server to suit your environment, perform the following steps:

1. Log into the WebLogic Console.
2. Navigate to soa_domain and then **Services**.
3. Click the **JTA** tab.
4. Increase the default value of Java Transaction API (JTA) timeout to a value that is long enough time to complete transactions, but not so long that it impacts performance.
5. Oracle recommends that you increase the Extended Architecture (XA) Transaction timeout for the XA data source as described in http://docs.oracle.com/cd/E28271_01/admin.1111/e10226/soainfra_config.htm#BHCDIBCE.

In a clustered SOA server environment, perform the following configurations to ensure that all composites in a flow participate in one global transaction:

1. Navigate to the EM Console:

   http://<server name>:<port number>/em/

   a. Navigate to farm_soa_domain, select **SOA**, then right-click **soa-infra**.

   b. Select **SOA Administration**, then select **Common Properties**.

   c. In theServer URL property, enter the load-balancer URL for your server cluster (for example, http(s)://lbhost:lbport/).

   Note: Be sure to use the ending backslash (/). If it is omitted, the function will not work correctly.

2. Open the WebLogic Console.

   a. Navigate to the **Domain Structure/<domain name>/environment/Clusters** page.

   b. Select the cluster name.

   c. Click the **Configuration/HTTP** tab.

   d. Enter values in the following fields:

   Frontend Host: Enter the host DNS address of the load balancer.

   Frontend HTTP Port: Enter the port number of the load balancer.

   Frontend HTTPS Port: If SSL communication is enabled, use this field instead of Frontend HTTP Port.

3. Restart the node manager, admin, and SOA servers.

8.8 Disabling the Acknowledgment Flow

The Acknowledgement flow requires InForm Adapter. If you do not have InForm Adapter or are not using it, you can disable the Acknowledgement flow by shutting down the following services through Enterprise Manager (EM):

- ReportDrugSafetyReportReadAckFileAdapter

- ReportDrugSafetyReportResponseArgusReqABCSImpl
- HealthSciencesDrugSafetyReportResponseEBS
- ReportDrugSafetyReportResponseInFormProvABCSImpl

8.8.1 Shutting Down the Services

To shut down the services, perform the following steps:

1. Navigate to the EM Console:

   http://<server name>:<port number>/em/
2. Log in with the server admin user name.
3. Navigate to **soa-infra/services/default**.

   The list of services is displayed.
4. Click on the service to shut down, then click **Shut Down**.
5. Click **Yes** in the confirmation window.

> **Note:** To restart a service, click **Start Up**.

9

Verifying Installation

To verify the installation of Adverse Event: InForm and Argus Safety Integration, follow these steps:

1. Open the log files from the following location and look for warnings and error messages:
   - Linux and Solaris SPARC-based systems: Review the install log located at <AIA_HOME>/aia_instances/<AIA_Instance_name>/logs.
   - Windows: Review the install log located at <AIA_HOME>\aia_instances\<AIA_Instance_name>\logs.
2. Confirm that the Oracle Health Sciences InForm and Oracle Argus Safety Integration components were successfully installed:
   a. Navigate to the EM Console: *http://<server name>:<port number>/em/*
   b. Log in with the server admin user name. For access details, contact the system administrator.
   c. Navigate to soa-infra/services/default and look for the following:
      * HealthSciencesDrugSafetyReportEBS
      * HealthSciencesDrugSafetyReportResponseEBS
      * InFormDrugSafetyReportJMSProducer
      * InFormDrugSafetyReportJMSConsumer
      * ReportDrugSafetyReportInFormReqABCSImpl
      * ReportDrugSafetyReportArgusProvABCSImpl
      * ReportDrugSafetyReportWriteE2BFileAdapter
      * ReportDrugSafetyReportReadAckFileAdapter
      * ReportDrugSafetyReportResponseArgusReqABCSImpl
      * ReportDrugSafetyReportResponseInFormProvABCSImpl

9.1 Validating Security Policies

This integration pack leverages the security infrastructure provided by the Oracle 11g SOA Suite, the AIA Foundation Pack, and the underlying transport layer security features for Web Service security. The Foundation Pack assigns global service and client security policies that use user name or SAML tokens for authentication. These global policies are automatically assigned during deployment of the AIA services.

The global server policy name is `oracle/aia_wss_saml_or_username_token_service_policy_OPT_ON` and the global client policy name is `oracle/aia_wss10_saml_token_client_policy_OPT_ON`.

9.1.1 Verifying the Security Policies

To verify the security policies, perform the following steps:

1. Navigate to the WebLogic EM Console: *http://<server name>:<port number>/em/*.
2. Log in with the server admin user name. For access details, contact the system administrator.
3. Navigate to **Farm_soa_domain** > **SOA** > **soa-infra(<managed server name>)** > **default (<service_name>)**.

   The default managed server name is soa_server1.
4. Select an integration pack service for which the security policy needs to be verified.
5. On the right side, select **Policies**.
6. Verify that the security policy listed in the following table is applied for the service.

9.1.2 Policy Applied for Services Deployed

Refer to Table 9–1 for verifying the security policies.

By default, AIA applies global policies. Local policies will override global policies, where applicable.

For more information about security validation, see *Oracle® Fusion Middleware Developer's Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.6.0)*.

For Adverse Event: InForm and Argus Safety Integration, see *Oracle Health Sciences Adverse Event Integration Pack for InForm and Oracle Argus Safety Implementation Guide*.

Table 9–1 Security Policies

Service Name	Policy Name
ReportDrugSafetyReportResponseInFormProvABCSImpl	oracle/wss_username_token_client_policy is locally applied on Safety reference.

10

Undeploying Adverse Event: InForm and Argus Safety Integration

To undeploy Adverse Event: InForm and Argus Safety Integration from the SOA Server, perform the following steps:

1. Navigate to <AIA_HOME/aia_instances/<AIA Instance name>/bin and run the following command, as appropriate for your platform, to configure the installation environment.
   - Linux: `source aiaenv.sh`
   - Windows: `aiaenv.bat`
2. Run the undeployment command for your platform.

Table 10–1 Undeployment Command for the Adverse Event: InForm and Argus Safety

Platform	Undeployment Command
Linux Solaris SPARC	`ant -f $AIA_HOME/Infrastructure/Install/AID/AIAInstallDriver.xml -DPropertiesFile=$AIA_HOME/aia_instances/<AIA_Instance_name>/config/AIAInstallProperties.xml -DDeploymentPlan=$AIA_HOME/pips/AEInFormandArgus/DeploymentPlans/AEInFormandArgusUndeployDP.xml -l $AIA_HOME/pips/AEInFormandArgus/DeploymentPlans/AEInFormandArgusUnDeployDP.log`
Microsoft Windows	`ant -f %AIA_HOME%\Infrastructure\Install\AID\AIAInstallDriver.xml -DPropertiesFile=%AIA_HOME%\aia_instances\<AIA_Instance_name>\config\AIAInstallProperties.xml -DDeploymentPlan=%AIA_HOME%\pips\AEInFormandArgus\DeploymentPlans\AEInFormandArgusUndeployDP.xml -l %AIA_HOME%\pips\AEInFormandArgus\DeploymentPlans\AEInFormandArgusUnDeployDP.log`

Note: The undeployment script does not undeploy Shared JMS resources such as SECUREJDBCJMSServer (JMS Server), SECUREJDBCJMSModule (JMS Module), JMS Queues, SECUREJMSDS (Data Source), and SECUREDATASTORE (Persistent Data Store).

10.1 Verifying the Undeployment of the Integration

To verify the undeployment of the integration:

1. Navigate to the following log file path to check whether the integration is successfully undeployed:

```
$AIA_HOME/pips/AEInFormandArgus/DeploymentPlans/
AEInFormandArgusUndeployDP.log
```

If the undeployment was successful, the log file contains the 'Build Success' message. If the undeployment was not successful, the log file contains the 'Build Failed' message.

2. Restart the SOA server.

The following composites are removed by the undeployment command:

- HealthSciencesDrugSafetyReportEBS
- HealthSciencesDrugSafetyReportResponseEBS
- InFormDrugSafetyReportJMSProducer
- InFormDrugSafetyReportJMSConsumer
- ReportDrugSafetyReportInFormReqABCSImpl
- ReportDrugSafetyReportArgusProvABCSImpl
- ReportDrugSafetyReportWriteE2BFileAdapter
- ReportDrugSafetyReportReadAckFileAdapter
- ReportDrugSafetyReportResponseArgusReqABCSImpl
- ReportDrugSafetyReportResponseInFormProvABCSImpl

11

Uninstalling Oracle AIA

This section describes how to uninstall the PIPs and DIs included in pre-built integrations and the Foundation Pack. This section includes:

- Section 11.1, "Uninstalling the Pre-Built Integrations and the Foundation Pack"
- Section 11.2, "Uninstalling the Adverse Event: InForm and Argus Safety Integration"
- Section 11.3, "Cleaning the Environment"
- Section 11.4, "Verifying the Uninstall Processes"

Note: Before uninstalling, consider the impact on any customizations you have made.

11.1 Uninstalling the Pre-Built Integrations and the Foundation Pack

The AIA uninstaller removes the pre-built integrations and the Foundation Pack that were installed on your system.

To uninstall all applications in AIA_HOME using the undeployment plan, follow these steps:

1. Manually back up your customizations.
2. To undeploy the PIPs and DIs that belong to the pre-built integrations for your PIP or DI, launch the respective undeployment plan for your PIP or DI.
3. Launch the pre-built integrations OUI wizard, which is located at AIA_HOME/oui/bin. You must enter `./runInstaller -deinstall`.
4. On the Deinstall AIA Home screen, ensure that the AIA_Home shown is correct, then select **DEINSTALL**.
5. Exit the uninstaller.

11.2 Uninstalling the Adverse Event: InForm and Argus Safety Integration

You cannot uninstall a PIP or DI individually. Individual PIPs and DIs can only be undeployed by running their respective undeployment plans. For information on undeploying PIPs, see Chapter 10. When you run the Uninstall, it removes all individual integrations and the Foundation Pack installed in AIA_HOME.

11.3 Cleaning the Environment

To clean the environment, perform the following:

1. Navigate to the WebLogic console and click **Deployments** in the left navigation bar.
2. Select any AIA related deployments that exist and click **Delete**.
3. Repeat the previous step for Datasources, JMS modules, and JMS resources, if they exist.
4. Navigate to **Security Realms** and select your realm (myrealm).
5. Click the **Users and Groups** tab, then remove AIA users and AIA groups.
6. Shut down the SOA managed server, then shut down the Admin server.
7. Start the Admin server.
8. Open the console and verify whether you have any changes to activate in the **Activation** center. If there are changes, activate them. If they do not get activated, undo all changes.
9. Open the **Middleware/domains/<your_domain>** folder and remove the file **edit.lok**.
10. Open the **Middleware/domains/<your_domain>/pending** folder and remove all files.
11. Restart the SOA Server.
12. Attempt a fresh installation. Ensure that you have completed all pre-installation steps before attempting the installation.

11.4 Verifying the Uninstall Processes

If you chose to uninstall the AIA Home directory and its installed processes, navigate to the AIA Home directory and delete any residual files. You may have added files to the home directory that the AIA Pre-Built Integrations Installer did not automatically remove.

Also identify associated Oracle Enterprise Manager Fusion Middleware Control and SOA Composer services and confirm that these services are no longer shown in the Oracle Enterprise Manager Fusion Middleware Control and SOA Composer.