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

Installation Guide for On-Premise Deployment

Release 1.0.1

E36158-02

July 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 1.0.1

E36158-02

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 integration).

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 1.0.1 [this document]*
- *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Implementation Guide Release 1.0.1*
- *Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Security Guide Release 1.0.1*

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.

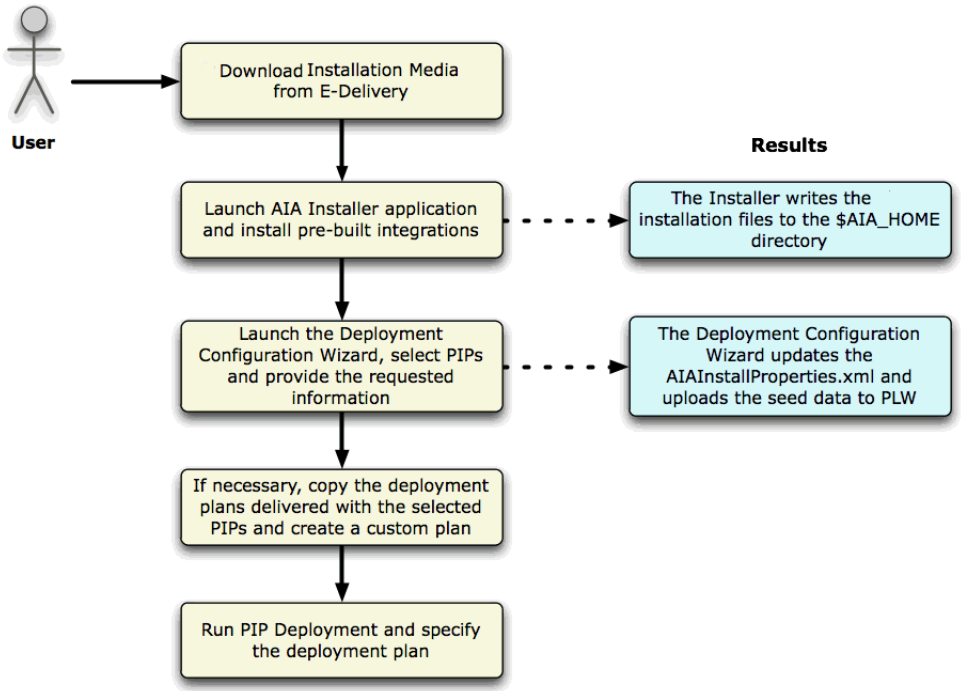
1

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) and enables you to install the integration. The installer is platform independent.

You can also use the installer to uninstall the integration.

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-certific

ation-100350.html and download the xls file.

The Deployment Configuration Wizard (DCW) defines the configurations needed for each pre-built integrations 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 DCW helps you configure the integration. This section discusses various configuration options and screens that appear.

When you configure the integration, DCW prompts for the integration specific information.

- When configuring the integration over an existing configuration, which has one or more integrations, and the new integration selected 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, and integration2 shares a participating application with integration1 such as Argus Safety, then DCW shows the captured details and asks you to overwrite or not. 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 get delivered when you install the integration. However, the routing rules implementation can differ depending upon the various installation scenarios.

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

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

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

For more information about how to use these delivered 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

There are several installation and deployment topologies possible using the installer. Choose the installation that best suits your need. For more 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 given direct or process integration when installed through the installer. After installing using the installer, you can configure pre-built integrations to connect to multiple instances. For details on configuring more than one instance of a participating application, see this integration's Implementation Guide.

3

Pre-built Integration Deployment

This section discusses the deployment of the pre-built integration included in this release.

The deployment of a pre-built integration is done through the deployment plan. The deployment plan and the configured AIAInstallProperties.xml are passed as parameters to the AIA Install Driver (AID) for deployment.

You must configure the AIAInstallProperties.xml with the corresponding pre-built integrations Server details using the Configuration Wizard. AID does not perform any checks to validate the AIAInstallProperties.xml has been configured with the corresponding pre-built integrations Server details.

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 AID with the configured AIAInstallProperties.xml. 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 DIs when neither is part of a pre-built integration group. Before you install multiple PIPs or DIs on a single 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 functional impact or common PIP or DI components, such as common routing rules.

3.2 Pre-built Integration Undeployment

The undeployment of the PIP is done through the undeployment plan. The undeployment plan and the configured AIAInstallProperties.xml are passed as parameters to AID for undeployment.

The generated deployment plan generates an undeployment plan with the install deployment plan.

4

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 7.0.1 or 7.0.2
- Oracle® Application Integration Architecture (AIA) Foundation Pack Release 11.1.1.6

  Roll-up Patch (RUP) 16542319
- InForm Publisher 1.0.3
- InForm Adapter 1.3.6.1 (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
- Service-Oriented Architecture (SOA) Suite patch 14137846 and 14630316

5

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.

Backup 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 the Patch on top of AIA Foundation Pack 11.1.1.6.

Argus File Structure:

- Create a file structure in 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 in 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 all the processed acknowledgement files.

  For 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 Multi-tenant Argus installation, within each of these directories, there are sub-directories for each enterprise. In the following sample folder structure, <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 enables file adapters on SOA_Server to exchange the files with the Argus Safety system. The SOA server must be able to access in, out, and ack-archive directories of Argus Interchange (Argus ESM) server.
- Create a folder for archiving the files. For example, C:\INF-ARG-INTEGRATION\Archive.
- 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 SOA server is on a Linux environment:

  On SOA server, create a folder. For example, the Argus Interchange server will 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 the Operating System (OS) level security. On the Argus Interchange server, only the owner and the group (administrator) will have read and write access to the file. The user who

logs in as well as shares the folder with should have local administrator rights.

5.1 Enabling SSL on SOA Server

You need to enable SSL on the SOA server for the following reasons:

- Since patient data is sent in the message from InForm Publisher to the SOA server, Oracle recommends that you utilize https to send the data.
- Default SOA server endpoint has a global policy that requires SAML or user name token authentication. InForm publisher sends user name token in the SOAP header. To pass the user name token in the SOAP header, InForm Publisher requires SSL enabled SOA server endpoint.

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

5.2 Configuring SOA Server to Invoke InForm Adapter Over HTTPS

To invoke InForm Adapter in secure mode, perform the following:

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 keystores.

   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 in the SOA server machine.

      For example, copy 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, then 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: startWebLogic.sh requires the location of the custom trust keystore and hence modifying this script is necessary.

---

h. Restart 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 being 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 key store. The name of this key will be entered on a screen in the Configuration Wizard.

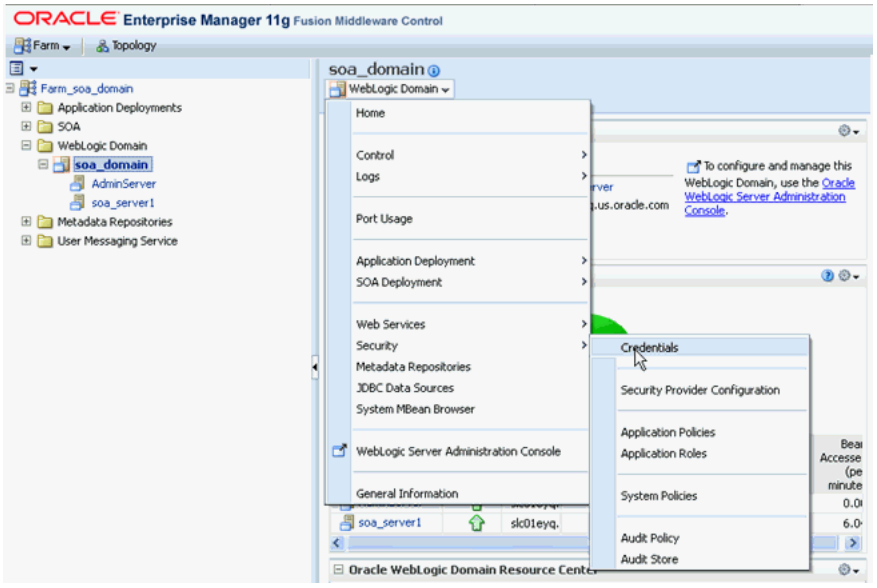
If you use different users per trial, follow the instructions provided in the Oracle Health Sciences Adverse Event Integration Pack for Oracle Health Sciences InForm and Oracle Argus Safety Implementation Guide for setting up a trial for this integration.

a. Open Enterprise Manager.

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

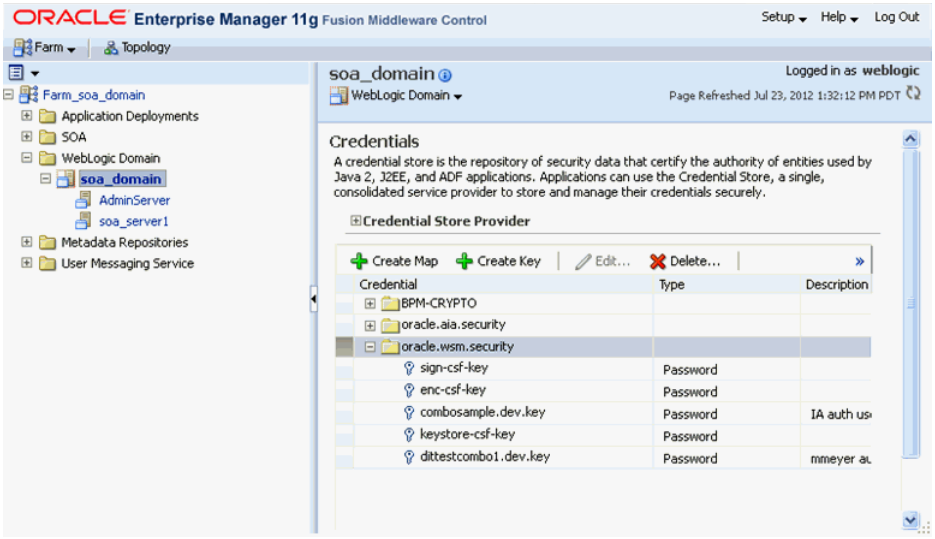
c. Click on the WebLogic Domain drop-down box and select **Security > Credentials**.

Figure 5–1 WebLogic Domain



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

Figure 5–2 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.

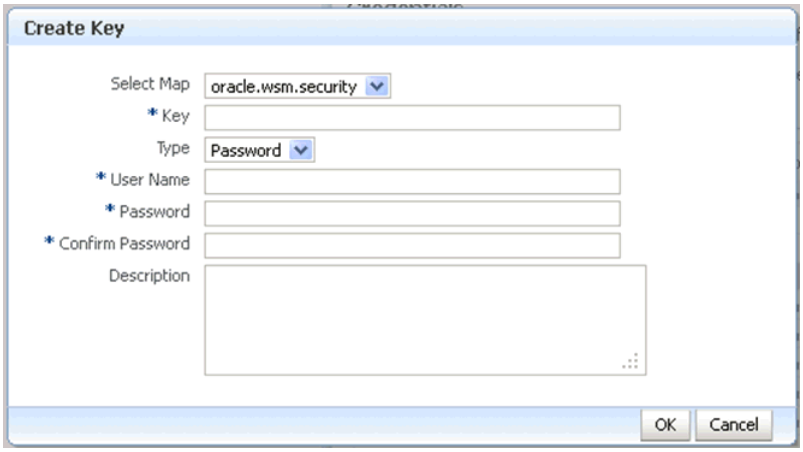
c. Right-click the domain name, click **Security**, then **Credentials**.

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.

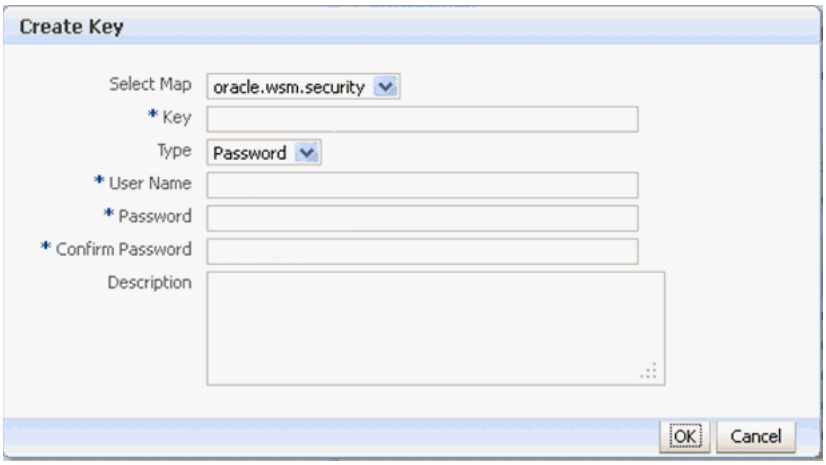
Figure 5–3 Create Key



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 5–4 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 will read the value in the AIAConfigurationProperties.xml file, which is applicable to all trials on the SOA server. Integration pack obtains credential information from the credential store through the key value. The credentials are then passed to the SOAP header when invoking InForm Adapter in secure mode.

5.3 Verifying Wildcard Hostname

If you are using wildcard certificate for https communication, you must enable verifying wildcard hostnames on the SOA server. To configure, perform the following steps:

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**.

5.4 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:

- **Backup custom extensible style sheet language transformations (XSLTs)**: These are the extensions performed on the AIA Transformation style sheet. Oracle AIA

does not contain any XSLTs for its components and utilities. As the process content is delivered only in PIPs, you must manually backup the XSLTs if you have developed any for the custom integrations, and reapply them as a post install step.

- **Backup custom routing rules in the (EBS)**: If you have defined any routing rules on any of the EBS available as part of the PIP, on top of the rules provided ready-to-use, you must manually take a back up of the EBS. You must merge the EBS manually as a post installation step.
- **Backup 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.

6

Configuration Wizard

The configuration wizard screens prompt you to enter the data required for successful configuration of the Adverse Event: InForm and Argus Safety integration. Enter the details of the Adverse Event: InForm and Argus Safety integration screens below, take a printout and keep it ready when you run the configuration wizard. This enables faster and error free configuration.

6.1 Pre-Built Integration Server Details Screen

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

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

Field	Description
Admin Host Name	This is 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	This is 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	This is WebLogic server domain where SOA server is created. For example, `domain1` The Domain Name is _____
Admin User	This value is the WebLogic admin user name. To find this value, contact your WebLogic administrator. The Admin Username is _____
Admin Password	This value is 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 populates with managed servers for the domain. Select the managed server from the list. If you are deploying the integration to a SOA cluster, you should select the cluster name in this field. 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 in the list.

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 Argus Safety application is hosted or not. If this check box is selected, Argus Safety is hosted by Oracle.
Interchange Files Root Directory Path	This is 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	This is the full file path of E2B+ DTDs on the Argus server. The DTD Directory Path is _____
Argus Database ID	Unique identifier for the Argus Safety database. The Argus Database ID is _____

6.3 InForm and InForm Adapter Details Screen

You can use this screen to enter details related to your InForm application instance.

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 or not. If this check box is selected, InForm is hosted by Oracle.
InForm Internet Protocol	For example: `https://`
InForm Hostname	This value is 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	This value is 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://`
InForm Adapter Server Hostname	This value is the fully-qualified machine name of the InForm Adapter Server host. Enter this value if all trials use the same URL to access InForm Adapter.
InForm Adapter Server Port	This value is 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	This value is the path to InForm Adapter Web service. Enter this value if all trials use the same URL to access InForm Adapter. For example, the URL for InForm Adapter Server Path is `http://<hostname>/informadapter/safety/safety.svc`. The InForm Adapter Server path is `<informadapter>`.

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

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

7

Installing the Adverse Event: InForm and Argus Safety

This chapter contains the following topics:

7.1 Installing the Adverse Event: InForm and Argus Safety

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

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 the **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, which lists prerequisites and information about how to begin the installation process.

5. Click **Next**.
6. Wait for the prerequisite checks to complete and then click **Next**.

   The following prerequisite system checks are performed:

   - Operating system certification

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

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

   The Installation location screen is displayed.

8. Select AIA Home where 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 do the 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 <Oracle
    Home>/Middleware/jdk160_24/jre -silent -response <Oracle Home>/11.1_Installer_
    response.xml
    ```

11. Click **Install**.

    A warning message is displayed indicating that any customizations would 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 backup AIA_HOME and preserve customizations, see Section 5.4.

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 the Adverse Event: InForm and Argus Safety

The Configuration Wizard screens will prompt you to enter the data that is required for successful configuration of the Adverse Event: InForm and Argus Safety. Keep the completed worksheet of the Configuration Wizard screens ready before you launch the configuration wizard. For more information, see Chapter 6.

To configure the Adverse Event: InForm and Argus Safety:

1. Navigate to <AIA_Instance>/bin and run the following command as per your platform to configure the installation environment:

   - On Linux: `source aiaenv.sh`

- On Windows: `aiaenv.bat`

2. Navigate to <AIA_HOME>/bin and run the following command as per your platform:
   - On Linux: `./aiaconfig.sh`
   - On Windows: `aiaconfig.bat`

   This launches the AIA Configuration Wizard.
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**.

7.2.1 Specify Pre-Built Integration Server Details

To specify Pre-Built Integration Server details:

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

7.2.2 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**.

7.2.3 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**.

7.2.4 Complete Configuration

To complete configuration:

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

   If you want to make changes to the configuration before starting the installation, use the navigation pane on the left and select the topic you want 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 this configuration and begin the installation.

   The system displays progress of the configuration in the Configuration Progress screen.

   The system displays any warnings or errors 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 AIA Configuration Wizard displays the Configuration Complete screen.

4. Click **Finish** to close the configuration wizard.

5. AIAInstallProperties.xml file is updated; this file is located under `<AIA_HOME>/aia_instances/<AIA_instance_name>/config` folder. Use this file for deploying the integration pack on SOA server.

7.3 Configuring the Adverse Event: InForm and Argus Safety Using Response File

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

1. Open the response file.

   When you create a response file through Oracle Universal Installer (OUI), passwords get 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 to configure the environment:

   - On Linux: `source aiaenv.sh`
   - On Windows: `aiaenv.bat`

4. Navigate to <AIA_HOME> / bin and run the following command:

   - On Linux: `./aiaconfig.sh <Response File Location and Name>`
   - On Windows: `aiaconfig.bat <Response File Location and Name>`

7.4 Configuring Pre-deployment Security for InForm-Argus Safety

The InForm-Argus Safety integration stores messages containing the 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 for InForm-Argus Safety, perform the following:

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. For creating a wallet that is used by the TDE encryption, follow the instructions in the *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 sqlnet.ora 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 sqlnet.ora file.
4. Navigate to the folder <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. Connect to the database as a user with SYSDBA role using SQL*Plus.

   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. A secure tablespace is created upon successful execution of the script.
10. Exit SQL*Plus.
11. Connect to the database as a user with <AIA_INSTANCE>_JMSUSER role using SQL*Plus.

    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
    ```

    A secure tablespace is created in <AIA_INSTANCE>_JMSUSER schema upon successful execution of the script.

13. Exit SQL*Plus.

7.5 Deploying the Adverse Event: InForm and Argus Safety

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

To deploy the integration to SOA Server, run the following commands specific to your platform.

1. Navigate to `<AIA_HOME/aia_instances/<AIA_instance_name>/bin` and perform the following:
   - On Linux: `source aiaenv.sh`
   - On 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 which can be used in your integrations. You can modify these native artifacts or add new natively supported artifacts using AIA Lifecycle Workbench and 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 now deploy third party technology artifacts which 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 InForm - Argus Safety integration, which includes:

- Section 8.1, "Creating a User in Oracle WebLogic Server"
- Section 8.2, "Creating File Adapter Control Directory in Oracle WebLogic Server"
- Section 8.3, "Enabling Customization"
- Section 8.4, "Installing Patch Set"
- Section 8.5, "Setting Up Argus E2B Profile"
- Section 8.6, "Configuring Argus Safety for Using Extension Profile"
- Section 8.7, "Configuring Folders for XML File Sharing"
- Section 8.8, "Changing Parameters on the SOA Server"
- Section 8.9, "Disabling Acknowledgment Flow"

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

Note: Ensure to install the patch set 1.0.1 for the integration. You can download it from MOS as patch 16523094.

8.1 Creating a User in 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:

1. Navigate to WebLogic console.
2. Under Domain Structure of **soa_domain**, select **Security Realms**, then select **myrealm**.
3. Select the **Users and Groups** tab, and then select the **Users** tab.
4. Click **New**.

5. In the **Name** field, enter the user name the 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**.

8.2 Creating 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. It is required to create a control directory for File Adapter high availability when 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, control directory ensures that there is only one composite instance per incoming file.

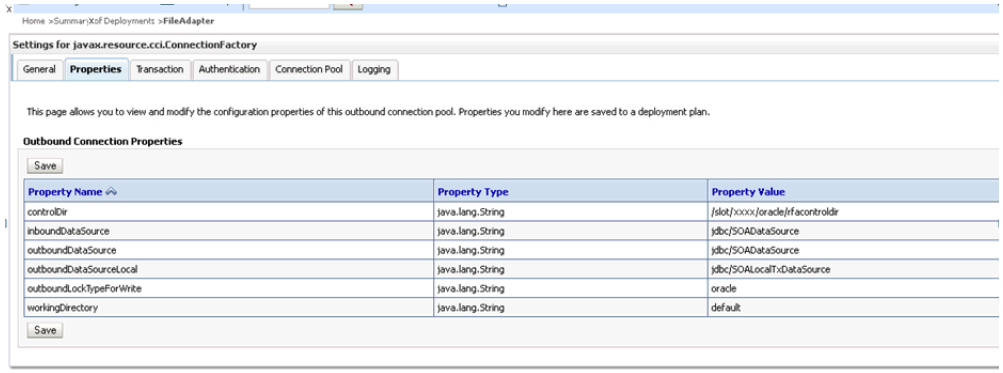
1. Log in to Oracle WebLogic Server Administration Console.

   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 for the connection factory corresponding to high availability is displayed.
7. Update the **controlDir** property:
   - Set the property to the directory structure where the control files can be stored.

     This must be set to a shared location if multiple WebLogic Server instances run in a cluster. The directory specified must be write accessible to all WebLogic server instances.
   - Specify the directory path in the controlDir property.
   - Press **Enter** after updating the controlDir property.

Figure 8–1 Outbound Connection Properties



8. Click **Save**. Save the deployment plan when prompted.

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

8.3 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*.

8.4 Installing Patch Set

You must install the following patch set for the integration before proceeding with post-installation steps: Patch 16523094. 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 1.0.1 Patch Set Readme*.

For any questions or problems, contact Oracle Support for AIA.

8.5 Setting Up Argus E2B Profile

Argus Interchange server is used for this integration.

If you are using the Multi-tenant feature of Argus Safety, create the following:

- Reporting destination for each enterprise.
- One in, out, and ack-archive directories for placing E2B+ and acknowledgement files. Within each of these directories, create sub-directories for each enterprise.

For information about directories, see Chapter 5. Ensure that the following setup is completed on the Argus Interchange server.

Note: Ensure to install the Adverse Event: InForm and Argus Safety integration patch set 1.0.1 before setting up the Argus E2B profile. Check MOS for the most recent patches.

To set up Argus E2B Profile, perform the following:

1. Navigate to the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile` and copy the **ich-icsr-v2.1-FDA-PIP.dtd** file to the Interchange server folder `<Oracle_Home>\Argus\InterchangeService\DTDFiles\`.

Note: Argus DTD is updated to have more extension fields to support custom extensions and non-custom, non-E2B fields.

---

2. Copy all the files from the SOA_Server directory `<AIA_HOME>/data/AEInFormandArgus/sql/ArgusProfile` to a folder on 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.

4. Run the batch file **Setup_Safety_Integration_Profile.bat**. These scripts will import all custom extension fields, and non-custom or non E2B extension fields that are added to integration specific DTD.

   Note: Run the batch file **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 the log file path (C:\Temp_config_folder\profilecreationoutput.log).

   Note: If Argus Safety is installed in the Single-tenant mode, you do not have to provide the enterprise short name. Press **Enter**.

6. Press **Enter**.

8.5.1 Updating an Existing Argus Profile

Note: Please perform the following steps only if you have already created ICH-ICSR V2.1 MESSAGE TEMPLATE - FDA PIP Argus profile, before applying Patch set described in Section 8.4, "Installing Patch Set".

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

- Create an Argus profile before applying the patch set
- Upgrade Argus Safety from 7.0.1 to 7.0.2 after applying the patch set

You can update an existing Argus profile using the following steps:

1. 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` to a temporary directory on the Argus Interchange server.
2. On the Argus Interchange Server, open ESM Mapping Utility.

   You must select a specific enterprise name for Multi-tenant Argus.
3. Select `Profile - ICH-ICSR V2.1 MESSAGE TEMPLATE - FDA PIP` from the Profile drop-down list.
4. Select **Administrator** and then **Delete Profile**.

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

5. Click **Yes**.

   The following error message is displayed on 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.
```

This error may be ignored by clicking on **Continue**, because you are deleting the profile that is being referred in the reporting destination configuration on Argus Console. In the next steps below, the profile is created again and hence reporting destination's reference to the profile will be intact.

6. Click **Continue**.
7. Open the command prompt and navigate to the temporary directory where the Argus 7.0.2 profile creation scripts are copied.
8. Run **Setup_Safety_Integration_Profile.bat**.

   These scripts will import all custom extension fields, and non-custom or non E2B extension fields that are added to integration specific DTD.
9. Enter the database name, enterprise short name, ESM owner's user name (for example, esm_owner), password, and the log file path (for example, C:\Temp_config_ folder\profilecreationoutput.log).

   Note: For Single-tenant Argus, you do not have to provide the enterprise short name. Press **Enter**.
10. 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 same data into these tables.
11. After the script completes, the profile is updated for the Argus7.0.2 E2B import process.

8.6 Configuring Argus Safety for Using Extension Profile

To configure Argus Safety for using the extension profile, perform the following:

1. Open the Argus Console.
2. Navigate to the **Reporting Destination** folder from the Browser.
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 Description

Fields	Description
Agency Name	Enter INFORM-ARGUS-INTEGRATION. Note that this agency is being added for the integration only and should not be used for sending reports to any regulatory agencies. The E2B files received by this agency cannot be sent in the same format to the regulatory authorities such as FDA. You need to modify the sequence of standard E2B fields. For example, positions of companynumb element and primarysourcecountry element have been swapped to ensure that we have companynumb element in all acknowledgement files that are auto-generated by Argus due to M2 validation failure.
Report for Marketed Licenses	This field contains default value **Always**.
Report for Investigational Licenses	This field contains default value **Always**.

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

Table 8–2 Local Company Contact Tab Field Description

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

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

Table 8–3 EDI Tab Field Description

Fields	Description
SGML or XML	Select **XML**. This field represents the format of incoming E2B and outgoing acknowledgement files.
Agency Identifier	Enter **INFORM_01**. This value should match sender identifier in E2B file.
Company Identifier	Enter **ARGUS_01**. This value should match receiver identifier in E2B file.
Method	Select **E2B-XML transmission** from the list.
Message Profile	Select the ICH ISCR 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 in the URL of Message DTD field. 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 in the URL of ACK DTD field. 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 E2B extension for the selected agency.

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

8.7 Configuring Folders for XML File Sharing

For the exchange of E2B and acknowledgement files between Argus Safety and SOA Server, you must create folders and configure them. For folders' details, see Chapter 5.

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

To configure the folders, perform the following:

1. On Argus ESM Server, open ESM Mapping Utility. To open the ESM Mapping Utility, 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 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.

> **Note:** If 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 8–4.

6. Select the database name (for example, AS70xx). This opens the Service DB Setup screen.
7. In the System Directories pane, select **INFORM-ARGUS-INTEGRATION** from the list.

Table 8–4 Field Description of Service DB Setup Screen

Fields	Description
Database Section	
Enterprise Short Name	Select the enterprise short name. For example, ent1
Database Name	Enter the database name. For example, AS70xx
Unique Database ID	Enter unique database ID. For example, 123

Table 8–4 (Cont.) Field Description of Service DB Setup Screen

Fields	Description
User ID	Enter the database user name.
Password	Enter the database password.
Process	Enter `C:\Program Files\Oracle\Argus\InterchangeService\EsmProc.exe`.
Receive Process	Enter `C:\Program Files\Oracle\Argus\InterchangeService\E2BReceive.exe`.
Archive Folder	Select the folder for archiving the files. You had created this folder as one of the Prerequisites listed. For example, `C:\INF-ARG-INTEGRATION\Archive`.
Receive Processes	Enter the value as `1`.
Process Elapse Time	Enter the value of `1 minute`.
Time Out Section	
EDI Transmit Time Out value (File is not picked up by Gateway)	Enter time out value as `10 minutes`.
Physical Media Transmit Time Out value (File is not picked up manually)	Enter time out value as `10 minutes`.
Receive ACK Time Out value (ACK is due for transmitted reports)	Enter time out value as `10 minutes`.
Processing Time Out value (E2B Report not Processed by User)	Enter time out value as `10 minutes`.
XML Transmit Time Out value (File is not picked up by Gateway)	Enter time out value as `10 minutes`.
Binary Transmit Time Out value (File is not picked up by Gateway)	Enter time out value as `10 minutes`.
MDN Time Out Value (For E2B Reports which have received Bus ACK)	Enter the value `0 hours`.
System Directories Section	
Agency Name	Select INFORM-ARGUS INTEGRATION agency configured in the Argus Console, Reporting Destination.
Local Company	This value is displayed based on Reporting Destination Configuration.

Incoming Folder	Specify the folder path for incoming files.
	You had created this folder as one of the Prerequisites listed.
	For example,
	For Multi-tenant Argus, agencies from two different enterprises cannot share the same folder for incoming E2B files. Therefore, it is necessary to have the following folder structure in the file system:
	Incoming files
	`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:
	Incoming files
	`C:\<FILE_EXCHANGE_DIR_ROOT>\in`

Table 8–4 (Cont.) Field Description of Service DB Setup Screen

Fields	Description
Outgoing Folder	Specify folder path for outgoing files. You had created this folder as one of the Prerequisites listed. For example, For Multi-tenant Argus, the folder structure is as follows: Outgoing files 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: Outgoing files C:\<FILE_EXCHANGE_DIR_ROOT>\out

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

8.8 Changing Parameters on the SOA Server

8.8.1 Changing Parameters to Increase Performance

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

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** and then select **Mediator Properties**.
4. Change the default value of ResequencerLockerThreadSleep from 10 to 1.

8.8.2 Changing Default Values of Transaction Timeout

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

1. Log in to 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 as the default JTA transaction timeout value may not be enough to complete transaction.

   Ensure to increase this value to be large enough to complete your transactions but not so large that it will impact performance.
5. Oracle recommends you to increase the Extended Architecture (XA) Transaction timeout for XA data source as mentioned in http://docs.oracle.com/cd/E28271_01/admin.1111/e10226/soainfra_config.htm#BHCDIBCE.

In the clustered SOA server environment, perform the following configurations to ensure 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** and then select **Common Properties**.

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

   Note: Ensure to use the ending backslash (/), otherwise the function will not work correctly.

2. Open the WebLogic Console.

   a. Navigate to **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: Specify the host DNS address of the load balancer.

   Frontend HTTP Port: Specify 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 node manager, admin, and SOA servers.

8.9 Disabling Acknowledgment Flow

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

- ReportDrugSafetyReportReadAckFileAdapter
- ReportDrugSafetyReportResponseArgusReqABCSImpl
- HealthSciencesDrugSafetyReportResponseEBS
- ReportDrugSafetyReportResponseInFormProvABCSImpl

8.9.1 Shutting Down the Services

To shut down the services, perform the following:

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 will be displayed.

4. Click on the service you want to shut down and click **Shut Down**.

5. Click **Yes** in the confirmation window.

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

9

Verifying Installation

To verify the Adverse Event: InForm and Argus Safety installation:

1. Open the log files from the following location and look for warnings and error messages:
   - For Linux and Solaris SPARC based systems: Review the install log located at <AIA_HOME>/aia_instances/<AIA_Instance_name>/logs to verify that the integration is successfully installed.
   - For Windows: Review the install log located at <AIA_HOME>\aia_instances\<AIA_Instance_name>\logs to verify that the integration is successfully installed.
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 items listed below.
      * HealthSciencesDrugSafetyReportEBS
      * HealthSciencesDrugSafetyReportResponseEBS
      * InFormDrugSafetyReportJMSProducer
      * InFormDrugSafetyReportJMSConsumer
      * ReportDrugSafetyReportInFormReqABCSImpl
      * ReportDrugSafetyReportArgusProvABCSImpl
      * ReportDrugSafetyReportWriteE2BFileAdapter
      * ReportDrugSafetyReportReadAckFileAdapter
      * ReportDrugSafetyReportResponseArgusReqABCSImpl
      * ReportDrugSafetyReportResponseInFormProvABCSImpl

9.1 Validating Security Policies

This integration pack fully leverages the security infrastructure provided by the Oracle 11g SOA Suite, AIA Foundation Pack, and the underlying transport layer security features for Web Service security. This is implemented through Foundation Pack by

assigning 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:

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 security policy needs to be verified.
5. On the right hand side, select **Policies**.
6. Verify 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 implementation, see *Oracle Health Sciences Adverse Event Integration Pack for InForm and Oracle Argus Safety 1.0 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 the Adverse Event: InForm and Argus Safety

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

1. Navigate to <AIA_HOME/aia_instances/<AIA Instance name>/bin and run the following commands to configure the installation environment.
   - On Linux: `source aiaenv.sh`
   - On 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. The log file contains the 'Build Success' message, if the undeployment is successful. If the undeployment is not successful, the log file contains the 'Build Failed' message:

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

2. Restart the SOA server.

The following composites are removed after the undeployment command is run:

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

11

Uninstalling Oracle AIA

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

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

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

11.1 Uninstalling Pre-Built Integrations and Foundation Pack

The AIA uninstaller removes the pre-built integrations and Foundation Pack installed on your system. To uninstall all applications in AIA_HOME using the undeployment plan:

1. Manually back up your customizations.
2. Undeploy all the PIPs and DIs that belong to the pre-built integrations by launching the respective undeployment plan for your PIP or DI.
3. Launch the pre-built integrations OUI wizard. This is located at AIA_HOME/oui/bin. You must enter `./runInstaller -deinstall`.

   On the Deinstall AIA Home screen, ensure that the AIA_Home shown is correct and select **DEINSTALL**.
4. Exit the uninstaller.

11.2 Uninstalling the Adverse Event: InForm and Argus Safety

A PIP or DI can never be uninstalled individually. Individual PIPs or DIs can only be undeployed by running its respective undeployment plan. For more information on undeploying the PIP, see Chapter 10. When you run the Uninstall, it removes all individual integrations and Foundation Pack installed in AIA_HOME.

11.3 Cleaning the Environment

To clean the environment, perform the following:

1. Navigate to WebLogic console and click **Deployments** in the left navigation bar.

2. Select all AIA related deployments if they exist (ideally they get removed during uninstallation) and click **Delete**.
3. Repeat the above step for Datasources, JMS modules, and JMS resources if they exist.
4. Navigate to **Security Realms**, select your realm (myrealm).
5. Click the **Users and Groups** tab and remove AIA users and AIA groups.
6. Shutdown the SOA managed server and then shutdown 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 any, activate them. If they do not get activated undo all changes.
9. Open the folder **Middleware/domains/<your_domain>** and remove the file **edit.lok**.
10. Open the folder **Middleware/domains/<your_domain>/pending**, and remove all files.
11. Restart the SOA Server.
12. Attempt a fresh installation. Ensure that you have completed all preinstallation steps before attempting the installation.

11.4 Verifying 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 additional 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.