Oracle® Device and Drug Adverse Event Data Integration Pack for Siebel Adverse Event Complaint Management and Oracle Argus Safety

Installation Guide

Release 11.1

E26804-02

April 2012

This guide discusses how to install the Oracle Device and Drug Adverse Event Data Integration Pack for Siebel Adverse Event Complaint Management and Oracle Argus Safety. This guide includes the following sections:

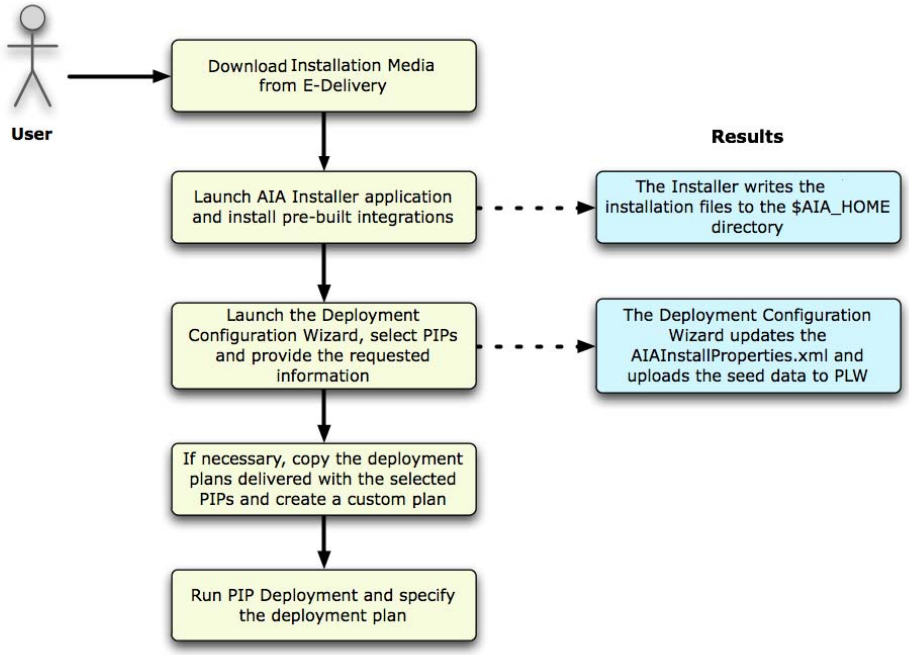
- Section 1, "Pre-built Integration Installation"
- Section 2, "Pre-built Integration Configuration"
- Section 3, "Pre-built Integration Deployment"
- Section 4, "Software Requirements"
- Section 5, "Installing the Device and Drug Adverse Event: Siebel AECM and Argus Safety"
- Section 6, "Configuration Wizard"
- Section 7, "Installing the Device and Drug Adverse Event: Siebel AECM and Argus Safety"
- Section 8, "Performing Post-Installation Configurations"
- Section 9, "Verifying Installation"
- Section 10, "Undeploying the Device and Drug Adverse Event: Siebel AECM and Argus Safety"
- Section 11, "Uninstalling Oracle AIA"
- Section 12, "Documentation Accessibility"

1 Pre-built Integration Installation

The Device and Drug Adverse Event: Siebel AECM and Argus Safety PIP installation consists of three stages:

- Installation
- Configuration
- Deployment

Figure 1 Illustrates the flow of the pre-built integration installation


User
Download Installation Media from E-Delivery
Launch AIA Installer application and install pre-built integrations
Launch the Deployment Configuration Wizard, select PIPs and provide the requested information
If necessary, copy the deployment plans delivered with the selected PIPs and create a custom plan
Run PIP Deployment and specify the deployment plan
Results
The Installer writes the installation files to the $AIA_HOME directory
The Deployment Configuration Wizard updates the AIAInstallProperties.xml and uploads the seed data to PLW

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-certification-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 Section 2, "Pre-built Integration Configuration"

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 Section 3, "Pre-built Integration Deployment"

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 Siebel Life Sciences, then DCW shows the captured details and asks you to overwrite or not. If you choose not to overwrite then 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 are deployed with all default routing rules.

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

The routing rules for this integration are available in `AIA_HOME/pips/DrugDeviceAESEBLandArgus/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. Refer to the whitepaper *AIA Installation and Deployment -Strategies, Topologies and Flexibilities* on www.oracle.com for more details.

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. Refer to *Oracle Device and Drug Adverse Event Data Integration Pack for Siebel Adverse Events and Complaints Management and Oracle Argus Safety Implementation Guide* for details on configuring more than one instance of a participating application.

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 Un-Deployment

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

The generated deployment plan generates an un-deployment plan with the install deployment plan.

4 Software Requirements

The Device and Drug Adverse Event: Siebel AECM and Argus Safety requires:

- Argus Safety 6.0.3
- Siebel AECM 8.1.1.6 with Quick Fix No. 0601 for ACR 712

  Instructions in Siebel 8.1.1.x MRG for ACR 712 must be followed.

> **Note:** While this section lists a specific fix pack (FP) or patch set (PS) for a given supported participating application version, Oracle recommends that when you are ready to implement the integration, you obtain the latest FP or PS for the respective applicable participating application version as specified in the AIA Certification Matrix.

5 Installing the Device and Drug Adverse Event: Siebel AECM and Argus Safety

This section describes how to install Device and Drug Adverse Event: Siebel AECM and Argus Safety 11.1 using the Installer.

5.1 Prerequisites

- Install AIA Foundation Pack 11.1.1.5 with RUP 13247584 before you install the Device and Drug Adverse Event: Siebel AECM and Argus Safety PIP. 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`, download the latest version and install it. This guide is constantly updated and bug fixed.
- Make a backup of any customizations. If you do not create a backup, your customizations are overwritten.

  For more information about backing up your customizations, see Section Section 5.2, "How to Create Backups of your Customizations".
- The SOA server must be able to access in and out directories of Argus Interchange (Argus ESM) server.

  Create a mount point between the parent folder of incoming and outgoing folders and SOA_Server. This enables file adapters on SOA_Server to exchange the files with the Argus Safety system.

  Consider the information provided here for creating the folders, and assigning permissions to the folders for enabling the file sharing:

  Create a folder in Argus ESM Server. (For example: C:\AECM-Argus-Int). The parent folder should have two subfolders named **in** and **out**. In addition to this, there can be an **Archive** folder that is used by Argus for archiving the XML files. You need to create a folder named **archive** underneath the **out** directory. This is required by the PIP to move the acknowledgement files once they have been read. Example for creating the folder structure:

  - C:\AECM-Argus-Int\in
  - C:\AECM-Argus-Int\out
  - C:\AECM-Argus-Int\out\archive
  - C:\AECM-Argus-Int\Archive

  You can use a pre-existing **Archive** folder, if it is available. This folder is used by Argus to archive the XML files. A database connection can have one **Archive** folder and this folder is not mounted. Multiple agencies that are configured as part of same database connection share the same Argus **Archive** folder.

  Argus ESM Server user needs read and write permissions to the folders. Assign read and write permissions to these folders:

  - C:\AECM-Argus-Int\in
  - C:\AECM-Argus-Int\out
  - C:\AECM-Argus-Int\out\archive

  Consider the following if SOA_Server is on a Linux environment:

  On SOA_server, create two folders for sending input to Argus Safety and receiving output files from Argus Safety. For example,

  - /<oracle_home>/ArgusSafety/in
  - /<oracle_home>/ArgusSafety/out

Mount the new directory that you created on the SOA_server (For example, <oracle_home>/ArgusSafety) to the new directory you created on the ESM Server (For example, c:\AECM-Argus-Int).

The soa_server user must have permissions to read from and write to these SOA_ Server folders.

Consider the following if both Argus Safety and SOA_Server are on Windows environment:

Create a fileshare between SOA_Server and Argus Safety. For example, map SOA_ Server's network drive. (Example: Z:) to Argus Safety's C:\AECM-Argus-Int so you can access SOA_Server mapped network drive folders such as:

- Z:\AECM-Argus-Int\in
- Z:\AECM-Argus-Int\out

5.2 How to Create Backups of your Customizations

This section discusses the key tasks that you must perform before you perform the installation of 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. 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 the XSLTs if you have developed any for the custom integrations, and reapply them as a post install step.
- **Back up 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 out of the box, you must manually take a back up of the EBS. You must 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.

6 Configuration Wizard

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

6.1 PIP Server Details Screen

All artifacts associated with the PIP infrastructure components will be deployed to the PIP server. This screen contains the following fields.

Table 1 PIP 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. 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. Example: `7001`. The Admin Port is ______________________________
Domain Name	This is WebLogic server domain corresponding to the Admin Server. Example: `domain1` The Domain Name is ___________________________
Admin User	This value is the WebLogic admin username. To find this value contact your WebLogic administrator. The Admin User 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 PIP to a Service-Oriented Architecture (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 Siebel Life Sciences Server Details

Use this screen to enter details related to your Siebel Adverse Event Complaint Management System Server instance.

The screen contains the following fields:

Table 2 Siebel Life Sciences Server Details Screen Fields

Field	Description
Siebel Hostname	This value is the fully-qualified computer name of the Siebel AECM host. Example: example1.corp.siebel.com Siebel Hostname is ________________
Siebel Http Port	This value is the Siebel AECM application port. To find this value, contact your administrator. For example: 80 Siebel Http port is ________________
InternetProtocol	This value is the Siebel host internet protocol. Example: https:// **Important:** Oracle strongly recommends that you use https secure protocol since Siebel contains information about patient adverse events.

Table 2 (Cont.) Siebel Life Sciences Server Details Screen Fields

Field	Description
Siebel Enterprise Server Name	This value is the Siebel enterprise server name. To find the value, contact your administrator. For example, siebel. Siebel Enterprise Server Name is ___________
Siebel EAI Application User	This is the Siebel user the integration uses to make EAI Web service calls. To find this value, contact your administrator. Example: sadmin Siebel EAI Application User is _____________
Siebel EAI Application Password	This is the password for the EAI user. To find the value, contact your administrator. Siebel EAI Application Password is _________
Siebel Version	This is the version of the Siebel application. Siebel Version is __________
Siebel Language	This is the language used by the Siebel application. To find the value, contact your administrator. Example: enu

6.3 Argus Safety Server Details

Use this screen to enter details related to the Argus database and Argus ESM server.

The screen contains the following fields:

Table 3 Argus Safety Server Details Screen Fields

Field	Description
Case Directory Path	This is the full path to the directory on the SOA server that is mapped or mounted to the directory on the Argus ESM server where the XML files will be written. *Note that the path provided in this field must be soa_server path and not the Argus ESM server path*. ■ On Linux: /<oracle_home>/ArgusSafety/in ■ On Windows: Z:\Aecm-Argus-Int\in Argus Safety Case Directory Path is __________
Acknowledgement Directory Path	This is the path to the directory on the SOA server that is mapped or mounted to the directory on the Argus ESM server where the acknowledgement files will be written by Argus. *Note that the path provided in this field must be soa_server path and not the Argus ESM server path* ■ On Linux: /<oracle_home>/ArgusSafety/out ■ On Windows: Z:\Aecm-Argus-Int\out Argus Safety Acknowledgement Directory Path is ____

Table 3 (Cont.) Argus Safety Server Details Screen Fields

Field	Description
DTD Directory Path	This is the full path to the directory on the Argus ESM Server where the DTD files are kept. It must include the dtd file name. Example: C:\Program Files\Oracle\Argus\ESMService\DTDFiles\ich-icsr-v2.1-FDA-PIP.dtd Argus Safety DTD Directory Path is __________
Argus Database ID	This value is the SID of the Argus Safety database. To find this value, contact your Argus Database Administrator. Example: AS60X Argus Safety Database ID is ______________

6.4 Session Pool Manager Screen

This PIP uses the Session Pool Manager utility to interact with Siebel Web services. If the AIA server must invoke Siebel Web services through a proxy server, please fill in the values in this screen. If no proxy server is involved, these values can be left blank.

Use this screen to enter details related to your Session Pool Manager.

The screen contains the following fields:

Table 4 Session Pool Manager Screen Fields

Field	Description
Proxy Host URL	Specify the proxy host location. Example: `www-proxy.your.company.com` Proxy Host URL is _________________________
Proxy Port	Specify the proxy port. Example: `80` Proxy Port is _____________________________

For information about Session Pool Manager, see *Oracle Application Integration Architecture Process Integration Pack Utilities Guide*, "Session Pool Manager".

7 Installing the Device and Drug Adverse Event: Siebel AECM and Argus Safety

This section discusses the PIP installation process. The installation process has three steps:

1. Install the PIP.
2. Configure your PIP using the configuration wizard.
3. Deploy the PIP to the SOA Server.

Note: For information about how to install the Oracle AIA Foundation Pack, see the *Oracle Fusion Middleware Installation and Upgrade Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.5)*. This guide is available on the Oracle Technology Network (OTN) at http://www.oracle.com/technetwork/middleware/foundation-pack/documentation/index.html

7.1 Install the Device and Drug Adverse Event: Siebel AECM and Argus Safety

When you use the Installer the following takes place.

- You see a welcome screen that lists prerequisites and information about how to begin the installation process.
- The following prerequisite system checks are performed:
  - Operating system certification
  - Recommended operating system packages
  - Kernal parameters
  - Recommended gilbc version
  - Physical memory
- You are prompted to enter the installation location.
- You see an installation summary, which includes directory details, disk space required and available, and a list of the applications that are installed.
- You can choose to save the Response file, which stores the values that you have input and are displayed on the installation summary page.

To install the Device and Drug Adverse Event: Siebel AECM and Argus Safety

1. Download Oracle Device and Drug Adverse Event Data Integration Pack for Siebel Adverse Event Complaint Management and Argus Safety 11.1 from edelivery.
2. Unzip aia-aecm_argus-pip.zip.
3. Navigate to the Disk1 directory: **aecm_argus-pip/Disk1**.
4. Follow the launch instructions for your platform. The following table lists the commands that you must use based on your platform.

Table 5 Launching the PIP Installer

Field	Description
Linux x86 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 2008 (32 bit or 64 bit)	Double-click **setup.exe**.

Installer launches **Welcome** screen.

5. Click **Next**.
6. Wait for the prerequisite checks to complete and then click **Next**.
7. Select AIA Home where Foundation Pack is installed.
8. Click **Next**.
9. 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 Response file instead of using the wizard.

   This is an example of the command. Observe the `-silent` and `-response` arguments.

   ```
   ./runInstaller -invPtrLoc /slot/ems4965/oracle/<SOA_Home>/oraInst.loc -jreLoc
   /slot/ems4965/oracle/Middleware/jdk160_24/jre -silent -response
   /slot/ems4965/oracle/11.1_Installer_response.xml
   ```

10. Click **Install**.

    The warning message: *This installation will overwrite your AIAHOME with new content. Should your AIAHOME have customizations that you wish to preserve, please make a backup before you proceed. Are you sure you are ready to continue with the current installation?* is displayed.

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

    OR

    Click **No** to go back to the previous screen. Refer to the section Section 5.2, "How to Create Backups of your Customizations" for backing up the AIAHOME and preserving customizations.

11. Click **Next**.
12. To exit the installer, click **Finish**. The installation is complete.
13. Exit installer once installation is complete. Verify that the PIPManifest.xml file exists under <AIA_HOME>/pips/DeviceDrugAESEBLandArgus/config. Also review the install log files located in <AIA_HOME>/cfgtoollogs/oui directory.

7.2 Configure the Device and Drug Adverse Event: Siebel AECM and Argus Safety

The screens that appear prompt you to enter the data that is required for successful configuration of the Device and Drug Adverse Event: Siebel AECM and Argus Safety. Keep the completed worksheets of the Device and Drug Adverse Event: Siebel AECM and Argus Safety screens ready before you launch the configuration wizard.

To configure the Device and Drug Adverse Event: Siebel AECM and Argus Safety

1. Navigate to <AIA_Instance>/bin and run the following command as per your platform to configure the installation environment:
   - for Linux based systems: `source aiaenv.sh`
   - for Microsoft Windows: `aiaenv.bat`

2. Navigate to <AIA_HOME>/bin and run the following command as per your platform:

   - for Linux based systems: `./aiaconfig.sh`
   - for Microsoft Windows: `aiaconfig.bat`

   This launches the AIA Configuration Wizard.
3. Click **Next**.
4. Select **Core Process Integration Packs** in the navigation tree.
5. Select the **Device and Drug Adverse Event: AECM and Argus Safety** check box.
6. Click **Next**.

7.2.1 Specify PIP Server Details

To specify PIP Server details:

1. Enter information related to your PIP server in the **PIP Server Details** screen.
2. Click **Next**.

7.2.2 Specify Argus Safety Server Details

To specify Argus Safety Server details:

1. Enter information about your Argus Safety Server instance in the Argus Safety Server Details screen.

   Refer to the field description table for entering the values in Argus Safety Server Details screen.
2. Click **Next**.

7.2.3 Specify Siebel Life Sciences Server Details

To specify Siebel AECM details:

1. Enter information about your Siebel AECM Server in the Siebel Life Sciences Server Details screen.
2. Click **Next**.

7.2.4 Specify Session Pool Manager Details

To specify Session Pool Manager details:

1. Enter information related to your Session Pool Manager installation in the **Session Pool Manager Details** screen.
2. Click **Next**.

7.2.5 Complete Configuration

To complete configuration:

1. Review the configuration information on the **Configuration Summary** screen.

Note: 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 **Configuration Progress** screen.

3. Click **Next**.
4. When the configuration process completes without errors, the AIA Configuration Wizard displays the **Configuration Complete** screen.
5. Click **Finish** to close the configuration wizard.
6. 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 Pre-Deployment Security Configuration for Device and Drug Adverse Event: Siebel AECM and Argus Safety

The PIP 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 enable this encryption, follow these steps:

1. Follow the instructions in the *Oracle® Database Advanced Security Administrator's Guide 11g Release 2 (11.2)* for creating a wallet that is used by the TDE encryption.
2. Open sqlnet.ora at $ORACLE_HOME/network/admin.

   For example, /slot/ems2057/oracle/db11g/product/11.2.0/dbhome_1/network/admin.

   Make sure 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=/slot/ems2057/oracle/db11g/admin/phrmdev2/wallet/)))

3. Save sqlnet.ora file.
4. Navigate to the folder <AIA_HOME>/data/DrugDeviceAESEBLandArgus/sql/.
5. Open CreateSecureTableSpace.sql in an editor.

6. Modify CreateSecureTableSpace.sql file to indicate the location where you want your tablespace data to be stored and change any of the creation parameters to suit your environment.

7. Save CreateSecureTableSpace.sql.

8. Connect to the database as a user with SYSDBA role using SQL*Plus.

   For example, `sqlplus <username>/<password> as sysdba@<hostname>`

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

9. Execute CreateSecureTableSpace.sql.

   For example, `SQL>@CreateSecureTableSpace.sql`

   The SQL script prompts for the wallet password. A secure tablespace is created upon successful execution of the script.

10. Exit SQL*Plus.

11. Navigate to the following directory on the SOA_server:

    <AIA_HOME>/data/DrugDeviceAESEBLandArgus/sql

12. Connect to the database as a user with <AIA_INSTANCE>_JMSUSER role using SQL*Plus.

    For example, `sqlplus AIA11115_JMSUSER/<password>@<db sid>`

    > **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.

13. Execute CreateSecureTable.sql.

    For example, `SQL>@CreateSecureTable.sql`

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

14. Exit SQL*Plus.

7.4 Deploying the Device and Drug Adverse Event: Siebel AECM and Argus Safety

You need to deploy the PIP components on the SOA server as part of post install configurations.

To deploy the PIP to SOA Server, run the command specific to your platform:

1. Navigate to <AIA_HOME>/aia_instances/<AIA_instance_name>/bin and run the following command:

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

2. Run the command for your platform.

Table 6 Deployment commands for the Device and Drug Adverse Event: Siebel AECM and Argus Safety

Platform	Deployment Command
Linux	`ant -f <AIA_HOME>/Infrastructure/Install/AID/AIAInstallDriver.xml -DPropertiesFile=<AIA_HOME>/aia_instances/<AIA_Instance_name>/config/AIAInstallProperties.xml -DDeploymentPlan=<AIA_HOME>/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusDP.xml -DSupplementaryDeploymentPlan=<AIA_HOME>/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusSupplementaryDP.xml -l <AIA_HOME>/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusDP.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/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusDP.xml -DSupplementaryDeploymentPlan=<AIA_HOME>/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusSupplementaryDP.xml -l <AIA_HOME>/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusDP.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, refer to *Oracle® Fusion Middleware Developer's Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.45.0), "Generating Deployment Plans and Deploying Artifacts"*.

8 Performing Post-Installation Configurations

This section discusses post-installation configurations for the Device and Drug Adverse Event: Siebel AECM and Argus Safety. The section includes:

- Section 8.1, "Create a User in Oracle WebLogic Server"
- Section 8.2, "Setting Up Argus E2B Profile"
- Section 8.3, "Configuring Argus for Using Extension Profile"
- Section 8.4, "Configuring Folders for XML File Sharing"

- Section 8.5, "Configuring Session Pool Manager"

8.1 Create a User in Oracle WebLogic Server

As part of this integration, Siebel AECM writes messages to a JMS queue on the SOA server. Ensure that the user you choose for connecting Siebel to the SOA server exists in the Oracle WebLogic server. sadmin user, the default admin user of Siebel, is given here as an example.

To create a User:

1. Navigate to WebLogic console.
2. Under Domain Structure of **soa_domain,** select **Security Realms**, then select **myrealm**.
3. Select **Users and Groups** tab, then select **Users** tab.
4. Click **New**.
5. In the **Name** field, enter `sadmin` as the provider name.
6. In the **Password** field, enter password as given during configuration of corresponding Siebel Workflow.
7. In the **Provider** list, select the default authentication provider for the user.
8. Click **OK**.

8.2 Setting Up Argus E2B Profile

Argus ESM Server is used for this integration. Make sure that the following setup is completed on the Argus ESM Server:

To set up Argus E2B Profile:

1. Navigate to the SOA_Server directory <AIA_HOME>/AIAMetaData/AIAComponents/ApplicationObjectLibrary/ArgusSafety/V1/schemas and copy the file **ich-icsr-v2.1-FDA-PIP.dtd** to the Interchange server folder <Oracle_Home>\Argus\ESMService\DTDFiles\.
2. Copy all the files from the SOA_Server directory <AIA_HOME>/data/DrugDeviceAESEBLandArgus/sql to a folder on Argus ESM server. (For example, C:\Temp_config_folder)
3. Open a command prompt and navigate to the folder where you copied the scripts in step 2. Run the batch file **Setup_AECM_Profile.bat**.
4. Enter the log file path (For example: C:\Temp_config_folder\profilecreationoutput.log) and database name, ESM owner's username (For example: esm_owner), and password.
5. Press **Enter**.
6. After running the script, check the log file for errors.

8.3 Configuring Argus for Using Extension Profile

Perform the following steps to configure Argus Safety for using the extension profile for the selected agency. Note that only the user interface fields that are required for the integration to work are described here. All other fields that are not required for the integration can have either default or empty values. For more information, refer to *Oracle® Argus Interchange User's Guide, Version 6.0*

To configure Argus E2B Extension for the selected agency:

1. Log on to the Argus Console and select **Code List** on the top menu bar.
2. Navigate to the **Reporting Destination** folder from the **Browser**.
3. Click **Add New** button to create new agency details to serve as a reporting destination.
4. Enter the agency information in the **Agency Information** pane. Refer to the field description and example values given in the table:

Table 7 Agency Information Tab Field Description

Fields	Description
Agency Name	Agency name is the unique name of the destination that is configured to receive the E2B files. Enter the agency name as: **AECM-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. Note that 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.

5. Click the **Local Company Contact** tab and enter the contact details. Refer to the field description and example values given in the table:

Table 8 Local Company Contact Tab Field Description

Fields	Description
Company Name	Enter the company name. This is a mandatory field. Example: INTEGRATIONS

6. Click the **EDI** (Electronic Data Interchange) tab and enter the values in the fields. Refer to the field description and example values given in the table:

Table 9 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	This value must match the sender Identifier in the E2B file. The sender ID is the system ID of Siebel AECM defined in the AIA system registry. By default, this value is **SEBLCLIN_01**.
Message Profile	Select the ICH-ICSRV2.1MESSAGE_TEMPLATE – FDA PIP extension profile from the Message Profile list.

Table 9 (Cont.) EDI Tab Field Description

Fields	Description
ACK Profile	Select the ICH-ICSRV1.1ACKNOWLEDGMENT TEMPLATE - FDA acknowledgment profile from the ACK Profile list.
Company Identifier	Enter **ARGUS_01** as a company identifier. This value must match receiver identifier in the E2B file.
File Name	Enter the E2B file name format as **Safety_####.xml**.
Method	Select **E2B - XML Transmission** from the list to indicate that XML format is used for E2B transmission.
URL of Message DTD	Enter the extension DTD file path in the URL of Message DTD field: <ORACLE_HOME>\Argus\ESMService\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: <ORACLE_HOME>\Argus\ESMService\DTDFiles\FDA-icsrack-v1.1.dtd

7. Click **Save**.
8. Click **OK**.

8.4 Configuring Folders for XML File Sharing

For the exchange of E2B and Acknowledgement files between Argus Safety and SOA Server, you must create the folders and configure them. Refer to Prerequisites on page 5 for folders' details.

To configure the folders:

1. On Argus ESM Server, open ESM Mapping Utility. To open the ESM Mapping Utility, Click **Start** then select **All Programs** and select **Oracle** and then select **ESM Mapping**.
2. Enter the username, password, and database name to run the mapping tool.
3. In the ESM Mapping Utility navigate to Administrator and select **Setup INI File**.
4. 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.
>
> Refer to the field description table for entering the values in the **Service DB Setup** screen.

5. Select the database name (For Example, AS602R). This opens the **Service DB Setup** screen.
6. In the **System Directories** pane select the **Agency Name** from the list.

Table 10 Field Description of Service DB Setup Screen

Field	Description
Database Section	
Database Name	Enter database name. Example: AS60X
Unique Database ID	Enter unique database ID. Example: 123
User ID	Enter Database user name.
Password	Enter Database password.
Process	Enter the path to ESM process. Example: C:\Program Files\Oracle\Argus\ESMService\EsmProc.exe
Receive Process	Enter the path to Receive process. Enter C:\Program Files\Oracle\Argus\ESMService\E2BReceive.exe
Archive Folder	Select the folder for archiving the files. You had created this folder as one of the Prerequisites listed on page 5. Example: C:\<FOLDER>\Archive
Receive Processes	Enter **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 Agency Name **AECM-ARGUS-INTEGRATION** that you configured in the Argus Console, Reporting Destination.

Table 10 (Cont.) Field Description of Service DB Setup Screen

Field	Description
Local Company	This value is displayed based on Reporting Destination Configuration.
XML Incoming Folder	Specify folder path for incoming files. You had created this folder as one of the Prerequisites listed on page 5. Example: C:\ AECM-Argus-Int \In
XML Outgoing Folder	Specify folder path for outgoing files. You had created this folder as one of the Prerequisites listed on page 5. Example: C:\ AECM-Argus-Int \Out

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

8.5 Configuring Session Pool Manager

This PIP uses the Session Pool Manger utility. Configure Session Pool Manager after you install the PIP. For information on how to configure Session Pool Manager for your integration environment and needs, refer to *Oracle Application Integration Architecture Process Integration Pack Utilities Guide*, "Session Pool Manager".

9 Verifying Installation

To verify the Device and Drug Adverse Event: Siebel AECM 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 PIP is successfully installed.
   - For Microsoft Windows: Review the install log located at <AIA_HOME>\aia_instances\<AIA_Instance_name>\logs to verify that the PIP is successfully installed.
2. Confirm that the Device and Drug Adverse Event: Siebel AECM and Argus Safety 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.
   - AIASessionPoolManager
   - HealthSciencesDrugSafetyReportEBS
   - HealthSciencesDrugSafetyReportResponseEBS
   - ReportDrugSafetyReportSEBLReqABCSImpl

- ReportDrugSafetyReportResponseSEBLProvABCSImpl
- ReportDrugSafetyReportArgusProvABCSImpl
- ReportDrugSafetyReportResponseArgusReqABCSImpl
- ReportDrugSafetyReportWriteE2BFileAdapter
- ReportDrugSafetyReportReadAckFileAdapter
- SEBLCLINDrugSafetyReportJMSConsumer

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 username 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.

Tables containing JMS messages are persisted in an encrypted tablespace. Tablespace encryption process encrypts an entire tablespace. All objects created in the encrypted tablespace are automatically encrypted. Tablespace encryption is useful in securing sensitive data in tables.

For this integration pack, the services that invoke session pool manager do not work with SAML token authentication. Local client policy name is oracle/No_Authentication_Client_policy.

Verification of no_client_authentication Policy

1. Navigate to the **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** > **ReportDrugSafetyReportResponseSEBLProvABCSImpl**
4. On the right hand side, select **Policies**.
5. Verify the two no_authentication_client_policy attached to the two Siebel Inbound Web services.

For more information about security validation, see *Oracle® Fusion Middleware Developer's Guide for Oracle Application Integration Architecture Foundation Pack 11g Release 1 (11.1.1.4.0)*, "Working with Security."

For PIP implementation, see *Oracle Device and Drug Adverse Event Data Integration Pack for Siebel Adverse Events and Complaints Management and Oracle Argus Safety for Application Integration Architecture (AIA) Service Pack 11.1 Implementation Guide*.

10 Undeploying the Device and Drug Adverse Event: Siebel AECM and Argus Safety

To undeploy the PIP from SOA Server:

1. Navigate to <AIA_HOME>/aia_instances/<AIA Instance name>/bin and run the command `source aiaenv.sh` for Linux based systems and `aiaenv.bat` for Microsoft Windows to configure the installation environment.
2. Run the command for your platform.

Table 11 Undeployment command for the Device and Drug Adverse Event: Siebel AECM and Argus Safety

Platform	Undeployment Command
Linux Solaris SPARC IBM AIX Based Systems.	`ant -f $AIA_HOME/Infrastructure/Install/AID/AIAInstallDriver.xml -DPropertiesFile=$AIA_HOME/aia_instances/<AIA_Instance_name>/config/AIAInstallProperties.xml -DDeploymentPlan=$AIA_HOME/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusUndeployDP.xml -l $AIA_HOME/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusUnDeployDP.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/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusUndeployDP.xml -l $AIA_HOME/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusUnDeployDP.log`

3. To verify the undeployment of the integration, navigate to the log file path: $AIA_HOME/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusUndeployDP.log to check whether the PIP is sucessfully undeployed. The log file contains the 'Build Success' message, if the undeployment is successful. If the undeployment is not successful, then the log file contains the 'Build Failed' message.
4. Session Pool Manager does not get undeployed when you undeploy the PIP as it belongs to common components. To undeploy Session Pool Manager, run the command specific to your platform.

Table 12 Undeployment command for Session Pool Manager

Platform	Undeployment Command
Linux Solaris SPARC IBM AIX Based Systems.	`ant Uninstall -f <AIA_HOME>/Infrastructure/Install/AID/AIAInstallDriver.xml -DPropertiesFile=<AIA_HOME>/aia_instances/<AIA_Instance_name>/config/AIAInstallProperties.xml -DDeploymentPlan=<AIA_HOME>/utilities/SessionPoolManager/V1/DeploymentPlans/SessionPoolManagerUndeployDP.xml`
Microsoft Windows	`ant Uninstall -f <AIA_HOME>\Infrastructure\Install\AID\AIAInstallDriver.xml -DPropertiesFile=<AIA_HOME>\aia_instances\<AIA_Instance_name>\config\AIAInstallProperties.xml -DDeploymentPlan=<AIA_HOME>\utilities\SessionPoolManager\V1\DeploymentPlans\SessionPoolManagerUndeployDP.xml`

5. The Console shows the 'Build Success' message, if the undeployment is successful. If the undeployment is not successful, then the console displays the 'Build Failed' message along with the reason for the failure. AIASessionPoolManager service is removed after the undeployment command is run.
6. Restart the SOA server.

10.1 Verifying the Undeployment of the Integration

To verify the undeployment of the integration, navigate to the log file path: $AIA_HOME/pips/DrugDeviceAESEBLandArgus/DeploymentPlans/DrugDeviceAESEBLandArgusUndeployDP.log to check whether the PIP is sucessfully undeployed. The log file contains the undeployment success message and in case of failure the reason for failure is provided.

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

- SEBLCLINDrugSafetyReportJMSConsumer
- ReportDrugSafetyReportSEBLReqABCSImpl
- HealthSciencesDrugSafetyReportEBS
- ReportDrugSafetyReportArgusProvABCSImpl
- ReportDrugSafetyReportWriteE2BFileAdapter
- ReportDrugSafetyReportReadAckFileAdapter
- HealthSciencesDrugSafetyReportResponseEBS
- ReportDrugSafetyReportResponseArgusReqABCSImpl
- ReportDrugSafetyReportResponseSEBLProvABCSImpl

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 Device and Drug Adverse Event: Siebel AECM 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 perform the uninstall of 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 type ./runInstaller -deinstall. On the **Deinstall AIA Home** screen, make sure the AIA_Home shown is correct and select **DEINSTALL**.
4. Exit the Uninstaller.

11.2 Uninstalling the Device and Drug Adverse Event: Siebel AECM 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, refer to Section 10, "Undeploying the Device and Drug Adverse Event: Siebel AECM and Argus Safety" of this guide. 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:

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.

    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.

12 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.

Oracle Device and Drug Adverse Event Data Integration Pack for Siebel AECM and Oracle Argus Safety Installation Guide, Release 11.1
E26804-02