Oracle Life Sciences Argus Safety and Oracle Life Sciences Argus Insight

Installation Guide

Release 2026.1.01
G49216-01
March 2026

ORACLE

Oracle Life Sciences Argus Safety and Oracle Life Sciences Argus Insight Installation Guide, Release 2026.1.01

G49216-01

Contents

Part II Set Up Argus Middle and Client Tiers

3 Install and Configure Oracle Argus Safety Web

4 Install Oracle Argus Insight

5 Configure Web Service Interfaces on Web Server

Part III Install or Upgrade Oracle Argus Safety Database Tier

13 Install Oracle Argus Safety Database

Part IV Configure Other Products

17 Configure and Enable Oracle Argus Dossier

18 Install and Configure Axway B2Bi

19 Install and Configure Oracle B2B

20 Configure Oracle Analytics Server or Oracle Analytics Publisher

21 Configure the Oracle Analytics Publisher Environment for Oracle Argus Insight

22 Configure the Oracle Analytics Server Environment for Oracle Argus Insight

23 Configure Argus Centralized Coding

24 Extract, Transform, and Load Data

Part V Secure Oracle Argus Safety

25 Oracle Argus Safety Password Management—Cryptography Tool

A Create ODBC Connection for OAS Administration Tool for Oracle Argus Insight

Preface

This preface contains the following section:

- Related resources

Related resources

For information about Oracle Argus patches, see My Oracle Support.

All documentation and other supporting materials are available on the Oracle Help Center.

Part I

Prepare to Install Oracle Argus Safety

Oracle Argus Safety and Oracle Argus Insight are configurable systems and, based on user needs, you (administrators) may install all or some of the components.

We recommend that you follow the steps in the order presented.

Oracle Argus Insight also supports Oracle Argus Mart as an additional data source. If you are using Oracle Argus Mart as a data source in a multi-tenant environment, then you may create Oracle Argus Mart Advanced Condition that queries Oracle Argus Mart database.

In this section:

1

System Requirements

In this chapter:

Hardware Requirements

> **Note**
>
> The server hardware configurations in this table are for general informational purposes only. They represent typical, high-level guidance based on customer size—not a definitive sizing recommendation.
>
> Actual hardware needs will vary based on each customer's environment and requirements, including (but not limited to): workload characteristics, data volumes, user concurrency, integrations, customizations, availability and disaster recovery objectives, and operational practices.
>
> Customers are responsible for their own sizing and capacity planning, which should include performance and load testing using realistic, representative user volumes and business scenarios to validate the appropriate configuration.
>
> All values shown are estimates only and do not constitute a commitment, guarantee, or warranty of performance, capacity, or outcomes.

- **Database Server**

Hardware Requirements	Small	Mid-Sized	Large
RAM	32 GB	64GB	>=64 GB
CPU or Processor	Equivalent to 4 - 8 Dual Core x 3GHz	Equivalent to 4 - 8 Dual Core x 3GHz	Equivalent to 16 Dual Core x 3GHz
Fail Support System (physical standby option)	Dataguard	Dataguard	Dataguard
Virtualization	Optional	Optional	Optional
Oracle RAC 19c (19.19+)	Optional	Optional	Optional

- **Web Server, Transaction Server, and Interchange Server**

Hardware Requirements	Small	Mid-Sized	Large
RAM	24 GB	32 GB	64 GB
CPU or Processor	Equivalent to 8 Core x 3GHz	Equivalent to 8 Core CPUs x 3 GHz	Equivalent to 16 Core CPUs x 3 GHz
Virtualization	Physical Server or Oracle Virtual Machine (OVM 3.2.10, 64-bit)	Physical Server or Oracle Virtual Machine (OVM 3.2.10, 64-bit)	Physical Server or Oracle Virtual Machine (OVM 3.2.10, 64-bit)
Minimum Resolution	1280 x 1024	1280 x 1024	1280 x 1024

- **Web Client**
  - RAM: 8 GB
  - 3 GHz Dual Core CPU
  - Minimum Resolution: 1280 x 1024

Software Requirements

For more information, see the following:

- Operating System
- Oracle Components
- Other Components
- Generic—Other Supported Features
- Install Language Packs to Generate Reports
- General Installation Notes and Information

Operating System

Operating System	Oracle Database Server	Web Server	Transaction Server	Oracle Argus Interchange Server	Web Client
—	Operating System as certified for Oracle 19c (19.19+)	—	—	—	—
Microsoft Windows 2025 (64-bit)	—	Yes	Yes	Yes	—
Microsoft Windows 2022 (64-bit)	—	Yes	Yes	Yes	—
Microsoft Windows 2019 (64-bit)	—	Yes	Yes	Yes	—
Microsoft Windows 11 (64-bit) (English/ Japanese)	—	—	—	—	Yes

Oracle Components

> **Note**
>
> Make sure that you install the same version of Oracle Database Server and Client.
>
> If you are using Oracle Argus Enterprise Edition, you must install Enterprise Edition of the Oracle Database Server.

Oracle Components	Oracle Database Server	Web Server	Transaction Server	Oracle Argus Interchange Server	Web Client
Oracle Database Server version 19c (19.19+) (Enterprise/Standard Edition 2 over CDB/PDB or non-CDB format)	Yes	—	—	—	—
Oracle Client version 19c (19.19+) (64-bit only) (See Install and Apply Oracle Patch Set)	—	Yes	Yes	Yes	—
MTS	—	Yes	Yes	Yes	—
ODP.NET	—	Yes	Yes	Yes	—
Java JRE 1.8 or above	—	Yes (Required for Liquibase and WebGate only)	—	—	—
Oracle Advanced Security Network Encryption	Optional	—	—	—	—
Oracle XML Developer's Kit (XDK)	Optional (Required only for PMDA R3 Paper Reports)	—	—	—	—

Other Components

Other Components	Oracle Database Server	Web Server	Transaction Server	Oracle Argus Interchange Server	Web Client	Schema Creation Tool + Interchange Mapping Tool
Google Chrome (latest available version)	—	—	—	—	Yes	—

Other Components	Oracle Database Server	Web Server	Transaction Server	Oracle Argus Interchange Server	Web Client	Schema Creation Tool + Interchange Mapping Tool
Microsoft Edge (Chromium based, latest available version) (64-bit)	—	—	—	—	Yes	—
Microsoft Visual C++ 2015 - 2022 Redistributable (x64) - 14.38.33135 or above	—	Yes	Yes	Yes	—	Yes
Microsoft Access Database Engine 2016 Redistributable (x64) Or Microsoft 365 Access Runtime (x64)	—	—	—	—	—	—
Microsoft .NET 4.8 Framework	—	Yes	Yes	Yes	—	Yes
Microsoft Word + Excel (64-bit)	—	—	—	—	—	—
Adobe Acrobat Reader DC/XI with East Asian Fonts	—	—	—	—	Yes	—
Chinese, Korean, and Japanese supplemental fonts Required supplemental fonts: Dotum, FangSong, Meiryo, and Meiryo UI	—	Yes	Yes	Yes	—	Yes

Generic—Other Supported Features

If you are using...	You must install...
Argus generated reports for viewing	Any Word/Excel/PDF compatible viewer.

If you are using...	You must install...
Data encryption	Oracle Database TDE feature on the Database Server, which is a part of the Oracle Advanced Security option available for Oracle Database Enterprise Edition: 19c (19.18+). TDE provides the capability to encrypt sensitive data in the Oracle Database in a manner that is transparent to applications. Oracle Argus Safety product has been functionally certified with tablespace level encryption using the Oracle Database TDE feature.
MedDRA Recode	Microsoft Word + Excel (64-bit)
Multi-tenant environment	Single Sign-On
Single Sign-On	• Oracle Access Manager (OAM) version 12.2.1.4 OR Oracle Identity Management Suite (IDM) (Oracle Identity Governance 12.2.1.4 integrated with Oracle Accces Manager 12.2.1.4) • Compatible IIS WebGate version 12.2.1.4 (64-bit) on the Web Server.
Built-in Reports to run the PMDA E2B (R3) Paper Reports or Flexible Aggregate Reporting	• For Argus Enterprise Edition - Oracle Analytics Server 2024 or 2025 • For Argus Standard Edition, either one of the following: – Oracle Analytics Server 2024 or 2025 Or – Oracle Analytics Publisher 2024 or 2025 • Oracle Analytics Publisher Desktop tool on the client machine to customize the reports. See Configure Oracle Analytics Server or Oracle Analytics Publisher.
LDAP for authentication support	LDAP/LDAPS Protocol Version 3.0
E-mail capabilities within Oracle Argus Safety	Microsoft Modern Authentication. SMTP Protocol. The following Oracle Argus Safety components support SMTPS: • Oracle Argus Safety—Supports SMTPS and TLS 1.2 (Forced). Both Implicit and Explicit modes. • Axway 2.6 UP 2025-11—Supports SMTPS and TLS 1.2. Implicit mode only. • Oracle Analytics Server/Oracle Analytics Publisher—Supports SMTPS and TLS 1.2, and must have JDK 8u451+ for SMTPS. Both Implicit and Explicit modes. To send emails using the modern authentication, you must register Oracle Argus Safety in the Microsoft Azure portal. See the Microsoft Documentation for details on registering and configuring email on Azure portal. Note that B2B does not supports SMTPS.
Documentum for Storage	Documentum 22.1 on Web, Transaction, and Interchange Servers.
Faxing capabilities for Expedited Reports	RightFax 22.4 on Transaction Server.

If you are using...	You must install...
E2B Reporting for exchange	• Oracle B2B 12.2.1.4 + Latest patches—Certified with both AS1 and AS2 protocols for E2B exchanges between regulatory authorities and pharmaceutical companies. Apply patch 26795544 to support AES encryption. • Axway 2.6 UP 2025-11
Microsoft Windows 2019, 2022, or 2025	IIS 10

Tips

- Enable HTTP Compressions on your windows server.
- Enable SSL that is supported for your windows server.

Install Language Packs to Generate Reports

To generate reports, you must install Windows Supplemental Language Support for Chinese, Korean, and Japanese font packs on all the servers except the Oracle database server.

1. Make sure that you have sufficient free disk space before installing the language packs.
2. Select `Start > Settings > Time & Language > Language`.
3. Click **Add a language**.
4. Select Chinese (Simplified, China), and click **Next**.
5. Select the options, and click **Install**.

   The language pack is installed as a background process.
6. Repeat from Step 2 to Step 5 for all available Chinese language pack options, Korean, and Japanese language packs.
7. After the language packs are installed, restart the server.
8. Proceed with the Argus installation.

General Installation Notes and Information

- All the information about LDAP, Single Sign-On Header, and SMTP configuration will be synchronized in real-time and also by ETL.
- Ensure that you have configured the Oracle Argus Safety URL in the Oracle Argus Safety Load Balancer Server.
  To do so:
  1. Navigate to **Argus Console, System Management** (Common Profile Switches), and select **Network Settings**.
  2. In the Argus Safety Load Balancer Server text box, enter either the Oracle Argus Safety URL or the Oracle Argus Safety Load Balancer URL.

2

Install Oracle Database

Install Oracle Database on the Database Server.

In a multi-tenant environment, you must install the Oracle database with the Oracle Database Server Enterprise edition (and not the Standard edition).

In this chapter:

Get the Oracle Database Installation Guide

Open or download the installation guide for your operating system:

- For version 19c (19.19+)— `https://docs.oracle.com/en/database/oracle/oracle-database/19/install-and-upgrade.html`

Install Oracle Database

Follow the instructions in the *Oracle Database Installation Guide*, making selections appropriate for Oracle Argus Safety as noted in the following sections.

You can configure the database as part of the database software installation or after, using the Database Configuration Assistant (DBCA). Oracle Argus Safety supports installation on either a Container Database (CDB) containing a Pluggable Database (PDB) or a non-CDB database.

For an explanation of which options require an additional license, see the Oracle Database *Licensing Information User Manual* at `http://docs.oracle.com/database/`

For more information, see the following:

- Database Software Installation Options
- Database Configuration Options
- Install and Apply Oracle Patch Set

Database Software Installation Options

During installation of the database software (binaries, or server code), select the following:

- Advanced or Typical installation
- Time Zone
- Oracle Real Application Clusters (RAC) (Optional)

Database Configuration Options

Feature or Option	Mandatory	Recommended	Optional	Notes
Character Set: AL32UTF8	Yes	—	—	—
Oracle Text	Yes	—	—	Included automatically if you install the database during server installation.
Oracle JVM	Yes	—	—	Included automatically if you install the database during server installation.
Oracle XML DB	Yes	—	—	Included automatically if you use the Oracle Database Configuration Assistant to create the database. http://docs.oracle.com/database/121/ADXDB/appaman.htm#ADXDB2700
Oracle Automatic Storage Management	—	Yes	—	Provides an alternative to conventional volume managers, file systems, and raw devices.
Automatic Memory Management	—	Yes	—	Manages instance memory to allow the Oracle Database instance to automatically manage and tune it for you.
Oracle Advanced Security Transparent Data Encryption (TDE)	—	Yes	—	Available only for the Enterprise Edition.
Oracle Real Application Clusters (RAC)	—	—	Yes	—
Oracle Partitioning	—	—	Yes	Available only for the Enterprise Edition.

Install and Apply Oracle Patch Set

1. Download and install the latest patch set: WINDOWS DB BUNDLE PATCH through Oracle Support.

   To install Oracle Client, use the **Custom** option (NOT the Administrator option) and make sure that the **MTS component** is checked explicitly.
2. Set *oracle_home* to your client home location. For example:

   `SET ORACLE_HOME=<Oracle Client home path>`
3. Run `sqlldr help=y` or `sqlldr.exe`.
4. Apply the latest CPU patch.

Set Up Oracle Argus Safety Database Parameters

For more information, see the following:

Oracle Argus Safety Database Instance Parameters (Recommended)

We recommend that you evaluate each site before installation and on an ongoing basis to determine whether these settings are suitable for your business needs.

> **Note**
>
> Oracle Argus Safety database compatible parameter should be set as the <*current version*>.

#	Database Parameters	Small (under 30,000 cases reported per month)	Mid-Sized (30,000 to 200,000 cases reported per month)	Large (200,000 to 1,000,000 cases reported per month)	Very Large (over 1,000,000 cases reported per month)
1	MEMORY_TARGET	10 GB	16-24 GB	32-64 GB	>64 GB
2	PROCESSES	Expected concurrent users + 100	Expected concurrent users + 100	Expected concurrent users + 100	Expected concurrent users + 100
3	MEMORY_MAX_TARGET	>= value set for MEMORY_TARGET	>= value set for MEMORY_TARGET	>= value set for MEMORY_TARGET	>= value set for MEMORY_TARGET
4	OPTIMIZER_SECURE_VIEW_MERGING	FALSE	FALSE	FALSE	FALSE
5	CURSOR_SHARING (**Mandatory**)	EXACT	EXACT	EXACT	EXACT
6	WORKAREA_SIZE_POLICY	AUTO	AUTO	AUTO	AUTO
7	JOB_QUEUE_PROCESSES	25	25	25	25
8	DB_BLOCK_SIZE (bytes)	8192	8192	8192	8192
9	NLS_LENGTH_SYMANTICS (**Mandatory**)	CHAR	CHAR	CHAR	CHAR
10	GLOBAL_NAMES	TRUE	TRUE	TRUE	TRUE

Additional Database Setup Information

#	Setting	Small (under 30,000 cases reported per month)	Mid-Sized (30,000 to 200,000 cases reported per month)	Large (200,000 to 1,000,000 cases reported per month)	Very Large (over 1,000,000 cases reported per month)
1	Number and Size of Redo Log Files	5 Groups * 100 MB	5 Groups * 100 MB	5 Groups * 100 MB	5 Groups * 100 MB
2	TEMP Tablespace Size	8 GB	16 GB	32 GB	>=64 GB
3	Undo Tablespace Size	8 GB	16 GB	32 GB	>=64 GB

Oracle Argus Insight Configuration Requirements

For more information, see the following:

- Database Parameters
- Database I/O Configuration
- Recommended Configuration for the Database Server

Database Parameters

The table below lists the database parameters and the values that must be set for Oracle Argus Insight.

For those parameters that require a numeric value, the table below lists the minimum value recommended. You may need to increase the value depending on your system configuration and the number of cases. It is the responsibility of the database administrator to monitor the system and adjust the database parameters as necessary.

Table 2-1 Database Parameters for Oracle Argus Insight

Database Parameter	Required Value
`COMPATIBLE` (for Oracle Database 19c)	19c (19.19+)
`CURSOR_SHARING`	EXACT
`JOB_QUEUE_PROCESSES`	10 (Minimum value recommended)
`NLS_LENGTH_SEMANTICS`	CHAR
`OPTIMIZER_MODE`	ALL_ROWS
`OPTIMIZER_SECURE_VIEW_MERGING`	TRUE
`PARALLEL_MAX_SERVERS`	Minimum value recommended based on the total number of cases: • Small (< 30,000 cases): 16 • Medium (30,000 to 200,000 cases): 32 • Large (200,000 to 1,000,000 cases): Default • Extra Large (> 1,000,000 cases): Default

Table 2-1 (Cont.) Database Parameters for Oracle Argus Insight

Database Parameter	Required Value
PGA_AGGREGATE_TARGET	Minimum value recommended based on the total number of cases: • Small (< 30,000 cases): 0.5 GB • Medium (30,000 to 200,000 cases): 2 GB • Large (200,000 to 1,000,000 cases): 3 GB • Extra Large (> 1,000,000 cases): 4 GB
QUERY_REWRITE_ENABLED	TRUE (if computing statistics regularly) FALSE (if not computing statistics regularly)
SGA_MAX_SIZE	Greater than or equal to the value of the SGA_TARGET parameter.
SGA_TARGET	Minimum value recommended based on the total number of cases: • Small (< 30,000 cases): 1 GB • Medium (30,000 to 200,000 cases): 2.5 GB • Large (200,000 to 1,000,000 cases): 3.5 GB • Extra Large (> 1,000,000 cases): 4.5 GB The 32-bit architecture allows for 4 GB of physical memory to be addressed. DBAs should verify the maximum addressable RAM for their respective architectures.
UNDO_MANAGEMENT	AUTO
WORKAREA_SIZE_POLICY	AUTO
DB_BLOCK_BUFFERS (in MB) / DB_CACHE_SIZE	Leave set to the Oracle default value
DB_BLOCK_SIZE(in bytes)	Leave set to the Oracle default value
QUERY_REWRITE_INTEGRITY	Leave set to the Oracle default value
SHARED_POOL_SIZE	Leave set to the Oracle default value

Database I/O Configuration

Table 2-2 Recommended Database I/O Configuration for Oracle Argus Insight

Database I/O Configuration	Small (< 30,000 cases)	Medium (30,000 to 200,000 cases)	Large (200,000 to 1,000,000 cases)	Extra Large (> 1,000,000 cases)
Number and Size of Redo Log Files **Note:** The value depends on the characteristics of the I/O subsystem such as the I/O bandwidth, storage disks type, and RAID level. (Oracle recommends RAID 1+0 or similar.)	Default	3 X 500 MB	5 X 500 MB	5 X 500 MB
TEMP Tablespace Size	32 GB	32 GB	64 GB	128 GB

Table 2-2 (Cont.) Recommended Database I/O Configuration for Oracle Argus Insight

Database I/O Configuration	Small (< 30,000 cases)	Medium (30,000 to 200,000 cases)	Large (200,000 to 1,000,000 cases)	Extra Large (> 1,000,000 cases)
UNDO Tablespace Size **Note:** The recommended UNDO tablespace size is based on the projections with the following two parameter values: `RETENTION=NOGUARANTEE` and `UNDO_RETENTION=900 (seconds)`	16 GB	32 GB	64 GB	128 GB

Recommended Configuration for the Database Server

Table 2-3 Recommended Configuration for the Oracle Argus Insight Database Server

Database Server Configuration	Small (< 30,000 cases)	Medium (30,000 to 200,000 cases)	Large (200,000 to 1,000,000 cases)	Extra Large (> 1,000,000 cases)
RAM	4–8 GB	8–16 GB	16–32 GB	16–32 GB
CPU	Equivalent to 2–4 Dual Core, 3 GHz	Equivalent to 4–8 Dual Core, 3 GHz	Equivalent to 8–12 Dual Core, 3 GHz	Equivalent to 8–12 Dual Core, 3 GHz

> **Note**
>
> The Oracle Argus Insight Database and Oracle Argus Safety Database TNS names entry must be available in both Oracle Argus Insight Database Server and Oracle Argus Safety Database Server. Oracle Argus Safety Database TNS should also be present in the Oracle Argus Insight Web Server.

Part II
Set Up Argus Middle and Client Tiers

During the installation, the information in this manual may be different from what you see on your monitor if additional modules were selected during the Oracle Argus Safety Web installation.

Prerequisites:

- Obtain a domain account with Local Administrator privileges.
- In case of application upgrade, make sure to Backup Configuration Files of the existing Oracle Argus Safety application before setting up the machines.

Recommendation:

- Generate New Cryptography Key, and place the updated `ArgusSecureKey.ini` file under the `.\Windows` folder of the web server.
- You may need to reinstall the printer driver for site printers after setting up Oracle Argus Safety middle and client tiers.

If the current installed Oracle Argus Safety version does not support upgrade:

1. From your Windows folder, backup the **`ArgusSecureKey.ini`** file.
2. When the installation is complete, replace the exiting **`ArgusSecureKey.ini`** file with the backed up file in the Windows folder.
   Replace the file on all the Windows servers.

In this section:

3

Install and Configure Oracle Argus Safety Web

In this chapter:

Prerequisites

- Make sure that the regional settings are US settings.
- Install Internet Information Services (IIS).
- Install Language Packs to Generate Reports.
- Generate New Cryptography Key, and place the updated `ArgusSecureKey.ini` file under the `.\Windows` folder of the server.

> **Note**
>
> To set up ASP.NET correctly, you must install IIS before running Windows Updates.
>
> If Windows Updates are run before installing the IIS, Windows Updates will install Microsoft.Net without setting up the ASP.NET. In this scenario, refer to Microsoft Support on how to re-register ASP.NET in IIS.
>
> This is usually accomplished by running `aspnet_regiis.exe -i` from the `.NET v4.0.30319` folder.

Install Oracle Argus Safety Web

1. Log in as the Administrator on the system where Oracle Argus Safety is being installed.
2. Copy the installation package to the local directory of the target machine.
3. Open the Oracle Argus Safety folder and click **setup.exe**.
4. In the Argus Suite Solution Components Installation Wizard screen, click **Next**.
5. Enter the User Name and Company Name, and click **Next**.
6. In the Default Directory screen, to select the default installation directory where the Argus Suite Solution Components will be installed, click **Browse**.
7. To display the Argus Suite Components list, click **Next** and select the default installation directory.
8. Under the **Web Server**, select **Argus Safety Web**, and click **Next**.

   The Argus Suite Solution Components Report Directory appears.

> **Note**
>
> (Optional) You can now install Oracle Argus Insight while installing Oracle Argus Safety by selecting it from the list of modules.

9. Select the directory where temporary reports will be stored.

   You can browse through any path or leave this as default (`C:\Temp`).

10. (Optional) To configure minimum security on this server, enter the domain account login credentials, and click **Next**.

    The Setup Status screen appears with the installation progress.

> **Note**
>
> If the minimum security is not being setup, leave these fields blank, and click **Next**.

11. To configure a database, click **Yes** when prompted.
12. Enter a database name and click **Next**.

    This database name will appear on the Argus Login page.

13. Enter the database SID and click **Next**.
14. In the Setup Completed screen, click **Finish**.
15. Click **OK** to reboot the system.
16. Set up the Argus Cryptography key by following the instructions in the Oracle Argus Safety Application Servers.
17. After setting up the application servers, copy the **`ArgusSecureKey.ini`** file from the **`.\Windows`** folder of the system, where the database is created or upgraded, and replace the **`.\Windows`** folder of each installed application server.

Configure Load Balancer in Oracle Argus Safety Web

To set up a Load Balancer in Oracle Argus Safety, you need to setup:

- The Argus Web Load Balancer IP Address
- The Load Balanced Folders
- The Shared Network Directory

For more information, see the following:

- Set Up Oracle Argus Safety Web Load Balancer IP Address
- Set Up Shared Network Directory

Set Up Oracle Argus Safety Web Load Balancer IP Address

If Argus Web is being installed in a Load Balanced Environment, the Load Balancer IP Address must be configured in Oracle Argus Safety Console.

1. Log in to Oracle Argus Safety Console.

2. From System Configuration Menu, select **System Management**.
3. Click the **Network Settings Folder**.
4. Do the following, and click **Save**.
   - For non-SSL environment, enter the IP Address or Oracle Argus Safety URL.
   - For an SSL environment, enter the SSL URL.

Set Up Shared Network Directory

The network directory is a shared directory that will be the same for all load balanced Web Servers.

Update `argus.ini` for messagecachepath=<*shared directory for the message cache*>.

Reset IIS

To make the latest data or configurations available to the rest of the system, reset IIS when the changes have been made to the following areas:

1. Changes in configuration files:
   - `Argus.ini`
   - `Argus.xml`
2. Changes in following screens through Console:
   - Common Fields
   - System Management
   - Enabled Modules

4

Install Oracle Argus Insight

The Oracle Argus Insight web component is merged with Oracle Argus Safety web. You cannot install Oracle Argus Insight alone in any web server.

Proceed to:

- Change the APR_USER Password

Change the APR_USER Password

You need to update the password on the database level and the Oracle Argus Insight Web Server. The Oracle Argus Insight application uses this password to communicate with the database initially.

Before changing the password for the APR_USER on any Oracle Argus Insight Web Server:

- Stop the Oracle Argus Insight service.
- Stop IIS on the Oracle Argus Insight Web Server.
- Stop the IIS.
- Update the password of APR_USER on database level.
  You need to update the password at the database level before you can modify the password for the Oracle Argus Insight Web Server.

To modify the APR_USER password

Visit: Update APR_USER Password

5

Configure Web Service Interfaces on Web Server

In this chapter:

Oracle Argus Safety Web Service Interface

The Oracle Argus Safety Web Service Interface supports outbound Interfaces (MedDRA, WHO Drug and LOT Number) which provide the capability to integrate with customer-hosted web services and inbound web services (the Product-Study-License Interface) hosted on the Oracle Argus Safety Web Server.

All web service-based interfaces communicate with the standard SOAP 1.2 Protocol and use WS-Addressing and WS-Security. The Oracle Argus Safety web service interface leverages Windows Communication Foundation to generate WS-Addressing and WS-Security header information. We recommended testing this message before moving too far into business testing. For more information on these specifications, see the OASIS and W3C websites.

You can edit a standard .config file to select which integrations to enable, which transport protocol to use, and authentication details.

All errors are handled through a SOAP fault. Should an error occur, logical or otherwise, a SOAP fault should be thrown by the host and caught by the client. The client application (web) of Argus displays the details of the SOAP fault to the user when possible. Oracle Argus Safety web services throw SOAP faults when an error occurs.

The Oracle Argus Safety web service interface in this release supports the following integrations through Web Service:

Interface	Description
MedDRA (outbound)	MedDRA Drug web service interface provides a mechanism to integrate customer-hosted MedDRA coding systems with Oracle Argus Safety via web services.

Interface	Description
WHO Drug (outbound)	WHO Drug web service interface provides a mechanism to integrate customer-hosted WHO coding systems with Oracle Argus Safety via web services.
Lot Query (outbound)	Lot Number web service interface provides a mechanism to integrate customer-hosted central product information systems with Oracle Argus Safety via web services.
Product Study License(PSL) - (inbound)	PSL web service interface provides a mechanism to integrate customer central system to push or query PSL data via web services hosted on the Oracle Argus Safety Web Server.

In a multi-tenant Argus system:

- Endpoint configuration of central MedDRA and WHO Drug web service is at the global level. Enterprise if configured to use MedDRA and WHO Drug web service interface uses same endpoint to connect.
- Endpoint configuration of Lot Number Interface is defined at an enterprise level. Enterprise if configured to use Lot Interface uses enterprise specific endpoint configuration.
- Outbound Interface: Message payload must have an `'EnterpriseShortName'`.
- Inbound Interface: Message payload must have an `'EnterpriseShortName'`.

For more information, see the following:

- Oracle Argus Safety Web Service Interface Framework

Oracle Argus Safety Web Service Interface Framework

Each outbound/inbound web service request/response is enclosed in a SOAP envelope that begins with a SOAP header, followed by a Body statement that contains a unique node under the SAFETY_MESSAGE node. This node uniquely identifies the Interface being used for Inbound/Outbound communication. When implementing the customer side of the interface, follow the structure defined by Oracle in the XSD/WSDL files located in the following directory:

`<Argus Web Install Path>\Integrations\XSD`

`<Argus Web Install Path>\Integrations\WSDL`

For example, `C:\Progam Files\Oracle\ArgusWeb\ASP\Integrations\XSD`

Edit .config Files

.config fies are categorized as either Outbound or Inbound. For more information, see the following:

- Edit the .config file for Outbound Interfaces
- Edit the .config file for Inbound Interface

Edit the .config file for Outbound Interfaces

1. Navigate to the root of the **ArgusWeb** directory.
2. Open the `web.config` file in a text editor.

   By default, the bindings are provided for:

- basic HTTP traffic
- basic SSL communication

3. Update the **address** attribute of the endpoint nodes to point to the correct web service address.
4. To use encryption, set the **bindingConfiguration** attribute of the endpoint node as `WSHttpBinding_IRelsysService_Secure`.

   Additional binding configurations may also be created and used.

   Note that the binding configurations between the host and the client must be compatible for successful communication.
5. To transmit the authentication information, add credentials in the **ClientCredentials** section of each endpoint node.
6. To transform messages, use either a custom transformation assembly or an XSLT. Lot Number and WHO Drug coding interfaces leverages this feature.
   - Update the **TransformerConfiguration** section to map an endpoint to a transformer.
   - If multiple transformers are specified for a particular endpoint, they are executed in the order in which they appear in the configuration file.
   - The transformers configured by Oracle should not be modified, but additional transformers may be added if necessary.

Edit the .config file for Inbound Interface

All inbound integrations (file based) are handled by the Oracle Argus Safety Windows Service.

1. Navigate to the `.\ArgusWeb\ASP\Argus.NET\Bin` directory.
2. Open the `RelsysWindowsService.exe.config` file in a text editor.

   This configuration file provide reference configuration files of the configured integrations.
3. To enable an integration, in the **RelsysConfigurationFiles** section, uncomment the required **add** node (s).
4. To disable an integration, in the **RelsysConfigurationFiles** section, comment the required **add** node (s).
5. In the **DatabaseConfiguration** section, enter the database credentials.

Safety Message

The XML message required by each integration varies and is defined by its own schema. However, each schema follows a standard. The root node of every XML Safety Message in inbound and outbound interface is `SAFETY_MESSAGE` with the following node or attribute:

Node/Attribute Name	Description
Type	This is an enumeration (currently either "Request" or "Response") to identify the directionality of the message.
EnterpriseShortName	• In the Oracle Argus Safety multi-tenant environment, EnterpriseShortName is a part of message payload for all outbound and inbound interfaces. • In the Oracle Argus Safety single-tenant environment, EnterpriseShortName is not a part of message payload for the outbound interfaces and is not required for inbound interface.

Node/Attribute Name	Description
EXTENSION	Every Safety Message may also contain an EXTENSION node with CUSTOM sub nodes. These are for future expandability and currently unused.

MedDRA Interface

The MedDRA Encoding Web Service Interface integrates customer-hosted central MedDRA dictionary web service with Oracle Argus Safety. Oracle Argus Safety expects the data from the central MedDRA dictionary web service in a defined format as specified by the MedDRA dictionary schema.

In a multi-tenant setup, endpoint configuration of central the MedDRA web service is stored at global level and all the enterprises in Oracle Argus Safety uses the same web service endpoint. The **EnterpriseShortName** attribute present in the request message payload identifies which enterprise has initiated the web service request.

This interface supports both English and Japanese MedDRA dictionaries.

> **Note**
>
> To upload the dictionaries, refer to the *Oracle Argus Safety Administrator's Guide*.

For more information, see the following:

- MedDRA Configuration
- MedDRA Encoding Flow
- MedDRA Interface XML Schema

MedDRA Configuration

MedDRA Configuration is detailed in the following:

- Enable MedDRA Integration through Oracle Argus Safety Console
- Edit the ArgusWeb/ASP/web.config file
- Edit the Argus.NET/web.config file

Enable MedDRA Integration through Oracle Argus Safety Console

1. From Oracle Argus Safety Web, open Console and select **System Configuration** > **System Management**.
2. Expand the **Case Processing** tree branch, then and select **Dictionary Browser**.
3. To use web services, select the **Argus Safety MedDRA Coding Method** radio button.
4. If the web service hosting MedDRA is not available, fails, or does not return a valid match, check the **Use Local MedDRA if Term not found by Web Services** checkbox. (Optional)
5. To use local MedDRA J, check the **Use Local MedDRA for Japanese terms** checkbox.

Edit the ArgusWeb/ASP/web.config file

1. Navigate to ArgusWeb/ASP.
2. Open the `web.config` file in a text editor.
3. Search for `endpoint` and update the following attributes:
   - **address**—to point to the correct web service address
   - **name**—MedDRA
   - **bindingConfiguration**—to use encryption
     Note that the binding configurations between the host and the client must be compatible for successful communication.

The endpoint configuration might look something like this:

```
<endpoint address="http://remotewebservice/MedDRAAutoEncode.svc"
binding="wsHttpBinding" bindingConfiguration="WSHttpBinding_IRelsysService_
Unsecure" contract="IRelsysService" name="MedDRA">
```

Edit the Argus.NET/web.config file

1. Navigate to ArgusWeb/ASP/Argus.NET.
2. Open the `web.config` file in a text editor.
3. Search for `endpoint` and update the following attributes:
   - **address**—to point to the correct web service address
   - **name**—MedDRA
   - **key**—version of MedDRA XML being used
     For example,
     - `<add key="MedDRAXMLVersion" value="2.0"/>`, or
     - `<add key="MedDRAXMLVersion" value="1.1"/>`, or
     - `<add key="MedDRAXMLVersion" value="1.0"/>`
   - **bindingConfiguration**—to use encryption
     Note that the binding configurations between the host and the client must be compatible for successful communication.
   - **paths**—to add path for both the Request and Response XSDs based on the version being used
     For example,
     - `<add InputXSD="..\..\Integrations\XSD\v2.0\MedDRA_Response.xsd" />`
     - `<add InputXSD="..\..\Integrations\XSD\v2.0\MedDRA_Request.xsd" />`

MedDRA Encoding Flow

When Oracle Argus Safety makes a call to the web service, it populates the REPORTED and CODED nodes with data entered by the user. The REPORTED term is essentially a verbatim term while the coded term is the term that is expected to be coded by the remote system. The returned message contains a PATHS node with PATH sub-nodes that have been encoded by

the remote system. Oracle Argus Safety displays the returned LLTs in the MedDRA browser from which you can select the correct LLT. Note that the MedDRA Browser does not open on the Case Bookin screen.

If autoencoding is enabled and finds an exact match, Oracle Argus Safety places the encoded LLT term in the case form. If autoencoding finds multiple matches, the system uses the primary path. If autoencoding is not enabled or does not find any matches, or the web service is unavailable, Oracle Argus Safety loads the MedDRA browser with local dictionary information, if the system is configured to allow this.

MedDRA Interface XML Schema

Schema files for request and response are located in the `<Argus Web Install Path>\Integrations\XSD` directory.

Verify the MedDRA Interface request and response functions for the following schema files:

- MEDDRA_Request
- MEDDRA_Response

MEDDRA_Request

Oracle Argus Safety makes a web service request to the externally hosted central product information system as defined in this schema.

- Schema File
  Version 1.0

  Top level file: `\v1.0\MedDRA_Request.xsd`

  Sublevel file: `\v1.0\Base.xsd`

  Version 1.1

  Top level file: `\v1.1\MedDRA_Request.xsd`

  Sublevel file: `\v1.0\Base.xsd`

  Version 2.0

  Top level file: `\v2.0\MedDRA_Request.xsd`

  Sublevel file: `\v1.0\Base.xsd`
- Namespace
  `http://www.oracle.com/Argus/MedDRA_Request/v1.0`

  `http://www.oracle.com/Argus/MedDRA_Request/v1.1`

  `http://www.oracle.com/Argus/MedDRA_Request/v2.0`
- Node/Attribute Name Description
  The MEDICAL_DICTIONARY node is the first child node identifying MedDRA integration.

MEDDRA_Response

Oracle Argus Safety expects the central MedDRA dictionary to send the response in this format.

- Schema File
  Version 1.0

Top level file: `\v1.0\MedDRA_Response.xsd`

Sublevel file: `\v1.0\Base.xsd`

Version 1.1

Top level file: `\v1.1\MedDRA_Response.xsd`

Version 2.0

Top level file: `\v2.0\MedDRA_Response.xsd`

- Namespace
  `http://www.oracle.com/Argus/MedDRA_Response/v1.0`

  `http://www.oracle.com/Argus/MedDRA_Response/v1.1`

  `http://www.oracle.com/Argus/MedDRA_Response/v2.0`
- Node/Attribute Name Description

Node/Attribute Name	Description
Action	Must have the value **Auto**. This attribute must be present in the request when a full hierarchy is required to be passed back to auto encode the term without using the MedDRA Browser. With an "Auto" message, the system requires that an LLT Term be passed in the request. If the full hierarchy is not found or returned, the system will open the MedDRA Browser and display the LLTs returned for manual encoding by the user using the local MedDRA instance. If multiple paths are returned, the Primary SOC path is used.
Source	An enumerated value that specifies additional information that may be required for coding based on origination as follows: • Reaction Case Form | Patient Tab | Patient Tab | Other Relevant History | ReactionCase Form | Patient Tab | Parent Tab | Other Relevant History | Reaction • Indication Case Form | Patient Tab | Patient Tab | Other Relevant History | IndicationCase Form | Patient Tab | Parent Tab | Other Relevant History | Indication • Condition should be verbatim Case Form | Patient Tab | Patient Tab | Other Relevant History | VerbatimCase Form | Patient Tab | Parent Tab | Other Relevant History | Verbatim • Lab Console | Code Lists | Lab Test Type • Description Case Form | Events Tab | Event Tab | Description to be CodedCase Form | Events Tab | Death Information | Cause of Death and Autopsy Results | Description as Reported • Diagnosis Argus Case Form | Analysis Tab | Analysis Tab| Company Diagnosis Syndrome
Term (v 1.0)	The TERM node specifies the information about a specific term that is either being looked up or populated with data and supports Reported and Coded nodes.
Term (v 1.1/2.0)	The TERM node specifies the information about a specific term that is either being looked up or populated with data and supports Reported, Coded, and Lang nodes.
Primary	The Primary attribute is Y if the term is the Primary SOC path for the selected term. In the event that multiple terms are returned for a MedDRA level, this attribute is only be available on the primary term.
PATHS/PATH (version 1.0)	The PATHS node has a PATH subnode for each MedDRA hierarchy returned. MedDRA hierarchy with English terms only.

Node/Attribute Name	Description
PATHS/PATH (version 1.1)	Contains MedDRA hierarchy with English and Japanese terms (without support for the J term currency detail).
PATHS/PATH (version 2.0)	Contains MedDRA hierarchy with English and Japanese terms (with support for the J term currency detail) for the LLT term.

Product Study License Interface

This section provides information for integrating with an external Product Study License configuration system.

Detailed steps and examples on using the PSL interface are available through the Technical Reference Manuals (TRMs). Customers can download these TRMs through the Oracle Consulting or Customer Support teams.

1. Navigate to `<Install Path>\Oracle\ArgusWeb\ASP\Integrations`.
2. Open the `Service.config` file in a text editor.
3. Search for **DatabaseConfiguration**, and update the following attributes:
   - **DBName**—TNS of the Oracle Argus Safety database.
   - **DBUser**—User name of an Oracle Argus Safety Service user. The PSL web service uses this User Context to perform updates in the Oracle Argus Safety Database.
4. To secure the configuration, set the **bindingConfiguration** attribute either manually or through the Service Config utility.

   Additional binding configurations may also be created and used.

   Note that the binding configurations between the host and the client must be compatible for successful communication.
5. To add logging information, use one of the following:
   - **Relsys Logger**—Logs information about errors, warnings, and processing of the PSL web service code. The logger internally uses **log4net** component to perform the logging.
     Update the **logConfig** attribute with one of the following values:
     - Error (default)
     - Warning
     - Information
     - Verbose

     To save log as a specific file, update **RollingLogFileAppender** with the filename. Make sure the web service has read/write permissions to this folder.
   - **SOAP Message RequestLogger**—Logs all the incoming and outgoing SOAP messages of the PSL web service. The messages are stored internally in the Oracle Argus Safety Database and are not available for querying.
     To disable this logging, set **Enabled** as **false**.

     ```
     <TransformersConfiguration> <Transformers> <add Transformer="RequestLogger"
     InterfaceType="Inbound" RequestType="Request,Response"
     MessageType="SoapMessage" Enabled="False" Metadata=""
     ```

```
Assembly="ConsoleInterface"
Type="Relsys.ArgusConsole.ConsoleInterface.Common.DBLoggerFactory" />
</Transformers> </TransformersConfiguration>
```

WHO Drug Coding Interface

WHO Drug web service Interface provides a mechanism to integrate customer-hosted central WHO Drug coding web service with Oracle Argus Safety. Oracle Argus Safety expects the data from central WHO Drug Coding system in defined format as specified by WHO Drug Coding schema.

In a multi-tenant setup, endpoint configuration of central WHO drug coding web service is stored at global level and all enterprises in Oracle Argus Safety will use the same web service endpoint. 'EnterpriseShortName' attribute will be present in the request message payload to identify which Enterprise initiated the web service request.

For more information, see the following:

- Configuration
- Drug Dictionary Coding Flow
- WHO Drug Coding: XML Schema

Configuration

- **Argus Console**
  Drug Dictionary integration must be enabled using Argus Console. This can be done by opening Console from Argus Web and selecting **System Configuration > System Management** from the menu. Expand the **Case Processing** tree branch and select **Dictionary Browser**. Select the radio button to use web services under the "Argus Safety WHO Drug Coding Method" section.

  An optional checkbox is also available to determine whether Oracle Argus Safety has to use the local WHODrug instance if the web service hosting the drug dictionary is not available, fails, or does not return a valid match.

- **Web.Config**
  `Web.config` file on each web server under must have the endpoint with the "name" attribute of "WHODrug" properly configured. At a minimum, the "address" attribute must be changed. Optionally, depending on the bindings employed, the "bindingConfiguration" attribute may also need to be changed. The 'BindingConfiguration' section must have a valid binding for the configured "bindingConfiguration" attribute.

  Sample endpoint configuration with binding configuration:

  ```
  <endpoint address="http://remotewebservice/WHODrugLookup.svc"
  binding="wsHttpBinding" bindingConfiguration="WSHttpBinding_IRelsysService_
  Unsecure"  contract="IRelsysService" name="WHODrug"></endpoint>
  ```

Drug Dictionary Coding Flow

When Oracle Argus Safety makes a call to the web service, it will populate the 'DRUG_NAME' node. Oracle Argus Safety expects the central drug dictionary to populate all possible information in the response XML as per define Drug Dictionary Interface response schema. Oracle Argus Safety will display this information in a browser from which the user can select the correct drug.

If the web service does not return any results or is unavailable, Oracle Argus Safety will present the user with the WHODrug browser with local dictionary information if the system is configured to allow this.

> **Note**
>
> If an ingredient is returned that is not in the 'LM_INGREDIENTS' table of Oracle Argus Safety, the ingredient will not be stored with the case. ATC code is also not stored with the case data. However, both of these items are visible in the browser.

WHO Drug Coding: XML Schema

Schema files for request and response are located in the *<Argus Web Install Path>*`\Integrations\XSD directory`.

Validate WHO drug coding request and response against the following schema files:

- Request: WHODrug_Request
- Response: WHODrug_Response

Request: WHODrug_Request

Oracle Argus Safety will make a web service request to externally hosted Central Drug Dictionary as defined in this schema.

Schema File

Top level file: `/v1.0/WHODrug_Request.xsd`

Sublevel file: `/v1.0/Base.xsd`

Namespace

`http://www.oracle.com/Argus/WHODrug_Request/v1.0`

where v1.0 is the version of the schema

Attribute/Node name	Description
DRUG_DICTIONARY	First Child node under SAFETY_MESSAGE which represents the WHO Drug Dictionary integration.
DRUG/DRUG_NAME	WHO Drug Name that needs to be searched in central WHO Drug Coding system.

Response: WHODrug_Response

Oracle Argus Safety expects Central Drug Dictionary to send the response in this format.

Schema File

Top level file: `/v1.0/WHODrug_Response.xsd`

Sublevel file: `/v1.0/Base.xsd`

Namespace

`http://www.oracle.com/Argus/WHODrug_Response/v1.0`

where v1.0 is the version of the schema

Attribute/Node name	Description
DRUG_DICTIONARY	First Child node under SAFETY_MESSAGE which represents the Drug Dictionary integration.
DRUGS/DRUG	WHO DRUG details

Lot Number Interface

Lot Number Interface provides a mechanism to integrate customer-hosted central product information systems with Oracle Argus Safety via Web service. Oracle Argus Safety expects the data from hosted web service in defined format as specified by Lot Number schema. Oracle Argus Safety stores the web service Configuration at an enterprise level to support integration with different central product information system per Enterprise. 'EnterpriseShortName' attribute will be present in the request message payload to identify which Enterprise initiated the web service request.

Lot Number Query Interface also provides a mechanism for central product information system to pass custom data toOracle Argus Safety system using 'Lot/Custom' node defined in Lot Number Schema. Data passed in the custom node will be stored in Oracle Argus Safety user defined fields of Dosage Regimen section.

For more information, see the following:

- Configuration
- Lot Validation Flow
- Lot Number: XML Schema
- Transformation

Configuration

Lot Number Interface needs to be enabled using Argus Console. This can be done by opening Console from Argus Web and selecting **System Configuration > System Management** from the menu. Expand the **Case Processing** tree branch and select **Lot Number Processing**. Following configurations are supported.

- **Use Centralized Lot Number Validation**
  Yes—Allows Lot Lookup in Case Form to query central product information system to get Lot Number Information.

  No—Lot Lookup in Case Form uses lot numbers defined in Product Configuration under Argus Console >Business Configuration.
- **Allow users to enter non-configured Lot Numbers**
  Yes—Allows user to enter non-configured Lot Number

  No—Mandates user to only select Lot Number from Lot Lookup Dialog.

  This switch is applicable when the lot validation service fails or is unable to provide a match for the lot number.
- **Lot Number Web Service Configuration XML**
  Lot Number Interface support endpoint, binding and transformation configuration of Web Service at an enterprise level. This allows customer to integrate an enterprise in Oracle Argus Safety with different central product information system.

Configuration file must have the endpoint with the "name" attribute of "LotQuery" properly configured.

At a minimum, the "address" attribute must be changed. Optionally, depending on the bindings employed, the "bindingConfiguration" attribute may also need to be changed. The BindingConfiguration section must have a valid binding for the configured "bindingConfiguration" attribute.

The endpoint configuration might look something like this:

```
<endpoint address="http://remotewebservice/LotValidate.svc"
binding="wsHttpBinding" bindingConfiguration="WSHttpBinding_IRelsysService_
Unsecure" contract="IRelsysService" name=" LotQuery"></endpoint>
```

<add Transformer="LotQuery2" **Assembly=**"RelsysInterfaceComponents" **Type=**"Relsys.InterfaceComponents.XSLTTFactory" **InterfaceType=**"Outbound" **RequestType=**"Response" **MessageType=**"RelsysMessage" **Enabled=**"true" **TransformID=**"LOT_NUMBER" **Metadata=**"InputValidationXSD=/Integrations/XSD/v1.0/Lot_Response.xsd;" />

- **Lot Number Web Service XSLT**
  XSLT file required for transforming the response XML. This is only required in case Central Product Information system is passing custom attributes which need to be save as part of Case data in dosage regimen user defined fields.

> **Note**
>
> Oracle Argus Safety provides sample config and XSLT files which can be accessed by clicking **Create** button in 'Lot Number Processing' configuration screen as discussed above.

Lot Validation Flow

When Oracle Argus Safety makes a call to the web service, it will populate the 'LOT_NUMBER' node with data provided by the user. The external lot validation system can provide zero, one, or many results in multiple LOT nodes.

Oracle Argus Safety reaction to various counts of returned lots:

- Zero—Oracle Argus Safety displays a message that the lot number could not be validated; based on the system configuration, the user may be able to keep the entered lot number, in which case Oracle Argus Safety creates a red denotation indicating that the lot number was not validated.
- One—Oracle Argus Safety keeps the user-entered lot number and creates a green denotation indicating a successfully validated lot.
- Many—Oracle Argus Safety displays a dialog from which the user can select the correct lot number; once selected, Oracle Argus Safety creates a yellow denotation indicating that the lot number was validated, but the user had to select from multiple matches.

The lot validation interface also allows for custom data to be returned, such as Albumin or Thermisol which is not natively supported by Oracle Argus Safety. This data is then stored in the user-defined fields available on the active case form page.

Lot Number: XML Schema

Schema files for request and response are located in the *<Argus Web Install Path>*\Integrations\XSD directory.

Validate Lot Number request and response against the following schema files:

- Request: Lot_Request
- Response: Lot_Response

Request: Lot_Request

Oracle Argus Safety will make a web service request to externally hosted central product information system as defined in this schema.

Schema File

Top level file:

\v1.0\Lot_Request.xsd

Sublevel file:

\v1.0\Base.xsd

\v1.0\ProductFamilyEntity.xsd

Namespace

http://www.oracle.com/Argus/Lot_Request/v1.0

where version 1.0 is the version of the schema

Nodes/Attributes

Attribute/Node name	Description
LOT_LOOKUP	First Child node under SAFETY_MESSAGE which represents the Lot integration
LOT	Oracle Argus Safety defined complex type element having following elements and attributes: • LOT_NUMBER • EXPIRATION_DATE

Response: Lot_Response

Oracle Argus Safety expects Central Lot Number Web service to send the response in this format:

Schema File

Top level file:

/v1.0/Lot_Response.xsd

Sublevel file:

/v1.0/Base.xsd

`/v1.0/ProductFamilyEntity.xsd`

Namespace

`http://www.oracle.com/Argus/Lot_Response/v1.0`

where v1.0 is the version of the schema

Attribute/Node name	Description
LOT_LOOKUP	First Child node under SAFETY_MESSAGE which represents the Lot Number integration.
LOT	• LOT Number • Expiration Date • Custom Provides a mechanism **Name**: Attribute value is used to identify Case Form field that is to be populated with data in the node. **Metadata**: Attribute value is used as labels in the LOT Number selection dialog displaying the data.

Transformation

If custom data is to be passed back by the lot validation service, then it is also necessary to modify the `LotIncomingTransform.xslt` file, located in the `.\ArgusWeb\ASP\Bin` directory. This transformation file reads the CUSTOM tags passed back by the lot validation service and maps them to the Oracle Argus Safety user-defined fields.

The CUSTOM tag has a "Name" attribute, which is used by the XSLT to identify to which Oracle Argus Safety field to map. The corresponding "Metadata" attribute is used simply to display a label in the lookup dialog if necessary. The XSLT file must be synchronized between all web servers in a web farm scenario.

Specific Oracle Argus Safety fields must be placed within the xsl:attribute tags of the XSLT in a comma delimited form. The system will attempt to populate each Oracle Argus Safety field specified by the value of the CUSTOM tags. If a field does not exist, no exception is thrown. In this fashion, if different pages in the case form have different definitions for the user-defined fields, the system can still properly populate the values in the fields.

It is inadvisable to modify any piece of the XSLT file with the exception of the piece that is shown in the example below. Consider the web service returns a CUSTOM node like:

```
<CUSTOM Name="Albumin" Metadata="Albumin Status">19.5 mg/gC</CUSTOM>And the
LotIncomingTransform.xslt contains the snippet:
<xsl:template match="@*" mode="CaseField">
  <xsl:choose>
    <xsl:when test=".='Thermisol'">
      <xsl:attribute name="CaseField">CASE_DOSE_REGIMENS_UD_TEXT_1,CASE_DOSE_
REGIMENS_UD_TEXT_2</xsl:attribute>
    </xsl:when>
    <xsl:when test=".='Albumin'">
      <xsl:attribute name="CaseField">CASE_DOSE_REGIMENS_UD_TEXT_3,CASE_DOSE_
REGIMENS_UD_TEXT_4</xsl:attribute>
    </xsl:when>
  </xsl:choose>
</xsl:template>
```

Then the value of 19.5 will be mapped to both user defined text fields 3 and 4. If only one of the fields is on the active case form page, the other field will be ignored.

Worklist Intake

This section provides information for integrating with an external system generating potential case data.

CASE_INTAKE is the first child node identifying a worklist intake integration.

For more information, see the following:

- Configuration
- Worklist Intake Flow

Configuration

Worklist Intake integration currently employs a file drop system. The drop directories should be on a shared path. The directories can be optionally unique to a user site and configured as such in Console. The first step is to set these directory references up in Console under the "User Sites" code list. For each user site, simply specify the UNC for the "Intake File Path" (they can all be the same or different).

Oracle Argus Safety Windows Service provides the mechanism by which the files are processed. Since a network resource is being accessed, it is essential that the service run as a domain account and not as the Local System Account (which is the default). To change this, stop the Oracle Argus Safety Windows Service by opening the Services control panel and double-clicking the Oracle Argus Safety Windows Service and clicking the **Stop** button. Next click the **Log On** tab and select the radio button for "This account". Enter valid domain user credentials and click OK.

The service itself contains additional configuration information in the `RelsysWindowsService.exe.config` file located in the `.\ArgusWeb\ASP\Argus.NET\Bin` directory. This file references the Intake.config file to obtain configurations specific to Worklist Intake. Simply uncomment the two "add" nodes in the "RelsysConfigFilesSection" that reference the `Intake.config` file in their "filePath" attributes. Also verify that the DatabaseConfiguration section in this file has a valid database and user credentials with which to connect to the database and access Oracle Argus Safety data.

In the same folder the `Service.config` file also requires some changes to specify information about the assemblies needed to process Worklist Intake messages. Similarly to the `RelsysWindowsService.config` file, uncomment the two "add" nodes whose "name" attributes refer to "Case Intake" and "Case Intake Ack".

Once configured, use the Services control panel to restart Oracle Argus Safety Windows Service. A successful configuration is evident when four new folders are then created in the shared file path (IN, OUT, INTERMEDIATE, and FAILURES).

If the shared folder happens to be on the same physical machine as the server on which “Argus Windows Service" is running, you can optionally configure the service to access the shared folder directly as a local folder instead of as a network shared path. The following configuration in `Intake.config` would enable this:

```
  <FolderConfiguration>
    <MonitorFolders MonitorAllConfiguredFolders="true"
MonitorLiteratureFolder="false">
      <add FolderPath="<configured share in console>" Monitor="true"
AlternatePath="C:\CaseIntake"/>
```

```
    </MonitorFolders>
  </FolderConfiguration>
```

In the above configuration, **MonitorAllConfiguredFolders** can be set to false if you want to configure that server to accept Intake files only for the folders configured in the above section and for which Monitor is set to true.

Worklist Intake Flow

When an XML file is dropped in the IN folder of the configured Intake folder, Oracle Argus Safety picks up the file and does an initial verification. If there are any attachments specified in the XML, they and the XML are moved to a GUID-created subfolder of the Intermediate folder. All the relevant data is extracted from the XML and stored in the database. During the parsing and extraction, if there are any errors, the unique folder and its associated XML and file attachments are moved to Failures folder. A file called `Error.xml` will be generated in that folder which contains more information about the failure. If an e-mail address is configured in Intake.config, an e-mail is also generated and processed via AGService.

Worklists for intake are based on user site. They are populated based on either the path in which the initial file was dropped (as per the configuration in Argus Console the path is associated to a specific user site) or by the value of the SITE node contained within the XML itself. If there is a conflict, the SITE node value takes precedence.

The Intake records that are absorbed into Oracle Argus Safety are visible to the Oracle Argus Safety User in Worklist Intake screen in Oracle Argus Safety or in afOracle Argus Affiliate. The Oracle Argus Safety user can do one of two operations on the Intake record.

1. **Accept**—When the user accepts an Intake, the case form book-in screen is shown which will contain information and attachments pre-populated from the Intake record.
    - If user books in a case, a response is generated which contains the case ID and case number. The attachment details and response XML are placed in the Out folder.
    - If user adds a follow up to an existing case, a similar response is generated as above and the response XML is placed in the OUT folder.
2. **Reject**—When the user rejects an Intake record, a response is generated which contains the Rejection Reason and the attachment details. This response XML is placed in the OUT folder.

Similarly, an Oracle Argus Affiliate user can create a local event from an Intake record from within Oracle Argus Affiliate. The flow is similar to that mentioned above with the exception that the response XML would contain the Local Event Number instead of the case number.

Literature Intake

This section provides information for setting up Literature Intake. Oracle Argus Safety accepts files of the following formats for Literature Intake.

- WORLD MEDICAL & DRUG INFORMATION SERVICE (WMDIS) (in the form of .xls or .xlsx file format)
- JAPIC (in the form of .txt file format)

For more information, see the following:

- Configuration
- Literature Intake Flow

Configuration

Literature Intake integration employs a file drop system. The drop folder should be on a shared path. The folder must be configured in Console under **System Configuration** > **Common Profile Switches** > **Argus J**.

The edit box provided for "Shared Path for Literature Intake" must be configured with the UNC file path of the shared folder. Oracle Argus Safety Windows Service provides the mechanism by which the files are processed. Since a network resource is being accessed, it is essential that the service run as a domain account and not as the Local System Account (which is the default).Argus Release Media

To change this, stop the Oracle Argus Safety Windows Service by opening the Services control panel and double-clicking the Oracle Argus Safety Windows Service and clicking the **Stop** button. Next click the **Log On** tab and select the radio button for "This account". Enter valid domain user credentials and click **OK**.

The service itself contains additional configuration information in the `RelsysWindowsService.exe.config` file located in the `.\ArgusWeb\ASP\Argus.NET\Bin` directory. This file references the `Intake.config` file to obtain configurations specific to Worklist Intake. Simply uncomment the two "add" nodes in the "RelsysConfigFilesSection" that reference the`Intake.config` file in their "filePath" attributes. Also verify that the DatabaseConfiguration section in this file has a valid database and user credentials with which to connect to the database and access Oracle Argus Safety data. In the same folder the `Service.config` file also requires some changes to specify information about the assemblies needed to process Worklist Intake messages.

- Metadata Configuration

Metadata Configuration

1. Go to the Oracle Argus Safety Web server machine.
2. Open the service.config file located at...

   <Argus Install Path>`\ArgusWeb\ASP\Argus.NET\Bin\`
3. In the service.config file, the metadata configuration is:

```
<add Name="Case Intake" Assembly="CaseIntakeServiceComponent"
Type="Relsys.CaseIntakeServiceComponent.FSWManager"
Metadata="InvokeDirect=true;PollInterval=1000;CaseIntake=true;LitIntake=true;
UseLocalInterimFolder=true; LocalInterimFolder=C:\Temp\CaseIntake"  />
```

Similarly to the `Service.config` file, uncomment the "add" node whose "name" attribute refer to "Case Intake". Ensure that 'LitIntake' is set to true in the Metadata configuration as shown below:

```
<add Name="Case Intake" Assembly="CaseIntakeServiceComponent"
Type="Relsys.CaseIntakeServiceComponent.FSWManager" Metadata="InvokeDirect=true;
PollInterval=1000;CaseIntake=true;LitIntake=true" />
```

In the same folder, the `Intake.config` file needs some changes. Set the MonitorLiteratureFolder attribute to true in FolderConfiguration/MonitorFolders section as shown below:

```
<FolderConfiguration>
<MonitorFolders MonitorAllConfiguredFolders="false"
MonitorLiteratureFolder="true">
<!-- <add FolderPath="<configured share in console>" Monitor="true"
```

```
AlternatePath="C:\LiteratureIntake"/> -->
</MonitorFolders>
</FolderConfiguration>
```

Once configured, use the Services control panel to restart Oracle Argus Safety Windows Service. A successful configuration is evident when four new folders are then created in the shared file path (IN, OUT, INTERMEDIATE, and FAILURES).

If the shared folder happens to be on the same physical machine as the server on which “Argus Windows Service" is running, you can optionally configure the service to access the shared folder directly as a local folder instead of as a network shared path. The following configuration in `Intake.config` would enable this:

```
<FolderConfiguration>
<MonitorFolders MonitorAllConfiguredFolders="false"
MonitorLiteratureFolder="true">
<add FolderPath="<configured share in console>" Monitor="true"
AlternatePath="C:\LiteratureIntake"/>
</MonitorFolders>
</FolderConfiguration>
```

Literature Intake Flow

When a WMDIS or JAPIC file is dropped in the IN folder of the configured Literature Intake folder, Oracle Argus Safety picks up the file and does an initial verification. The file is first moved to a GUID-created subfolder of the Intermediate folder. All the relevant data is extracted from the file and stored in the database. During the parsing and extraction, if there are any errors, the unique folder and the file in it are moved to Failures folder. A file called `Error.xml` will be generated in that folder which contains more information about the failure. If an e-mail address is configured in `RelsysWindowsService.exe.config`, an e-mail is also generated and processed via AGService. The Literature Intake Worklist shows all the records extracted from the above mentioned files.

The Oracle Argus Safety user can do one of the following operations on the Literature Intake record.

- Accept
- Reject
- Assign User
- Assign Literature Type
- Modify Product Family

Extended E2B Interface

For more details, from the Argus Safety OHC page, go to the desired release, navigate to the Books page of that release, and refer to the *Oracle Argus Safety ICSR Extensibility Guide*.

6

Install and Start Oracle Argus Safety Service

Before you begin

Make sure to Install Language Packs to Generate Reports.

Proceed to:

- Install Oracle Argus Safety Service
- Start Oracle Argus Safety Service

Install Oracle Argus Safety Service

1. Log in as the administrator on the system where Oracle Argus Safety is being installed.
2. Copy the installation package to the local directory of the target machine.
3. Open the Oracle Argus Safety folder and click **setup.exe**.
4. In the Argus Suite Solution Components Installation Wizard, click **Next**.
5. Enter the User Name and Company Name, and click **Next**.
6. In the Default Directory screen, to select the default installation directory where the Argus Suite Solution Components will be installed, click **Browse**.
7. To display the Argus Suite Components list, click **Next** and select the default installation directory.
8. Under **Transaction Server**, select **Argus Safety Service**, and click **Next**.

   The Argus Suite Solution Components Report Directory appears.
9. Select the directory where temporary reports will be stored, and click **Next**.

   You can browse through any path or leave this as default (C:\Temp).
10. In the Setup Completed dialog box, click **Finish**.
11. In the Argus Suite Setup dialog box, click **OK** to reboot the system.
12. See Other Tasks for information about tasks that must be completed after the Argus Safety service has been installed.
13. To set up the Argus Cryptography Key, refer to Oracle Argus Safety Application Servers.
14. To configure the Oracle Argus Safety Service user passwords, refer to Generate Encrypted String.

Start Oracle Argus Safety Service

Before you can start the Oracle Argus Safety Service, you must configure a single process or it will fail to start. To configure the Oracle Argus Safety Service process, refer to the *Oracle Argus Safety Service Administrator's Guide*.

To start the Oracle Argus Safety Service:

1. Select **Start** > **Control Panel** > **Administrative Tools**.

2. Double-click the Component Services shortcut.
3. In the left navigation pane, click **Services**.
4. From the list of services (in the right navigation pane), right-click the Oracle Argus Safety Service, and click **Properties**.
5. In the Oracle Argus Safety Service **Properties** > **General** tab, from the **Startup type** drop-down, select **Automatic**.
6. Click the **Log On** tab, select **This account**, enter the parameters, and click **OK**.

> **Note**
>
> You must enter a domain account with access to the domain printers.

7. Click **Start**.
8. Click **OK**.

> **Note**
>
> You can view the log file at the specified path in the Oracle Argus Interchange Service INI file.

7

Install and Configure Oracle Argus Interchange

The Oracle Argus Interchange Server is meant to off-load Oracle Argus Interchange Service from the Argus Transaction Server. Alternatively, Oracle Argus Interchange Service can be installed on the Transaction Server itself. To configure Oracle Argus Interchange Services through Oracle Argus Interchange Mapping user interface, both must be installed on the same system.

Prerequisites

1. Obtain a domain account with local administrator privileges.
2. Create a network account to enable Oracle Argus Interchange Service to communicate with the e-mail system and access the shared folders on the Axway B2Bi Server.
3. Install Language Packs to Generate Reports.

Install Oracle Argus Interchange Service

1. Log in as the Administrator on the system where Oracle Argus Safety is being installed.
2. Copy the installation package to the local directory of the target machine.
3. Open the Oracle Argus Safety folder and click **setup.exe**.
4. In the Argus Suite Solution Components Installation Wizard, click **Next**.
5. Enter the User Name and Company Name, and click **Next**.
6. In the Default Directory screen, to select the default installation directory where the Argus Suite Solution Components will be installed, click **Browse**.
7. To display the Argus Suite Components list, click **Next** and select the default installation directory.
8. Under **Transaction Server**, select **Argus Interchange Service**, and click **Next**.

   The Argus Suite Solution Components Report Directory appears.
9. Select the directory where temporary reports will be stored, and click **Next**.

   You can browse through any path or leave this as default (C:\Temp).
10. Click **Yes** to configure a database for Oracle Argus Interchange.

11. Enter the database name as you want it to appear in Oracle Argus Interchange and click **Next**.
12. Enter the database SID and click **Next**.
13. In the Setup Completed dialog box, click **Finish**.
14. Click **OK** to reboot.
15. To set up the Oracle Argus Safety Cryptography Key, refer to Oracle Argus Safety Application Servers.

Configure Oracle Argus Interchange Service

1. Select **Start** > **Control Panel** > **Administrative Tools**.
2. Double-click the **Component Services** shortcut.
3. In the left navigation pane, click **Services**.
4. From the list of services (in the right navigation pane), right-click the Oracle Argus Interchange Service, and click **Properties**.
5. In the Oracle Argus Interchange Service **Properties** > **General** tab, from the **Startup type** drop-down, select **Automatic**.
6. Click the **Log On** tab, select **This account**, enter the parameters, and click **OK**.

> **Note**
>
> You must enter a domain account with access to the domain printers.

7. Click **OK**.

> **Note**
>
> You can view the log file at the specified path in the Oracle Argus Interchange Service INI file.

Access EDI Gateway Shared Folders

1. Log in to the machine where Oracle Argus Interchange Service is installed.
2. Browse to the data folder in the EDI Gateway installation directory.

> **Note**
>
> If the data folder is not shared, contact the System Administrator for access to the folders.

3. Verify that you can access the following folders:
   - `<company profile>/ediin`
   - `<company profile>/ediout`

- `<company profile>/xmlin`
- `<company profile>/xmlout`

4. Log off of the EDI Gateway machine.
5. Log in the Oracle Argus Interchange Service machine and make sure no password is required for connecting to the shared folders on the EDI gateway machine.

Configure Interchange Server

To configure the Interchange Server, go to `Argus Console > System Configuration > Interchange > Service Configuration`. For more details, refer to the *Oracle Argus Interchange User's Guide*.

To move the existing Interchange Service configuration data from .INI file to the database, refer to the *MOS Knowledge Base article with Doc ID 2965425.1*.

8

Configure the Oracle Argus Insight Application

This chapter provides information about configuring the Oracle Argus Insight application and the Oracle Argus Insight scheduling service.

Log In to Oracle Argus Insight for Configuration and Setup

1. Log in with rights to a workstation from where you can access the Oracle Argus Insight application.
2. Start Chrome.
3. In the Address bar, enter the following URL to start the Oracle Argus Insight:

   `http://Argus_Insight_WebServer_Name:port_number/ArgusInsight`
   Where, the port number is same as ArgusSafety.
4. Press **Enter**.

   The Oracle Argus Insight Login screen appears.
5. Log in to the Oracle Argus Insight application:
   a. In the **User Name** field, enter `admin`.
   b. In the **Password** field, enter the password for the admin user.

      This password is the same as the password of the admin user in Oracle Argus Safety.
   c. Click **Login**.

> **Note**
>
> If you are using a Single Sign On (SSO) environment, you must ensure that SSO tools such as Oracle Access Manager are disabled on the Oracle Argus Insight Web Server for initial configuration. The only administrator user in Oracle Argus Insight is a non-LDAP user. A non-LDAP user cannot log in to Oracle Argus Insight with SSO tools set to Enabled.

> **Note**
>
> In case of a multi-tenant setup, you must ensure that the entire configuration is done using the default enterprise.
>
> - This will help in copying the configuration to a different enterprise
> - All the global configuration is available in the default enterprise.

Configure the Oracle Argus Insight Application Profile Switches

Profile switches are a collection of settings that let you configure the default behavior of the system. This section describes the profile switches that you must set to establish connectivity with your Oracle Analytics tool and to run the initial ETL.

For detailed information about all the profile switches, see:

- *Oracle Argus Insight Common Profile Enterprise Table Guide* (`CMN_PROFILE_ENTERPRISE.pdf`)
- *Oracle Argus Insight Common Profile Global Table Guide* (`CMN_PROFILE_GLOBAL.pdf`)

You can also visit the following for more information:

- Access and Modify the Profile Switches
- Set Up the Populate Data Attributes
- Set Up the Email Attributes
- Set Up the Attributes Specific ONLY to Oracle Argus Mart
- Set Up the Attributes Specific ONLY to Oracle Analytics Publisher
- Set Up the Attributes Specific ONLY to Oracle Analytics Server

Access and Modify the Profile Switches

To access and modify the Oracle Argus Insight profile switches:

1. Log in to the Oracle Argus Insight application.
2. On the Oracle Argus Insight home page, from the upper-right corner, click the **Tools** tab.

   The Administration Tools screen appears.
3. Click the **List Maintenance** tab.
4. From the List Maintenance Items group, select **Profile Switches**.

   The Attributes group is updated with the profile switches that you may configure.

> **Note**
>
> When the Oracle Argus Insight Database Source profile switch is set to **Argus Mart**, then in the List Maintenance section, only **Profile Switches** and **Case Series Modification Justification** list maintenance items are available.
>
> For more information on this profile switch, see Set Up the Attributes Specific ONLY to Oracle Argus Mart.

Set Up the Populate Data Attributes

You may control data population based on data attributes.

The following is the list of profile switch along with their value required to be set to populate data attributes.

Table 8-1 Populate Data Attribute-Value set

Attribute	Value
POPULATE AFFILIATE DATA	0 — Do not bring any affiliate data into the Oracle Argus Insight data mart. 1 — Bring all affiliate data into the Oracle Argus Insight data mart.
POPULATE INTERCHANGE DATA	0 — Do not bring any interchange data into the Oracle Argus Insight data mart. 1 — Bring all interchange data into the Oracle Argus Insight data mart. 2 — Bring only the SAFETYREPORT, MESSAGES, and EDI_INFO tables data into the Oracle Argus Insight data mart.
POPULATE CASE/ CONFIGURATION DATA	0 — Populate configuration data only. 1 — Populate all the data (both case and configuration data).
LEGACY REPORTS CONFIGURATION	0 — Configuration items are not visible. 1 — Configuration items are visible. **Note** If Legacy Reports Configuration switch is set to 1, then legacy reports switches becomes available for obsolete reports, and you must configure the following switches: • POPULATE NARRATIVE LANGUAGES TABLE • COMPANY LOGO PATH • DAYS TO LOCK • UDN COLUMN FOR SUPPLIER NAME • FOLLOW-UP ACTION CODE • POPULATE DLL SLL REPORTS TABLE DATA To configure these switches, refer to *Oracle Argus Insight Installation Guide* (v7.02).

To set the data attributes:

1. On the Administration Tools screen, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select a profile switch, and click **Modify**.

   The Modify Attributes dialog box appears.

> **Note**
>
> See Table 8-1.

4. In the **Value** field, enter a numeric value, and click **OK**.

   The profile switch is set and you return to List Maintenance tab.

Set Up the Email Attributes

You may configure the profile switches that relate to sending and receiving email after an extract, transform, and load (ETL) operation has completed, as well as sending email for scheduled reports.

The following is the list of profile switch along with their value required to be set for email messages and delivery.

Table 8-2 Email Specific Attribute-Value set

Attribute	Value
ETL EMAIL SETUP	0 — Send no email message after an ETL operation. 1 — Send an email message only if an initial or incremental ETL fails. 2 — Send an email message only if an initial or incremental ETL succeeds. 3 — Send an email message after any initial or incremental ETL (failure or success).
ETL EMAIL RECEIVER ADDRESS	Specify the email address of each administrator who should receive email status messages of the ETL process. Use a semi-colon to separate each entry. If the Value field blank, then no email messages are sent.
EMAIL SENDER ADDRESS	Specify the email address of each administrator who should receive email status messages of the ETL process. Use a semi-colon to separate each entry. If the Value field blank, then no email messages are sent.
FAILED RECIPIENTS STATUS EMAIL ADDRESS	Specify the email address of the user who will receive information about undeliverable emails.

To configure the attributes related to email messages and delivery:

1. On the Administration Tools screen, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select a profile switch, and click **Modify**.

   The Modify Attributes dialog box appears.

> **Note**
>
> See Table 8-2.

4. In the **Value** field, enter a value, and click **OK**.

   The profile switch is set and you return to List Maintenance tab.

> **Note**
>
> Make sure you validate the network proxy settings before executing the Incremental ETL.
>
> Refer to *Oracle Argus Insight Installation Guide*, *Section 9.1.6 Verify and Update Network Proxy Settings*.

Set Up the Attributes Specific ONLY to Oracle Argus Mart

Oracle Argus Insight supports queries for analysis of the historical case data based on specific date/time through Oracle Argus Mart. To enable access to this data in Oracle Argus Mart, you need to set specific attributes.

The following is the list of profile switch along with their value required to be set to populate Oracle Argus Insight data into Oracle Argus Mart database.

Table 8-3 Oracle Argus Mart Specific Attribute-Value set

Attribute	Value
Oracle Argus Insight Application Data Source	Enables you to configure the data source for Oracle Argus Insight. You may run your queries for Oracle Argus Insight or Oracle Argus Mart depending on the value configured in this switch. **Argus Mart** — Enable queries on Oracle Argus Insight data source only. **Insight Mart** — Enable queries on Argus Insight data source only. **Both** (Oracle Argus Insight Mart and Oracle Argus Mart) — You may choose between Oracle Argus Insight Mart and Oracle Argus Mart data sources for creating and executing your queries. All the queries and case series created on these data sources can be identified in the application.
ARGUS MART DB NAME	Specify the database instance name for the Oracle Argus Mart data mart. This information enables to connect Oracle Argus Insight with Oracle Argus Mart database.
ARGUS MART USER NAME	Specify the schema user created for Oracle Argus Insight in Oracle Argus Mart database. This user may perform all the background functions from Oracle Argus Insight application to Oracle Argus Mart database including querying and reporting.
ARGUS MART USER PASSWORD	Specify the password of the schema user created for Oracle Argus Insight in Oracle Argus Mart database that is, the password of user configured in ARGUS MART USER NAME.

Table 8-3 (Cont.) Oracle Argus Mart Specific Attribute-Value set

Attribute	Value
ENABLE_AI_PROCESSING	**Note** Use Oracle Argus Safety Console to enable this profile switch. This profile switch must be set to **Yes** to link Oracle Argus Insight database to Oracle Argus Mart database. **Yes** — Enable Oracle Argus InsightProcessing for Oracle Argus Mart. **No** — Disable Oracle Argus Insight Processing for Oracle Argus Mart.

Note

These profile switches are optional and should be configured only if you want to run Advanced Conditions on Oracle Argus Mart database.

Oracle Argus Mart database TNS should be added in the Oracle Argus Insight Web Server TNS and Oracle Argus Insight Database Server TNS.

Oracle Argus Insight Database Server TNS should be added in the Oracle Argus Mart Database TNS.

To set these attributes:

1. On the Administration Tools screen, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select a profile switch, and click **Modify**.

   The Modify Attributes dialog box appears.

   Note

   See Table 8-3.

4. In the **Value** field, enter a value, and click **OK**.

   The profile switch is set and you return to List Maintenance tab.
5. Log on to Oracle Argus Safety Console in separate window, and set ENABLE_AI_PROCESSING profile switch to **Yes**.

Set Up the Attributes Specific ONLY to Oracle Analytics Publisher

If you are using Oracle Analytics Publisher as your Oracle Analytics tool with Oracle Argus Insight, you need to set the following Oracle Analytics Publisher-specific attributes:

- BIP WEB URL

- KEEP REPORT DATA

To define the attributes required for Oracle Analytics Publisher:

1. On the Administration Tools page, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select **BIP WEB URL**.
   a. Click **Modify**.

      The Modify Attribute dialog box appears.

   b. In the **Value** field, enter the name of the Oracle Analytics Publisher Web URL to open the Oracle Analytics Publisher home page.

      This URL can be the Oracle Analytics Publisher URL for standalone Oracle Analytics Publisher or the Load Balancer URL configured for multiple Oracle Analytics Publisher. If Oracle Analytics Publisher is configured for SSL, you must use https with the URL. For example: `https://<server name>:<Port Number>/xmlpserver`

   c. Click **OK** to save the changes and return to the List Maintenance tab.
4. From the Attributes group, select **KEEP REPORT DATA**.

   This attribute is used to determine if the report log tables needs to be populated or not.

   a. Click **Modify**.

      The Modify Attribute dialog box appears.

   b. In the **Value** field, enter **Yes** or **No**.

      The value **Yes** denotes that the Report Log tables should be populated. The value **No** denotes that the Report Log tables should not be populated.

   c. Click **OK** to save the changes and return to the List Maintenance tab.

Set Up the Attributes Specific ONLY to Oracle Analytics Server

If you are using Oracle Analytics Server with Oracle Argus Insight, you need to set the Oracle Analytics Server specific attributes:

- BI ANSWERS WEB URL

To define the attributes required for Oracle Analytics Server:

1. On the Administration Tools screen, click the **List Maintenance** tab.
2. From the List Maintenance Items group, select **Profile Switches**.
3. From the Attributes group, select **BI ANSWERS WEB URL**, and click **Modify**.

   The Modify Attributes dialog box appears.
4. In the **Value** field, enter the path for the BI ANSWERS WEB URL.

   For example, this path can be the OAS URL: `https://<server name>:<Port Number>/analytics`
5. Click **OK**.

   The profile switch is set and you return to List Maintenance tab.

Configure Duration Value Bands

In Oracle Argus Insight, you can map the following time values (entered in Oracle Argus Safety) to specific ranges called Duration Value Bands:

- Time to Onset from First Dose
- Time to Onset from Last Dose

You set the value of these fields in Oracle Argus Safety by navigating to Product tab, Drug Duration of Administration, and Events Tab.

By mapping the time values to Duration Value Bands in Oracle Argus Insight, you can specify query criteria based on ranges instead of specific values for the *Time to Onset* fields listed above.

Using the Duration Value Bands item on the List Maintenance tab, you can configure duration value bands in hours, days, weeks, months, and years. For each band, you can specify multiple ranges by entering minimum and maximum values for each range item. Any value that falls within a configured range will map to that range.

> **Note**
>
> Duration Value Band configuration must be done before running the Initial ETL.
>
> If Duration Value Bands are modified after Initial ETL, you must re-run the Initial ETL.

For more information, see the following:

- Modify a Duration Value Band

Modify a Duration Value Band

1. On the Oracle Argus Insight home page, click the **Tools** tab from the upper-right corner.

   The Administration Tools screen appears.
2. Click the **List Maintenance** tab.
3. From the List Maintenance Items group, select **Duration Value Bands**.

   The Attributes group displays the valid bands (Hours, Days, Weeks, Months, and Years). You can modify the values of these bands. You cannot, however, add more bands or delete an existing band.

   > **Note**
   >
   > When the Oracle Argus Insight Database Source profile switch is set to **Argus Mart**, then in the List Maintenance section, only **Profile Switches** and **Case Series Modification Justification** list maintenance items are available.
   >
   > For more information on this profile switch, see Set Up the Attributes Specific ONLY to Oracle Argus Mart.

4. Select the duration value band (Hours, Days, Weeks, Months, Years) you want to change, and click **Modify**.

   The Duration Value Bands Configuration dialog box appears with the factory-configured ranges.

   > **Note**
   >
   > - The Label column represents the name of the range.
   > - The Lower Range (>=) and Higher Range (<) columns contain the minimum and maximum values, respectively.
   > - The highest value band includes all values that are greater than the highest range value specified.

5. Modify the values:
   - To modify an existing range, edit the values in the **Lower Range (>=)** and **Higher Range (<)** fields.
   - To add a range, scroll to the current highest range and click in the blank **Higher Range (<)** field.

     Enter a value greater than the current highest range, and press **Tab** to add a new row.
   - To delete an existing range, click the **Delete** icon next to the row.

     Note that you cannot delete the lowest band.

     If you delete an intermediate range, the system automatically converts the highest value of the deleted range to the lowest value in the next range. However, the system does not change the range labels.
6. Click **OK** to save the changes.

Configure Derivation Functions

You can create a new List Maintenance item and derive specific cases to this item based on case attributes. These attributes are supplied to the system as SQL.

For example:

1. Create a new List Maintenance item called `Report Type 1`, and derive all the cases with the **Report Type** attribute defined as **Spontaneous**, **Literature**, or **Compassionate Use**.

   The Report Type 1 appears as an option in the query tool interface corresponding to the Report Type attribute.
2. From the Report Type, select **Report Type 1**, and execute the query.

   Cases with the Report Type attribute specified as Spontaneous, Literature, or Compassionate Use are returned.

You can specify more than one attribute.

For example, create a further specialized List Maintenance item called `Report Type 1 US`, and derive all the cases that have the **Report Type** attribute defined as **Spontaneous**, **Literature**, or **Compassionate Use**, *and* the **Country of Incidence** attribute defined as **United States**.

> **Note**
>
> There can be situations where two different List Maintenance items you create contain similar attributes in the SQL criteria. In this case, you can assign a priority level to individual List Maintenance items. The priority level determines which List Maintenance item SQL executes first.

For more information, see:

- Open the Derivation Fields Dialog Box
- Icons in the Derivation Fields Dialog Box
- Field Mapping Derivation Rules
- Fields and Check Boxes in the Derivation Fields Dialog Box

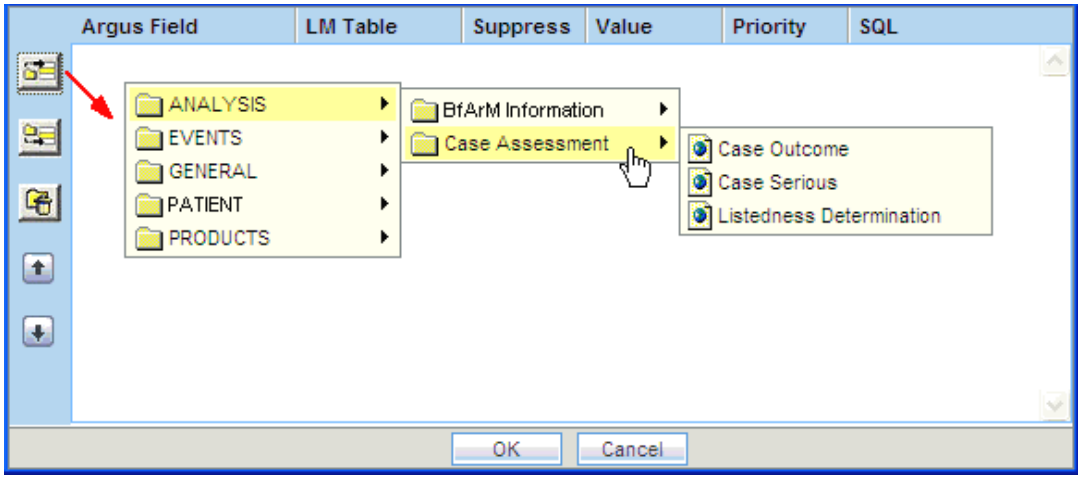
Open the Derivation Fields Dialog Box

To open the Derivation Fields dialog box and configure derivation functions:

1. On Oracle Argus Insight home page, click the **Tools** tab from the upper-right corner.

   The Administration Tools screen appears.
2. Click the **List Maintenance** tab.
3. From the List Maintenance Items group, select **Derivation Functions**.
4. From the Attributes group, select **All Derivations**, and click **Modify**.

   The Derivation Fields dialog box appears.



Icons in the Derivation Fields Dialog Box

Table 8-4 describes the icons in the Derivation Fields dialog box that you can use to add, delete, and reorder derivation field elements (rows).

Table 8-4 Icons in the Derivation Fields Dialog Box

Click…	To…
	Add a derivation field element (row) above the currently selected row
	Add a derivation field element (row) below the currently selected row
	Delete the currently selected derivation field element (row)
	Move the selected row up
	Move the selected row down

Field Mapping Derivation Rules

Table 8-5 lists the available field mapping derivation rules for Oracle Argus Insight.

Table 8-5 Field Mapping Derivation Rules

Function Category	Function Sub-category	Oracle Argus Insightt Field
ANALYSIS	BfArM Information	Causality
ANALYSIS	Case Assessment	Case Outcome Case Serious Listedness Determination
EVENTS	Event Information	Lack of Efficacy
GENERAL	General Information	Report Type Derived Pregnancy
PATIENT	Patient Information	Age Group Gender Patient weight BMI desc

Table 8-5 (Cont.) Field Mapping Derivation Rules

Function Category	Function Sub-category	Oracle Argus Insightt Field
PRODUCTS	Product Drug	Derived Drug Abuse
		Derived Drug Interaction
		Derived Overdose
		Last daily dose

> **Note**
>
> Causality, Report Type, Age Group, and Last daily dose are comma-separated derivation rules.

Fields and Check Boxes in the Derivation Fields Dialog Box

This section describes the fields and check boxes in the Derivation Fields dialog box.

- LM Table
- Suppress
- Value
- Priority
- SQL

LM Table

The LM Table field is the table name of the selected Oracle Argus Safety field (that is, automatically populated).

Suppress

The Suppress check box is available for fields associated with the list maintenance data. When suppress is enabled for a field, the corresponding list maintenance values that are not present in any case are deleted and thus not available for querying.

> **Note**
>
> The Suppress check box is applicable *only if* the condition specified in the SQL text box covers all the cases having the selected List Maintenance field.

Value

The Value field captures the value for the new derivation field. For the following rules, you must enter the new value for the rule as a comma-separated value:

- Causality
- Report Type

- Age Group
- Last Daily Dose

> **Note**
>
> Make sure to enter the values for these rules as defined in the following sections. Unexpected results and/or ETL errors may result if the values are not entered as specified.

Causality Rule

Parameters: VALUE, REPORTABILITY

where:

VALUE = New value for the rule

REPORTABILITY = Lower value of the group

Example: NewCausality,1

Report Type Rule

Parameters: VALUE, INC_LIT, INC_TRIAL, ABRV

where:

VALUE = New value for the rule

INC_LIT = 1 if Literature Report Type else 0

INC_TRIAL = 1 if Clinical Trial Report Type else 0

ABRV = A 3-letter abbreviation for the Report Type

Example: NewReportType,0,1,NRT

Age Group Rule

Parameters: VALUE, GROUP_LOW, GROUP_HIGH

where:

VALUE = New value for the rule

GROUP_LOW = Lowest value of the age group

GROUP_HIGH = Highest value of the age group

Example: NewAgeGroup,25,50

If you do not want to specify the High Value, then the comma is mandatory in the end.

Example: Unknown,70,

Last Daily Dose Rule

Parameters: VALUE, DAILY_DOSE_SORTING_ORDER

where:

VALUE = New value for the rule

DAILY_DOSE_SORTING_ORDER = 1 or 2 or 3 and so on to define the sorting order if there is more than 1 rule for the Last Daily Dose field

Examples: 1 -> 0to1,1; 2 -> 2to3,2 3 -> 5to8,3

Priority

The Priority field captures the priority for a list of derivation rules applied to a single List Maintenance field. The value should be from 1 to 255.

> **Note**
>
> The priority for derivation rules applicable to a single List Maintenance field should be unique.

SQL

The SQL field specifies the SQL statement to capture the cases for which the derivation rule is applicable.

> **Note**
>
> The SQL statement must follow the correct syntax.
>
> The system does not validate the length of the new values against the database. Make sure that new values being inserted into the Oracle Argus Insight data mart do not exceed the limit defined in the database.

Guidelines for correct syntax:

- The SQL query configured against a rule should not contain the table name. It should contain only the primary key column name(s) of the field in the SELECT clause. For example:

  ```
  Correct: SELECT CASE_ID FROM RPT_CASE WHERE…
  Incorrect: SELECT RPT_CASE.CASE_ID FROM RPT_CASE WHERE…
  ```

- Make sure that there is only one space after the SELECT clause in the SQL query. For example:

  ```
  Correct: SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…
  Incorrect: SELECT     CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…
  ```

- Make sure that no Oracle keyword (such as DISTINCT) is used after the SELECT clause in the SQL query. For example:

  ```
  Correct: SELECT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…
  Incorrect: SELECT DISTINCT CASE_ID, SEQ_NUM FROM RPT_PRODUCT WHERE…
  ```

Configure the Oracle Argus Insight Windows Service

To configure the Oracle Argus Insight Windows service:

1. Log in to the Oracle Argus Insight Web Server.
2. Click **Start**, and select **Run**.
3. In the text box, enter `services.msc`, and click **OK**.

   The Services screen appears.
4. Right-click **Argus Insight Service**, and select **Properties**.

   The Argus Insight Service Properties dialog box appears.
5. Set the value of the **Startup type** field to **Automatic.**
6. Click **Start** to start the Oracle Argus Insight Service.
7. Click **OK** to apply the changes.

> **Note**
>
> - To change the interval of different service tasks, modify the entries in the `Service.config` file located in the Bin folder of Oracle Argus Insight. All timestamps in the `Service.config` file are specified in seconds.
> - If the Oracle Argus Insight service is installed on transaction boxes, make sure that it remains in a stopped state.
> - In a multi-web server setup, make sure that the Oracle Argus Insight service is running only on the primary web server.

IMPORTANT! Make sure that the user who runs this service has administrator privileges.

Use Export and Import to Copy Configuration Data

Before configuring export and import functions, be aware of the following:

- Before importing or exporting to or from a network drive, verify that you have mapped the network drive. This tool does not support direct access to network drives.
- Before copying Oracle Argus Safety Data, incremental ETL should be completed on Source Insight Database from Source Argus.
- It is assumed that the configuration of the instance of Oracle Argus Safety used to run Initial and Incremental ETL on the source Oracle Argus Insight data mart will also be copied and applied on the new Argus Instance which will be associated with the new Oracle Argus Insight data mart.
- Data must be imported after loading Factory Data and before running Initial ETL on destination environment.
- In a multi-tenant environment, you must make sure that all the enterprises which are part of the source Oracle Argus Insight database, have been created in the Target Oracle Argus Insight database.

For more information, see:

- Export Data
- Import Data

Export Data

1. Go to `Utilities\Copy_Config` and run the `Data_ExportConfigOnly.bat` file.

   The Export Utility command prompt screen appears.
2. Enter the following details when prompted, and press **Enter**:
   a. TNSNAMES entry of the Oracle Argus Insight Database
   b. DBA User
   c. DBA User Password
   d. Oracle Argus Mart Schema Owner Name
   e. Oracle Argus Mart Schema Owner Password
   f. DB Directory path for export dump files (database server file path)

      Enter a directory path specific to your database environment.

      The Export Dump file and Export log file will be placed here as `INSIGHT.DMP` and `Export_log.log` respectively.
   g. Directory Name (in capital letters) to be created in the database

      A database directory is created with this name at the path mentioned in the previous step.
   h. Directory including full path for log/script files (Local Machine)

      Enter a directory path specific to the machine where the Copy Configuration utility is being run.

      The user specified log file and files named `application_type_check.sql`, `insight_export_tables.par`, and `truncate_delete_tables.sql` will be generated here.
   i. Name of the log file
3. Verify that the script is successfully connected as <*DBA User Name*>@<*Oracle Argus Insight Database Name*>, and press **Enter**.

   The command prompt screen with the Encryption wallet verification status appears.
4. Verify the details mentioned on the command prompt screen, and press **Enter** if:
   - TDE is setup and Wallet is open
   - TDE is not setup and Wallet is not open

   The command prompt screen with Directory creation status appears.
5. Press **Enter** if the Directory Path is valid.
6. Verify that the script is successfully connected as <*APR_MART User Name*>@<*Oracle Argus Insight Database Name*>, and press **Enter**.

   The command prompt screen with list of parameters appears.
7. Press **Enter** to resume if the parameters are valid.

   Verify the details mentioned on the command prompt screen, and press **Enter**.
8. Enter the password for the **APR_MART** user, and press **Enter**.

   A data export completed screen appears with a list of all the output files.

9. Verify the location of files, and press **Enter** to Exit.

   Make sure to review the all the log files for information about the export and export errors.

Import Data

1. Go to `Utilities\Copy_Config` and run the `Data_ImportConfigOnly.bat` file.

   The Import Utility command prompt screen appears.
2. Press **Enter** if all prerequisites are satisfied.
3. Enter the following details when prompted, and press **Enter**:
   a. TNSNAMES entry of the Oracle Argus Insight Database
   b. DBA User
   c. DBA User Password
   d. Oracle Argus Mart Schema Owner Name
   e. Oracle Argus Mart Schema Owner Password
   f. DB Directory path for import dump files (database server file path)

      Enter a directory path specific to your database environment.

      `INSIGHT.DMP` created in the export process is copied here. Beside, `Import_log.log` is also created here.
   g. Directory Name (in capital letters) to be created in the database

      A database directory is created with this name at the path mentioned in the previous step.
   h. Directory including full path for log/script files (Local Machine)

      Enter a directory path specific to the machine where the Copy Configuration utility is being run.

      The user specified log files are generated here.

      Besides, make sure that the files named `application_type_check.sql`, `insight_export_tables.par`, and `truncate_delete_tables.sql` that were generated during export process are also copied here.
   i. Name of the log file
4. Verify that the script is successfully connected as *<DBA User Name>@<Oracle Argus Insight Database Name>*, and press **Enter**.

   The command prompt screen with the Encryption Wallet Verification status appears.
5. Verify the details mentioned on the command prompt screen, and press **Enter** if:
   - TDE is setup and Wallet is open
   - TDE is not setup and Wallet is not open

   The command prompt screen with Directory Creation status appears.
6. Press **Enter** if the Directory Path is valid.
7. Verify that the script is successfully connected as *<APR_MART User Name>@<Oracle Argus Insight Database Name>*, and press **Enter**.

   The command prompt screen with list of parameters appears.
8. Press **Enter** to resume if the parameters are valid.

Verify the details mentioned on the command prompt screen, and press **Enter**.

9. Enter the password for the **APR_MART** user, and press **Enter**.

   A data import completed screen appears.

10. Press **Enter** to Exit.

    Make sure to review the all the log files for information about the import and import errors.

Use Oracle Argus Safety to Configure Enterprises for Oracle Argus Insight (for Mutli-tenant installation only)

You must be a valid LDAP user and have access to the Oracle Argus Safety global home page.

See the Global Enterprise Management section of the *Oracle Argus Safety Installation Guide* for detailed steps on logging and accessing Oracle Argus Safety global home page.

To create an enterprise in Oracle Argus Insight:

1. Log in to the Global Enterprise Management portlet.
2. From the Enterprises folder, select an enterprise from the left pane.

   The Enterprises folder includes enterprises as per you access privileges.
3. To create the selected enterprise in Oracle Argus Insight, click **Copy Enterprise to Insight**.

   Note that the **Copy Enterprise to Insight** button is:

   - disabled if the selected enterprise already exists in Oracle Argus Insight.
   - enabled if you have Copy Configuration role in any of the listed enterprises.
4. In the **Copy Enterprise Configuration From** field, select the source enterprise from which the information will be copied.

   Note that the drop-down list includes only those enterprises that meet the following conditions:

   - The enterprise has already been created in Oracle Argus Insight.
   - You have been assigned Copy Configuration privileges for the enterprise.
5. Click **Setup**.

   The process to copy the configuration begins and a status information appears throughout the process.
6. Click **Finish**.

Secure Sensitive Configuration and Operational Data

For security reasons, you should configure permission settings for certain files and folders on the Oracle Argus Insight Web Server. The permission settings make sure that only the IIS user can access these files. Local system login accounts that are not part of the Administrators group cannot make changes to the files.

Windows Directory File

For the user under which IIS is running, the `ai.ini` file requires a permission of **Full Control**.

Shared Folders

For the user under which IIS is running, the following folders require a permission of **Full Control**:

- CacheTemp
- ScheduledReports
- PDFReports
- ASP
- Bin

9

Upgrade the Oracle Argus Safety Application

You can upgrade the Oracle Argus Safety application from the following versions:

> **Note**
>
> Before you upgrade, review the respective release notes to verify application server upgrade paths. To upgrade the application from any version prior to Argus 8.2.1, you must re-install the middle tier servers. However, no re-installation is required for database upgrade.

- 8.2.1 to 8.2.1.11
- 8.2.2 to 8.2.2.2
- 8.2.3
- 8.2.3.001
- 8.2.3.1 to 8.2.3.4
- 8.4
- 8.4.0.1 and 8.4.0.3
- 8.4.1
- 8.4.2
- 8.4.2.001
- 8.4.2.002
- 8.4.2.1
- 8.4.3
- 8.4.3.001
- 8.4.3.1 to 8.4.3.5
- 8.4.3.201 and 8.4.3.202
- 8.4.4
- 8.4.4.1 to 8.4.4.4
- 8.4.4.201 and 8.4.4.202
- 8.4.4.301

For more information, see:

- Upgrade Oracle Argus Safety Application on the Web Server
- Upgrade Oracle Argus Safety Application on the Transaction Server

Upgrade Oracle Argus Safety Application on the Web Server

1. Log in as an administrator.
2. Stop Microsoft IIS (Internet Information Server).
3. Stop the `Argusvr2.exe` and `Argusvr2a.exe` services.

   Alternatively, make sure these processes are not running.
4. Copy the build contents to your local server for upgrade, and run the <*Software Path*>`\Argus Safety\Setup.exe` utility.

   The setup auto-detects a previous compatible version of the application.
5. When a compatible version is detected, click **Next**.
6. When prompted for database name (SID), enter the database SID.

   This database name appears in the `argus.ini` file.
7. Restart the server after the upgrade process is complete.

Upgrade Oracle Argus Safety Application on the Transaction Server

1. Log in as an administrator.
2. Stop the Oracle Argus Safety and Oracle Argus Interchange services.
3. Wait for the following processes to shut down:
   - `AGProc.exe`
   - `ESMMapping.exe`
   - `E2BReceive.exe`
   - `ESMProc.exe`
4. Copy the build contents to your local server for upgrade, and run the <*Software Path*>`\Argus Safety\Setup.exe` utility.

   The setup auto-detects a previous compatible version of the application.
5. When a compatible version is detected, click **Next**.
6. When prompted for database name (SID), enter the database SID.

   This database name appears in the `argus.ini` file.
7. Restart the server after the upgrade process is complete.

10

Set Up the Client Browser

In this chapter:

Prerequisites

Oracle Argus is supported to run on the below modern browsers with the version specified in the System Requirements > Other Components as the minimum baseline version:

1. Google Chrome
2. Microsoft Edge (Chromium based)

Supported scale (zoom) is 100%.

- If scale is not set to 100% it may lead to distortion or truncation of UI display of Argus. The recommended layout (display resolution) is minimum 1280 x 1024.
- Depending on the medium of device used (monitor, laptop, etc.) the supported layout may vary. Set the resolution according to your monitor settings.

Install Supplemental Fonts to View Reports

To view reports in Adobe Reader, you must install Windows Supplemental Language Support for East Asian languages and Japanese font pack on all Web client machines as common fonts are used for Oracle Argus Safety English and Oracle Argus Safety Japanese.

To download and install these fonts, see Adobe Reader Font Pack and Spelling Dictionary.

Post Application Install or Upgrade

You must clear your local browser cache after installation or upgrade of the Oracle Argus Safety application.

11

Post-installation Tasks

This chapter provides checklists and procedures to verify that Oracle Argus Safety is installed correctly:

General Checklist

Verify that:

- the correct modules are installed as follows:
  1. Go to Add/Remove Programs and select **Argus Safety Web**.
  2. Click **Modify** and click **Next**.
  3. Verify that the applications that you have installed are checked.
- the `Argus.XML` file has the same data across all the Web Servers.
- a single domain user account <*Domain User*> is running the Oracle Argus Safety Web application on all web servers.
- the login page appears when the server name is entered in your browser.
- you can log in successfully.
- take a backup of the MessageCache\{DbName} folder and remove contents from the new MessageCache\{DbName} folder, created after the installation. The location of this folder is provided in the Argus.ini file.

Configure Argus Bridge

Use Argus Bridge to configure the Document Management System and Translation capabilities provided with Argus.

> **Note**
>
> You must configure Argus Bridge whether you are performing a fresh installation or upgrading from an existing version.

1. Generate a new key for Argus Bridge.
   a. When installation is complete, go to the server where the database tools are installed.

b. From the main menu, open the Argus Crypto tool.

c. Click **New**.

d. Click **Generate Bridge Secure Keys**.

e. Open the `ArgusSecureKey.ini` file.

f. Copy the `JwtPrivateKey=value` and `JwtPublicKey=value`, and paste in the `Argussecurekey.ini` file on all Web Servers and Transaction Servers.

   The value in this is an long encrypted string.

2. Configure the database to be used with Argus Bridge.

   - In the `ArgusSecureKey.ini` file, make sure the **DatabaseName** parameter is configured with the correct database. For details, see Configure Argus.ini File.

3. Update the new Argus Bridge details in Oracle Argus Safety Console.

   a. Log in to Oracle Argus Safety.

   b. Go to `Argus Console > System Configuration > System Management (Common Profile Switches) > Network Settings`.

   c. In the **Argus Safety API Load Balancer URL** field, enter the internal load balancer URL with port.

      If you have the Load Balancer setup, then enter the Load Balancer URL. Otherwise, enter the Argus web server URL with port `8091` (instead of 8033). By default, this field is blank.

      > **Note**
      >
      > You must configure this profile switch. If it is configured incorrectly, the bridge configuration save and the case save operations fail or show unexpected result with generic errors.

   d. Click **Save**.

      The Argus Safety API Load Balancer URL profile switch is available for the default enterprise. It is set at the global level and not specific to the enterprise.

Configure Dictionary Loader on the Web Server

1. On the server where integrations component has been installed, navigate to the Oracle Argus Safety Windows Service folder.
2. To configure Windows Service for the Dictionary Loader feature, in the `RelsysWindowsService.exe.config` file, `DatabaseConfiguration` section, edit the following attributes :

   - DBName - TNS of the database to which the RelsysWindowsService should connect to. Example: `DBName="GOLDDEMO"`
   - DBUser - AGService Username. The RelsysWindowsService logs into the database using this login name. This has to be a user of type AGSERVICE. Example: `DBUser="agservice_user1"`

3. To configure separate database tablespaces or indexes for dictionary loads, in the `Service.config` file, `DictionaryLoader` service node, edit the Metadata attribute, and add the tablespaces or indexes.

Configure Worklist Intake on the Web Server

1. Identify the physical folders where the Intake XMLs will be dropped in. There could be one folder for all the available sites, or one folder each for each site. These folders can be on the same machine, or on different machines. Create shares for the folders.
2. Log in to the Oracle Argus Safety Console and open the Sites UI under **Access Management** menu.
3. Configure the UNC paths of the identified physical folders for the required Sites.
4. On the server where Integrations component has been installed, navigate to the path where the **Argus Safety Windows Service** is running.

```
<InterfaceSchemas>
<add InputXSD="..\..\Integrations\XSD\v1.0\Base.xsd" />
<add InputXSD="..\..\Integrations\XSD\v1.0\DataOperation.xsd" />
<add InputXSD="..\..\Integrations\XSD\v1.0\Dictionary.xsd" />
<add InputXSD="..\..\Integrations\XSD\v1.0\Case_Intake.xsd"
OutputXSLT="..\..\Integrations\XSLT\v1.0\CaseIntake_Transform.xsl"/>
</InterfaceSchemas>
```

   In the above tag, mention full Oracle Argus Safety Install Path. Typically, the Oracle Argus Safety Install Path is, <*Argus Install Path*>\Argus Safety. For example:

```
<InterfaceSchemas><add InputXSD="<Argus Install Path>\Argus
Safety\Integrations\XSD\v1.0\Base.xsd" /><add InputXSD="<Argus Install Path>\Argus
Safety\Integrations\XSD\v1.0\DataOperation.xsd" /><add InputXSD="<Argus Install
Path>\Argus Safety\Integrations\XSD\v1.0\Dictionary.xsd" /><add InputXSD="<Argus
Install Path>\Argus Safety\Integrations\XSD\v1.0\Case_Intake.xsd" OutputXSLT="<Argus
Install Path>\Argus Safety\Integrations\XSLT\v1.0\CaseIntake_Transform.xsl"/></
InterfaceSchemas>
```

5. Edit the following files:

- RelsysWindowsService.exe.config
- Service.config
- Intake.config

RelsysWindowsService.exe.config

1. Uncomment the following entries under the *<RelsysConfigFilesSection>/<RelsysConfigFiles>*
   - `Relsys.InterfaceComponents.ProcessorsConfiguration`
   - `Relsys.CaseIntake.FolderConfiguration`
2. Make sure that the DatabaseConfiguration section is configured for the following attributes:

Attribute	Description
DBName (Mandatory)	TNS of the database to which the RelsysWindowsService should connect to. Example: DBName="GOLDDEMO"

Attribute	Description
DBUser	AGService Username. The RelsysWindowsService logs into the database using this login name. This has to be a user of type AGSERVICE. Example: DBUser="agservice_user1"
GeneralEmailTo	The e-mail address to which the e-mails will be sent by the Intake Service, using the General Email feature of Oracle Argus Safety. Example: GeneralEmailTo ="rrecepient@oracle.net"
GeneralEmailFrom	The email address from which the e-mails will be sent by the Intake Service, using the General Email feature of Oracle Argus Safety. Example: GeneralEmailFrom ="admin@oracle.net"
GeneralEmailCc	This email address will be added to the Cc line when e-mails are sent by the Intake Service, using the General E-mail feature of Oracle Argus Safety. Example: GeneralEmailCc ="recepient@oracle.net"
GeneralEmailBcc	The email address will be added to the Bcc line when e-mails are sent by the Intake Service, using the General E-mail feature of Oracle Argus Safety. Example: GeneralEmailBcc ="recepient@oracle.net"

Service.config

1. Uncomment the entries for "Case Intake" and "Case Intake Ack" in the <*ServiceConfiguration*>/<*ServiceComponents*> section
2. The following configuration changes are optional:
   - "Recurrence": The value for this attribute specifies the frequency of instantiation of the associated Service Component. The value is specified in seconds. For example:

     ```
     <add Name="Case Intake Ack" Assembly="CaseIntakeServiceComponent"
     Type="Relsys.CaseIntakeServiceComponent.IntakeAckGenerator" Recurrence="600"
     Metadata="InvokeDirect=true" />
     ```

     The value of 600 for Recurrence above means, the "Case Intake Ack" service is instantiated every 600 seconds (10 minutes) to perform the job.

Intake.config

The following configuration changes are optional:

```
<FolderConfiguration><MonitorFolders MonitorAllConfiguredFolders="true"><add
FolderPath="\\172.16.38.154\Intake\US" Monitor="true" AlternatePath="C:\Intake\US"/></
MonitorFolders></FolderConfiguration>
```

The FolderConfiguration enables you to have more granular control over what folders are monitored on what machines. This is particularly useful when the Intake folders are distributed across multiple machines and in many cases if these machines are not accessible from one server.

If the server machine on which Integrations component has been installed, has to monitor only a subset of the configured folders (configured in Oracle Argus Safety Console), then set the attribute MonitorAllConfiguredFolders = "false"

When the value is set to false, each folder in the subset of folders that need to be monitored should be added as shown in the example above, using multiple <add /> entries. More info on each of the attributes:

FolderPath: The configured folder path, as specified in Sites UI in Oracle Argus Safety Console

Monitor: true means this folder should be monitored, false means this folder should not be monitored.

AlternatePath: Alternate way of accessing the same folder path.

Verify and Update Network Proxy Settings

1. Verify the value of PROXY_AUTO_DETECT:
   a. Log into SQL session on the database <*database_name*> and set up the enterprise context.
   b. To verify that the value of PROXY_AUTO_DETECT, execute:

      ```
      select value from CMN_PROFILE_GLOBAL where key = 'PROXY_AUTO_DETECT'
      ```

      If this value is set to a character value, True or False, then update this value to a numeric value, 1 or 0.
2. To update the Network Proxy settings:
   a. Log in to Oracle Argus Safety Console.
   b. From the **System Configuration** menu, select **System Management**.
   c. Expand the **Network Settings** folder and click **Proxy** folder.
   d. Check or uncheck the **Auto Detect Proxy?**, click **Save**.
   e. Verify the Network Proxy settings again as mentioned in step 1. The value should be set to 1 or 0.

Verify Files Installed on Middle Tier Servers

Verify the files installed on the server have not been modified or deleted from original installation.

1. Log in to the server as an Admin user.
2. Select **Start** > **Control Panel**.
3. Click **Programs and Features**.
4. Hover **Argus Suite** and right-click.
5. From the drop-down menu, click **Change**.

   The Preparing Setup dialog box appears.
6. Click **Modify** and click **Next**.
7. Select **Verify the current installation** and click **Next**.
8. In the File Verification dialog box, click **Next**.

12

Other Tasks

In this chapter:

Configure Argus.xml File

The `Argus.xml` file is generated during installation on the Oracle Argus Safety Web. You can update the database entry in this file after installation is complete. The file resides in the following directory:

<Argus Install Path>`/ArgusWeb/ASP`

The `Argus.xml` file contains the following type of xml tags:

XML Tag	Description
<ARGUS_DB>	Contains database details supported by the Oracle Argus Safety Web application. Each database is specified as a separate XML tag - *<DBNAME>* with *<ARGUS_DB>* as parent tag. For example, for a database that is recognized as "Testing Database" in the Oracle Argus Safety Web Login screen and whose alias in the Oracle `TNSNAMES.ORA` file is "TESTDB", the entry will be *<DBNAME id="TESTDB">*`Testing Database`*</DBNAME>*.

> **Note**
>
> Each web server must be configured with a single database.

If you update the `Argus.xml` file, you must restart the Internet Information Services (IIS) on the server for the changes to take effect.

Configure Argus.ini File

The `Argus.ini` file is generated during installation on Oracle Argus Safety Web and Transaction (AG) Server, but the user can update this file after installation.

To configure `Argus.ini`:

1. Select **Start** > **Run**.

2. In the Open field, enter `argus.ini,` and click **OK**.
3. Set the entries in the file as described in the Argus.ini Parameters.
4. Save the file.
5. Restart the Internet Information Services (IIS) on the server to reflect the changes.

For more information, see:

- Argus.ini Parameters

Argus.ini Parameters

With some exceptions, the parameters listed in the table are used by Oracle Argus Safety Web as well asOracle Argus Safety Service (AG Service or Transaction Server).

Parameters specific to the Web Server are:

- `MessageCachePath`
- `Upload`
- `Template`
- `ArgusInstallPath`
- `Pooling parameters`

The `Argus.ini` File Parameters are described in the following table:

Section	Parameter	Sample Value	Description
Workstation	`ArgusInstallPath`	`C:\Program Files\Oracle\ArgusWeb\ASP\`	Path of the location where the ASP files are placed. For use with Web Server.
Workstation	`ArgusLogPath*`	`C:\Temp\ArgusLogs\`	Path of the root folder for ArgusLogs.
Workstation	`Cache*`	`C:\ArgusReports\PDF Reports\`	Path for PDF Reports (Expedited/Periodic/Screen Prints etc.). In case of multiple Web Servers, this is a shared path on the network.
Workstation	`MessageCachePath*`	`C:\ArgusReports\MessageCache\`	Shared path to save the system level cache such as data for LM tables, CMN Fields, etc. In case of multiple Web Servers, this is a shared path on the network. For use with Web Server.
Workstation	`Upload*`	`C:\ArgusReports\UploadedLetters\`	Shared path for uploaded letters. In case of multiple Web Servers, this is a shared path on the network. For use with Web Server.

Section	Parameter	Sample Value	Description
Workstation	`Template`	`C:\Program Files\Oracle\E2BViewer\Templates\`	Location that stores the template and report files used to display CIOMS and MedWatch views. For use with Web Server.
Workstation	`DatabaseName`	*AS2026101UDB*	Defines the database SID through which the Web or Transaction server connects.
Argus Server	`SQLTimes`	1	Enables the Argus Web application to start creating log files for all the SQLs that are fired. These log files are created in `C:\Temp\ArgusLogs\Debug` folder and can be used for debugging. **Note:** Even though you can changes the log file path in the Argus.ini file, but the system overwrites the path to default as mentioned above.
Argus Server	`PDFTimes`	1	Enables the Argus Web application to start creating log files for all the PDFs that are generated. These log files are created in `C:\Temp\ArgusLogs\PDF_Debug` folder and can be used for debugging.
Argus Server	`PDFTimesUser`	*argus user id*	Argus user ID for which the PDFTimes log files will be created.
Argus Server	`Pool_Initial_Size`	3	Refers to the DB Connection Pool Initial Size. For use with Web Server.
Argus Server	`Pool_Maximum_Size`	120	Refers to the DB Connection Pool Maximum Size. For use with Web Server.
Argus Server	`Connection_Wait_Time`	3	Refers to the connection wait time in seconds. An exception occurs if the system cannot obtain a DB connection in the given time. For use with Web Server.

Note

* If any anti-virus software is running on Oracle Argus Safety Web or Transaction (AG) server(s), it must be configured not to scan these Oracle Argus Safety temp folders. Otherwise, it can lead to slower performance or unexpected errors on screens under heavy user load due to file locks by the anti-virus software.

Installation Maintenance Tasks

You may need to perform certain installation maintenance tasks on the installed Oracle Argus Safety Suite Solution Components.

For more information, see:

- Install New Components
- Uninstall Components
- Remove All Components

Install New Components

1. Select **Start** > **Control Panel**.
2. Click **Add or Remove Programs/Uninstall** or change a program.
3. Right-click Argus Suite and from the drop-down menu, click **Change**.

   The Argus Suite Solutions InstallShield Wizard opens the Preparing Setup dialog box.
4. Select **Modify** and click **Next**.
5. Select **Update installed Argus Components** and click **Next**.
6. In the Select Features dialog box, check the components to install and click **Next**.

> **Note**
>
> Make sure the checkboxes for components that are already installed contain a checkmark. If the checkmark is cleared from the checkbox for an existing component, the component will be uninstalled.
>
> Refer to the relevant chapters in this Installation Guide for instructions for installing individual components.

7. When the installation process is complete, the Argus Suite Setup- Maintenance Complete dialog appears.
8. Click **Finish**.

Uninstall Components

1. Select **Start** > **Control Panel**.
2. Click **Add or Remove Programs**.
3. Right-click **Argus Suite** and from the drop-down menu, click **Change/Remove**.

   The Argus Suite Solutions InstallShield Wizard opens the Preparing Setup dialog box.
4. Select **Modify** and click **Next**.
5. In the Select Features dialog box, uncheck the components to uninstall and click **Next**.

   The Oracle Argus Safety Components Installer will uninstall the selected components.
6. Follow the on-screen instructions to uninstall the components.

Remove All Components

1. Select **Start** > **Control Panel**.
2. Click **Add or Remove Programs**.
3. Right-click **Argus Suite** and from the drop-down menu, click **Change/Remove**.

   The Argus Suite Solutions InstallShield Wizard opens the Preparing Setup dialog box.
4. Select **Remove** and click **Next**.
5. In the Confirm Uninstall dialog box, click **OK**.

   The Oracle Argus Safety Components Installer uninstalls the required component(s).
6. Follow the on-screen instructions to uninstall the components.

Oracle Argus Safety Configuration Files

By default, the Oracle Argus Safety logs files are placed in the “C:\temp" folder (default temp directory of Oracle Argus Safety). You must make sure that the user under which the Oracle Argus Safety applications are running has access to this directory.

If you have a different “Temp" directory, change the temp directory path in the following files:

Background Processes (AG Server)

1. *Argus Install Path*/Argus Safety/AGProc.config
2. *Argus Install Path*/Argus Safety/Service.config
3. *Argus Install Path*/Argus Safety/RelsysWindowsService.exe.config

Argus Web Server:

1. *Argus Install Path*/ArgusWeb/ASP/Web.config
2. *Argus Install Path*/ArgusWeb/Bin/Argussvr2.config
3. *Argus Install Path*/ArgusWeb/ASP/Argus.Net/Web.config
4. *Argus Install Path*/ArgusWeb/ASP/Argus.Net/Bin/RelsysWindowsService.exe.config
5. *Argus Install Path*/ArgusWeb/ASP/ Argus.Net/Bin /Service.config
6. *Argus Install Path*/ArgusWeb/ASP/Integrations/Web.config

> **Note**
>
> It is recommended that you use the local server path rather than the network share path.

- Backup Configuration Files

Backup Configuration Files

You must back up the following configuration files before proceeding with the application upgrade. All system configuration (.config) files will be overwritten by this upgrade and your

manual configuration changes will be lost. These files may be stored on multiple servers, depending on components selected at the time of the Oracle Argus Safety installation (Web Server, integration server, transaction server, and so on). The directory structure of the file, however, remains constant.

Commonly modified configuration files are:

```
.\ArgusWeb\ASP\Argus.NET\bin\Intake.config

.\ArgusWeb\ASP\Argus.NET\bin\RelsysWindowsService.exe.config

.\ArgusWeb\ASP\Argus.NET\bin\Service.config

.\ArgusWeb\ASP\Argus.NET\web.config

.\ArgusWeb\ASP\ArgusConsole\web.config

.\ArgusWeb\ASP\Integrations\Service.config

.\ArgusWeb\ASP\Integrations\Web.config

.\ArgusWeb\ASP\web.config

.\ArgusWeb\Bin\Argusvr2.config

.\ArgusWeb\Bin\Argusvr2a.config

.\Argus Safety\AGProc.config

.\Argus Safety\Intake.config

.\Argus Safety\RelsysWindowsService.exe.config

.\ArgusSafety\Service.config

.\DBInstaller\ArgusDBInstall.exe.config

.\ESMMapping\ESMapping.exe.config
```

Part III

Install or Upgrade Oracle Argus Safety Database Tier

You may install or upgrade Oracle Argus Safety and Oracle Argus Insight database, and upload dictionaries.

> **Note**
>
> To upload dictionaries, refer to the *Oracle Argus Safety Administrator's Guide*.

In this section:

13

Install Oracle Argus Safety Database

In this chapter:

Create Oracle Argus Safety Database Schema

1. For Windows—To use the interactive user interface, execute the `dbinstallerUI.bat` file.

   For silent installation—execute the `dbinstaller.bat` file.

2. Create the tablespaces and schemas using the `dbinstallerUI.bat` or `dbinstaller.bat` file available at *`Argus Release Media`*`\Database\Argus Safety`.

   - Oracle Argus Safety database schema:
     - ArgusUser
     - Argus Login Schema
     - Argus Bridge Schema
     - Interchange Service Schema
     - ESM Query Schema
     - DLP Schema
     - DLP ESM Query Schema

> **Note**
>
> The mapping SQLs for ESM Generation and Import can be executed only through restricted database user account that have access only to Oracle Argus Safety and ESM Schema (ESM Query Schema and DLP ESM Query Schema).
>
> These DB users does not have access to create or execute anything that would result in change or alteration of the schema or database.
>
> DLP Schema and DLP ESM Query Schema are part of Oracle Argus Safety Database, but DLP setup can be enabled or disabled by executing separate batch files shipped with the software.
>
> Besides, features like Factory Data, DB Upgrade, and Oracle Text are merged with the Create Schema option.

> **Note**
>
> These schema other than the Argus Bridge schema are disabled for upgrade.

- Oracle Analytics Publisher Schema—This schema holds the Flexible Aggregate Reporting (FAR) objects and the Japanese PMDA R3 Paper Reports related objects. This schema must always be created.

> **Note**
>
> When creating new users in Oracle, the password can only contain any ASCII Character, 0-9, or any of the following special characters _ # $.

3. Create Axway B2Bi or Oracle B2B Database Instance (Optional)—Required only for respective gateway being integrated with Oracle Argus Safety.

For more information, see:

- Prepare to execute the DBInstaller
- Run Create DBA User Script
- Create Tablespaces (Optional)
- Prerequisites to Create the Schema
- Configure the Database Setup Properties File
- Create the Schema on Windows from the User Interface
- Create the Schema on Windows from a Batch file
- Create the Schema on Linux or Unix

Prepare to execute the DBInstaller

In this section:

- Prerequisites
- Install Java

Prerequisites

Before you execute the `dbinstallerUI.bat` or `dbinstaller.bat` file on a server, verify that:

- an Oracle client with Administrator option is installed on the server.
- database TNS entry should be added in the `TNSNAMES.ora` file.
- Java JRE 1.8 or higher must be installed and Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 8 is applied.
- login machine user should have administrative privileges.

Install Java

1. Download the `jce_policy-8.zip` file on your local machine from the following link:

   `http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html`
2. Unzip the `jce_policy-8.zip`.
3. Replace `local_policy.jar` and `US_export_policy.jar` files present in all Java JRE installation security folders with local_policy.jar and US_export_policy.jar shipped in `jce_policy-8.zip`.

   For example, the location of Java JRE 64-bit:

   `C:\Program Files\Java\jre1.8.0_161\lib\security`
4. From the command prompt verify that Java is properly installed by executing: `java-version`

   If no Java version appears, check that the environment variable settings and the path system variables have correct the Java installation path.

Set Java Install Path

1. Right-click the My Computer (or Computer) icon and from the drop-down menu select **Properties**.
2. From the left-pane, select **Advanced system settings**.

   The System Properties dialog box appears.
3. In the Advanced tab > Startup and Recovery section, click **Environment Variables...**
4. From the System variables section, scroll down to the **Path** variable and double-click.

   The Edit System Variable dialog box appears.
5. In the **Variable value:** field, enter the location where Java will be installed and end it with a semi-colon (;).
6. Click **OK** to close the Edit System Variable dialog box.
7. Click **OK** to close the System Properties dialog box.

Install XDB Schema for Oracle Argus Interchange

Oracle Schema XDB must be present for Oracle Argus Interchange packages to load. To create the XDB schema, if already not present:

1. Click `sqlplus.exe`.
2. Connect to **sys** as **sysdba**.
3. Execute the *`Oracle_Home`*/rdbms/admin/catqm.sql script.
4. Enter the following parameters:
   - `user password`
   - `user default tablespace`
   - `user temporary tablespace`

   For example: `SQL>@?/rdbms/admin/catqm.sql SYSTEM SYSAUX TEMP`

Run Create DBA User Script

You must run the Create DBA User scripts to create a new DBA user or grant required privileges to the existing DBA or SYSTEM user. Use this new DBA user account when running the **DBInstaller** to create the Argus Safety schema.

The DBA user created by this script can perform the actions as done by the SYSTEM user. All the manual grants which used to be assigned to the SYSTEM user (prior to the Argus Safety 8.1 release), are now part of this script. The term SYSTEM mentioned in this chapter can be replaced with the new DBA user. If you use the newly created DBA User to execute the **DBInstaller**, then the validation file might display extra or missing privileges for the SYSTEM or the newly created DBA user.If you do not wish to create a new DBA user, you may enter SYSTEM when running the script.

To create the DBA user:

1. From the command prompt, run the batch file <*`Argus Release Media`*>`\Database\Argus Safety\Utilities\Create_Dba_User\create_dba_user.bat`.

   A prompt appears as `Do you want to use SYSDBA to run the script? (Y/N):`. Enter **Y** to run as SYSDBA.
2. Enter the following parameters:
   a. TNSName of the database
   b. SYSDBA username
   c. Password for SYSDBA account
   d. Name for the new DBA User account that will be created
   e. Password for the new account
3. Follow the remaining steps to complete the script.
4. You may also run the script:
   - For Windows—execute the script from <*`Argus Release Media`*>`\Database\Argus Safety\Utilities\Create_Dba_User\create_dba_user.bat`

- For Linux—execute the script from <*Argus Release Media*>/Database/Argus Safety/Utilities/Create_Dba_User/create_dba_user

Create Tablespaces (Optional)

The **DBInstaller** creates the tablespaces if they do not exist with default parameter settings.

You can create tablespaces as per your parameter requirements before installing Oracle Argus Safety. The following is the list of tablespaces that is required for the Oracle Argus Safety installation:

Tablespaces for Oracle Argus Safety	Tablespaces for DLP
ARGUS_AEXP_DATA_01	DLP_DATA_01
ARGUS_AEXP_INDEX_01	DLP_DATA_02
ARGUS_AL_DATA_01	DLP_DATA_03
ARGUS_AL_INDEX_01	DLP_DATA_04
ARGUS_DATA_01	DLP_DATA_05
ARGUS_DATA_02	DLP_DATA_06
ARGUS_DATA_03	DLP_INDEX_01
ARGUS_DATA_04	DLP_INDEX_02
ARGUS_DATA_05	DLP_INDEX_03
ARGUS_INDEX_01	DLP_INDEX_04
ARGUS_INDEX_02	DLP_INDEX_05
ARGUS_INDEX_03	DLP_INDEX_06
ARGUS_INDEX_04	DLP_LOB_01
ARGUS_INDEX_05	--
ARGUS_INDEX_06	--
ESM_DATA_01	--
ESM_INDEX_01	--

Prerequisites to Create the Schema

- Create the Cryptographic Key, refer to the chapter Oracle Argus Safety Password Management—Cryptography Tool.
- A blank Oracle database instance is available.
- A DBA-privileged or a SYSTEM user account is available.
- The Oracle database is available from the machine where the DBInstaller is installed.
- Java is installed and JCE policy is applied. See Install Java.

Set database semantics to CHAR.

The Argus Safety Database requires the database semantics to be CHAR and not BYTE. Follow the steps below:

1. Log in to the database as the SYS user.
2. Execute: ALTER SYSTEM SET NLS_LENGTH_SEMANTICS=CHAR SCOPE=BOTH;
3. Shutdown and startup the database after applying the above statement.

Configure the Database Setup Properties File

Make sure the `dbinstaller.properties` file that contains the information for the Oracle Argus Safety Database setup has correct data. If not, edit the file.

The file is located on the database server at *`Argus Release Media`*`\Database\Argus Safety`.

> **Note**
>
> In case you are creating the schema on windows from the User Interface, you MUST update only the following parameter:
>
> - argus_securekey_path=*`path of the ArgusSecureKey.ini file`*
>
> The default value is C:/windows
> - tablespace_encryption=*blank* or *text*, where
>
> - blank = no encryption
>
> - text like: encryption using 'AES256' default storage (encrypt)
>
> You may ignore other parameters.

- #DB Connection Details
  - db_connect_string= *`host name`*`:`*`port/service name`*
  - dba_user=*`argus dba user or system user`*
- #Application Type
  - application_type=MULTI (for a multi-tenant setup) or SINGLE (for a single-tenant setup)
  - enterprise_name=DEFAULT
  - enterprise_short_name=DEFAULT
- #Complete path of Argus Secure Key ini file
  - argus_securekey_path=path of the `ArgusSecureKey.ini` file

    The default value is C:/windows
  - url—URL for the database connection
  - dbaUser—SYSTEM or DBA privileged user
- #Argus DB Schemas—Schema Name and Password (optional). If the password is left blank, it will be prompted at run-time.
  - To prompt for each password on the screen:
    * appSchema_argus_schema=argus_app
    * appSchema_argususer=argususer
    * appSchema_argus_login=argus_login
    * appSchema_vpd_schema=vpd_owner
    * appSchema_bip_schema=bip_app

        * appSchema_esm_login=esm_login
        * appSchema_esm_schema=esm_owner
        * appSchema_esmquery_schema=esm_query
        * appSchema_dlp_schema=dlp_owner
        * appSchema_dlp_esmquery_schema=dlp_esm_query
        * appschema_bridge_schema=argus_bridge
    - To avoid prompt for each password on the screen, set up the password as the login password for each user:
        * appSchema_argus_schema= `argus_app/`*`password`*
        * appSchema_argususer= `argususer/`*`password`*
        * appSchema_argus_login= `argus_login/`*`password`*
        * appSchema_vpd_schema= `argus_vpd/`*`password`*
        * appSchema_bip_schema= `bip_owner/`*`password`*
        * appSchema_esm_login= `esm_login/`*`password`*
        * appSchema_esm_schema= `esm_owner/`*`password`*
        * appSchema_esmquery_schema= `esm_query/`*`password`*
        * appSchema_dlp_schema= `dlp_owner/`*`password`*
        * appSchema_dlp_esmquery_schema= `dlp_esm_query/`*`password`*
        * appschema_bridge_schema=`argus_bridge/`*`password`*
- #Argus DB Roles—Enter the names of the database roles you need to be required. If this is an upgrade, list the roles under **For upgrade**. If this is a fresh installation, enter the roles under **For the new setup** in the file.
- #Argus Data Tablespaces—Define the tablespace and datafile details.

  Similarly ESM and DLP sections Define Data and Index datafiles.
- #Default and Temporary table spaces
    - default_ts=USERS
    - temp_ts=TEMP
- #TableSpace parameters
    - tablespace_encryption=*blank* or *text*, where

      - blank = no encryption

      - text like: encryption using 'AES256' default storage (encrypt)
    - tablespace_initial_size=10M
    - tablespace_autoextend=ON
    - tablespace_next_size=10M
    - tablespace_block_size=8K
- #Logging level parameters
    - log_level=info

      Logs the entire history of changes applied to the database. This is the default value.

  - log_level=debug

    Logs the entire history of changes applied to the database along with additional debug information.

- #Disable Hub API—Executes SQLLDR based on the operating system.
  Set liquibase.hub.mode=off

  Default value is N, that is, the DBInstaller is expected to run on Windows, and isLinux=N.

  To execute the DBInsatller on Argus Bridge on Linux, set this parameter to Y and isLinux=Y.

Create the Schema on Windows from the User Interface

1. Run the `dbinstallerUI.bat` file to invoke the user interface. You must run the file as an administrator.

   The Database Installer dialog box appears.

2. Enter the parameters and click **Next Step**.

   Argus Safety - Database Setup screen appears.

3. Enter the parameters, select the Application Type, and click **Next**.
   - Single Tenant—Select this option to allow the database to support only single tenant. The options to create multiple tenants in the safety system is disabled.
   - Multi-Tenant—Select this option to allow the database to support multiple tenants. Users are able to create multiple tenants using the Global Enterprise setup screens.
4. Create new tablespaces or use the existing tablespaces.
   - Under Complete Path and Data File Name, enter the database server path (complete path including the filename) where the data file is placed.

     Instead of entering path for each tablespace, you can set up a common folder path. To do so, in the text box, enter the datafile folder path, and click **Set Datafile Folder**.

- If the data file does not exist, the system creates a data file.
- If the data file exists, to use the current data file, click **Yes** in the confirmation dialog box.

> **Note**
>
> When you have existing tablespaces, you may use them; you are not required to create new ones. The system will not regenerate the tablespaces.

- Click **Next**.

5. Verify the **Setup Parameters** and click **Execute**.

   When execution is complete, a message appears in the Execution Log on screen 3 - `Liquibase Update Successful`.

6. To view the execution status or errors, open the schema creation log file with the latest timestamp from *`Argus Release Media`*`\Database\Argus Safety\logs`.

Create the Schema on Windows from a Batch file

1. Make sure the `dbinstaller.properties` are set up correctly. (See Configure the Database Setup Properties File.)
2. From Start menu, select **Run**, type `cmd`, and click **OK**.
3. In the command prompt, go to the following path:

   `cd` *`Argus Release Media`*`\Database\Argus Safety`

4. Type `dbinstaller.bat` and press **Enter**.
5. Monitor the execution log and progress on the running window.
6. To view the log file, go to *`Argus Release Media`*`\Database\Argus Safety\logs`.

Create the Schema on Linux or Unix

1. Make sure the `dbinstaller.properties` are set up correctly.

   (See, Configure the Database Setup Properties File.)

2. Copy the *`Argus Release Media`*`\Database\Argus Safety` folder in the Linux directory.

   You must have privileges to execute and create files in this directory and /tmp directory.

3. Open a terminal, log in as the Oracle Argus Safety DBA user, and execute the following command:

   `cd <`*`Argus Release Media`*`>/Database/Argus Safety`

4. Type `dbinstaller` and press **Enter**.
5. Type the DBA user password and press **Enter**.
6. View logs in *`Argus Release Media`*`/Database/Argus Safety/logs`.

Post Fresh Install Steps

1. Log in to ARGUS_APP schema.

2. Verify that the common profile switch DATABASE_TIMEZONE is not empty by executing the following script:

```
select key, value from cmn_profile where key = 'DATABASE_TIMEZONE';
```

Validate Oracle Argus Safety Database

You must validate the database after installation.

For more information on this, see:

- Validate Oracle Argus Safety Database on Windows
- Validate Oracle Argus Safety Database on Linux or Unix

Validate Oracle Argus Safety Database on Windows

1. From Start menu, select **Run**, type `cmd`, and click **OK**.
2. In the command prompt, go to the following location:

   `Argus Release Media``\Database\Argus Safety\SchemaValidation`
3. Type `SchemaValidation.bat` and press **Enter**.
4. Enter the following parameters:
   a. TNSNAMES entry to connect to the Argus database: *ASDB*
   b. DBA username in the Argus database: *argus_dba*
   c. Password for the DBA user
   d. Validation CTL file [Default `VLDN_845.CTL`]
   e. Schema difference log file [Default `SV_Schema_Diffs_asdb.log`]
   f. CTL loader log file [Default `SV_CTLFile_asdb.log`]
5. Check the log file for errors.

> **Note**
>
> If you are creating a fresh Argus Safety database, be sure the factory data is loaded before running the Schema Validation tool.

Validate Oracle Argus Safety Database on Linux or Unix

1. Copy the *`Argus Release Media`*`\Database\Argus Safety` folder in your Linux or Unix directory.

   You must have privileges to execute and create files in this directory and /tmp directory.
2. Open a Linux or Unix terminal, and execute the following command:

   `cd` *`Argus Release Media`*`/Database/Argus Safety`
3. Type `SchemaValidation` and press **Enter**.
4. Type the DBA user password and press **Enter**.
5. View logs in *`Argus Release Media`*`/Database/Argus Safety/logs`.

Enable and Disable Data Lock Point (DLP)

DLP allows a periodic report to use case data as it looked as of a certain date in the past. DLP is a specific type of *point-in-time query* which runs against the Argus History schema in the Oracle Argus Safety database. Argus History, once it is enabled at the system level, records all revisions of all cases, allowing point-in-time queries such as DLP to retrieve case data as it was captured at a previous date.

For more information, see:

Prerequisites

Before enabling or disabling DLP, make sure that:

- no one is logged on to the Oracle Argus Safety database before beginning the enable or disable DLP procedure.
- an Oracle Argus Safety database instance is available.
- a DBA-privileged user or a SYSTEM user account is available.
- the `dlpsetup.properties` file is correctly updated.

Enable DLP

- For Windows, execute the `enableDLP.bat` file from *`Argus Release Media`*`\Database\Argus Safety\Utilities\DLP_Setup`.
- For Linux or Unix, execute the **enableDLP** shell script.

Disable DLP

- For Windows, execute the `disableDLP.bat` file from *`Argus Release Media`*`\Database\Argus Safety\Utilities\DLP_Setup`.
- For Linux or Unix, execute the **disableDLP** shell script.

> **Note**
>
> Oracle Argus Safety Case Save will not function in case any DLP trigger (s) starting with T_DLP_CASE exists in Oracle Argus Safety application schema. This fail safe is to prevent any case data corruption in DLP Schema, in case any trigger is disabled.
>
> - To check if DLP trigger is disabled, use the following SQL from Oracle Argus Safety Application Login:
>
>   ```
>   SELECT trigger_name FROM user_triggers WHERE trigger_name LIKE 'T_DLP_CASE%'
>   AND status='DISABLED';
>   ```
>
> - If all the triggers are enabled, check the value of CMN Profile Global Switch DLP_TRIGGER_ENABLED and update the value if it is 0:
>
>   ```
>   SELECT key,value FROM cmn_profile_global WHERE key ='DLP_TRIGGER_ENABLED' ;
>
>   UPDATE cmn_profile_global SET value = 1 WHERE key ='DLP_TRIGGER_ENABLED' AND
>   value != 1;
>   COMMIT;
>   ```

Enable DLP on a Specific Enterprise

You can enable DLP for:

- a specific enterprise merged from a non-DLP system to a DLP enabled multi-tenant Oracle Argus Safety system.
- delta cases merged into an existing enterprise of a DLP enabled multi-tenant or single-tenant Oracle Argus Safety system.

For more information, see:

- Set Up the Base Database
- Enable DLP on Specific Enterprise or Delta Cases
- Validate the Schema

Set Up the Base Database

1. Set up an Oracle Argus Safety multi-tenant or single-tenant database for this release.

   Enable DLP on the Oracle Argus Safety database for this release, by executing the `enableDLP.bat` file. This sets up the initial DLP infrastructure on the Oracle Argus Safety database for all existing enterprises.

2. Validate the schema by executing the `SchemaValidation.bat` file. Use the compatible CTL file.

   If any MISSING object exists in schema validation log, fix it before proceeding to the next step.

3. Populate new Oracle Argus Safety cases into the existing enterprise of a DLP enabled multi-tenant or single-tenant Oracle Argus Safety system from a non-DLP system.

   Or, create new enterprise in a DLP enabled multi-tenant Oracle Argus Safety system using data migration or merge to multi-tenant utility.

Enable DLP on Specific Enterprise or Delta Cases

To enable DLP on a specific enterprise or delta cases in a specific enterprise, make sure that you use the correct login credentials and set up the appropriate enterprise context.

1. Extract the custom DLP Enable Enterprise Specific script from the following location into a machine's local folder where Oracle Argus Safety for this release is installed:

   Argus Release Media\Database\Argus Safety\Utilities\DLP_Enable_Enterprise_Specific

2. Double-click **DLP_Enable_Enterprise.bat** from:

   Argus Release Media\Database\Argus Safety\Utilities\DLP_Enable_Enterprise_Specific\Argus\DLP\

   This batch file execution handles the following scenarios to populate DLP data on newly created Oracle Argus Safety cases:

   - process all cases merged in Oracle Argus Safety system due to creation of new enterprise by merge process
   - process of delta cases merged in an enterprise due to any migration activity

3. Enter a name and location for the log file.

   For example, DLP_Enable_Enterpirse_Specific.log

4. Enter values at the prompts.

   A confirmation message appears.

5. Press **Enter**.

   The values you entered are displayed.

6. Verify that the details entered are correct and press **Enter**.

7. Check the log file for errors. If there are errors, the execution process pauses. Fix the errors and continue the process from another SQL window.

8. Check the log file to see if there are any Oracle Argus Safety cases missing in DLP.

   Argus Release Media\Database\Argus Safety\Utilities\DLP_Enable_Enterprise_Specific\Argus\DLP\DLP_ENABLE_Missing_Cases_in_DLP_log.log

Validate the Schema

After enabling DLP Enterprise Specific to this release, validate the schema by double-click on the SchemaValidation.bat file located in the *Argus Release Media*\Database\Argus Safety\SchemaValidation folder.

Extra objects related to table DLP_ENABLE_CASE_HISTORY are ignored in schema validation log file.

The following table and related objects are ignored in Schema Validation if Oracle Argus Safety DLP Enabled system with DLP_Enable_Enterprise_Specific scripts is applied for this release:

- Owner—DLP
- Table—DLP_ENABLE_CASE_HISTORY
- Index—PK_DLP_ENABLE_CASE_HISTORY

- Reason for extra object—Objects are part of Enable DLP Enterprise Specific implementation.

Copy Configuration Data (Optional)

The Copy Configuration Tool allows you to copy configuration data from one Oracle Argus Safety database to another.

For more information, see:

- Set Up the Copy Configuration Tool
- Use the Copy Configuration Tool

Set Up the Copy Configuration Tool

1. The Copy Configuration Tool creates a database directory in order to execute. Make sure to create a physical directory on the database server where export and import dump files are created and copied respectively. The physical path of these directories is required while performing the export and import.
2. Validate Schema on the source database using `SchemaValidation.bat` file.

   Make sure that there are no extra or missing objects exist in Schema Validation log file. Messages for extra custom objects created should be ignored.
3. Copy the **Copy Configuration Tool** utility files recursively from *`Argus Release Media`*`\Database\Argus Safety\Utilities\Copy_Config` to the `C:\CONFIG_EXP_IMP` folder.

Use the Copy Configuration Tool

1. Export the source database by running the batch file and following the prompts:

   `C:\CONFIG_EXP_IMP\Data_ExportConfigOnly.bat`
2. Copy `ArgusSecureKey.ini` (working with source database) from the .\Windows folder, and save it with generated source database file.

   In case you do not have `ArgusSecureKey.ini`, follow the steps listed in the Reset the Environment if ArgusSecureKey.ini is Lost.
3. Move the dump files generated on the source Database Server (physical path provided while performing the export) to the target Database Server (physical path where import will be done).
4. To perform the import on the client machine, in the **Directory Path on DB Server where dump files are placed for import** parameter, use the same folder as entered in the **DB Directory Path for export dump files** while executing the export process for logs.

   Or move the contents of the export logs folder provided to the **Directory including full path for log/script files** parameter while executing the export process, in the folder being used for the import process for log generation.
5. Create a new database (with or without TDE enabled) using the `dbinstallerUI.bat` or `dbinstaller.bat` file.
6. Import into the target database by running the batch file, and follow the prompts:

   `C:\CONFIG_EXP_IMP\Data_ImportConfigOnly.bat`

   Ignore any "ORA-28101: policy already exists" errors.

7. Validate Schema on the target database executing the `SchemaValidation.bat` file.
8. Copy `ArgusSecureKey.ini` from the source database folder and paste it in the .\Windows folder of application server(s) which are intended to be used with the target database.

Create Oracle Argus Safety Read-only Database Account (Optional)

1. From the command prompt, run the batch file: *`Argus Release Media`*`\Database\Argus Safety\Utilities\Create_Readonly_User`
2. Enter the following parameters and follow the instructions provided in the script.
   a. TNS name of Oracle Argus Safety database.
   b. DBA user in the above specified database.
   c. Password of the DBA user.
   d. New read-only user to be created.
   e. Password for the read-only user.
   f. New read-only role to be created.

> **Note**
>
> This is not a requirement to install and run Oracle Argus Safety. This is an optional script that can be used to create the read-only account for any external interface you may have that needs read-only access to the data.

Create Oracle Argus Safety ETL Dashboard Infra (Optional)

1. From the command prompt, run the batch file: *`Argus Release Media`*`\Database\Argus Safety\Utilities\Create_ETL_dashboard_infra`
2. Enter the following parameters and follow the instructions provided in the script.
   a. Name of the Oracle Argus Safety instance.
   b. Name of the Oracle Argus Safety Application user.
   c. Password of the Oracle Argus Safety Application user.
   d. Do you want to configure ETL Dashboard for Oracle Argus Insight (Y/N).

> **Note**
>
> If you enter N, skip the following Oracle Argus Insight parameters.

   e. Name of the Oracle Argus Insight instance.
   f. Name of the Argus Insight Mart user.
   g. Password of the Insight Mart user.
   h. Do you want to configure ETL Dashboard for Oracle Argus Mart (Y/N).

> **Note**
>
> If you enter N, skip the following Oracle Argus Mart parameters.

i. Name of the Oracle Argus Mart instance.
j. Name of the Oracle Argus Mart user.
k. Password of the Oracle Argus Mart user.
l. Name of the Oracle Argus Mart ODI Repository instance.
m. Name of the Oracle Argus Mart ODI repo user.
n. Password of the Oracle Argus Mart ODI repo user.
o. Name of the Oracle Argus Mart ODI DBA user.
p. Password of the Oracle Argus Mart ODI DBA user.
q. Do you want to configure ETL Dashboard for Oracle Argus Analytics (Y/N).

> **Note**
>
> If you enter N, skip the following Oracle Argus Analytics parameters.

r. Name of the Oracle Argus Analytics ODI Repository instance.
s. Name of the Oracle Argus Analytics ODI repo user.
t. Password of the Oracle Argus Analytics ODI repo user.
u. Name of the Oracle Argus Analytics ODI DBA user.
v. Password of the Oracle Argus Analytics ODI DBA user.

Enable ETL Notification via Email (Optional)

> **Note**
>
> The ETL Dashboard utility must be configured to enable ETL status notifications.

To enable the ETL status notification via email, configure the following parameters:

Argus Mart ETL

1. Go to `Argus Console > System Management (Common Profile Switches) > Argus Mart`.
2. Set **Enable ETL Notification via Email** to **Yes**.
3. In **ETL Notification Receivers**, enter at least one valid email address.
4. In **ETL Notification Sender**, enter the sender email address.

> **Note**
>
> The ETL Notification Sender parameter is not used in Safety One Argus as the system uses the sender email address that is configured in the `System Configuration > SMTP Configuration > Global From Address` field.

Argus Analytics ETL

1. Go to `Argus Console > System Management (Common Profile Switches) > Argus Analytics`.
2. Set **Enable ETL Notification via Email** to **Yes**.
3. In **ETL Notification Receivers**, enter at least one valid email address.
4. In **ETL Notification Sender**, enter the sender email address.

> **Note**
>
> The ETL Notification Sender parameter is not used in Safety One Argus as the system uses the sender email address that is configured in the `System Configuration > SMTP Configuration > Global From Address` field.

14

Upgrade Oracle Argus Safety Database

The space requirements for the upgrade are determined by the upgrade script. This requirement is mostly for new objects created during the upgrade. It is a fair estimate of space requirements.

In this chapter:

Prerequisites for Database Upgrade

- Log in to ARGUS_APP schema.
- Verify that the common profile switch DATABASE_TIMEZONE is not empty by executing the following script:

  ```
  select key, value from cmn_profile where key = 'DATABASE_TIMEZONE';
  ```

  > **Note**
  >
  > This is applicable only if you are upgrading from Argus version 8.1.1 or above.

- The Oracle Database Server version should be upgraded as per the technology stack (see Oracle Components).
- Verify that JRE 1.8 or above is installed, and JCE policy is applied.
- Verify that the Oracle TNSNAMES have been configured.
- To avoid errors during upgrade, do either of the following:
  - Keep datafiles AUTOEXTEND ON, or
  - Monitor free space and add more space, if required
- Create one large rollback segment or size 20 GB for LARGE size model.

  Keep all other rollback segments, except SYSTEM, offline.
- The source Oracle Argus Safety database must be AL32UTF8 character set.
- The database semantics must be CHAR and not BYTE.

Oracle Argus Safety Database Upgrade

> **Note**
>
> You will need to generate a key prior to the database upgrade or you can use `ArgusSecureKey.ini` from the existing setup.
>
> You must also make sure that the password information specified in the database is consistent with the information provided in the `ArgusSecureKey.ini` file.

> **Note**
>
> To execute the database creation and setup on a Linux server, copy the build folder from the *`Argus Release Media`*`\Database\Argus Safety` on the server.

You may be prompted to press **Enter** at screens that are not included in the procedure. This does not hinder the upgrade procedure. Where applicable, press **Enter** to continue with the upgrade process.

1. Make sure the **dbinstaller.properties** are set up correctly. (See Configure the Database Setup Properties File.)
2. Validate the existing Oracle Argus Safety using the `SchemaValidation.bat` file. Use the validation file of the existing installed version from the Schema Validation folder:

   `Argus Release Media``\Database\Argus Safety\SchemaValidation`
3. View the validation log file to make sure that the existing database has no errors, missing and invalid objects.
4. To create a new DBA user and refresh the existing DBA user grants, Run Create DBA User Script.
5. From the *`Argus Release Media`*`\Database\Argus Safety` folder, run the `dbinstallerUI.bat` file as an administrator, to invoke the user interface and enter the parameters.

   The Argus Safety - Database Setup screen appears.

   You cannot modify any details on this screen. In case, any of the information is incorrect, then you must re-create the schema.

   For a silent upgrade, from the *`Argus Release Media`*`\Database\Argus Safety` folder, run the **dbinstaller.bat** file as an administrator.
6. In case of upgrade, all the schema details will be auto-populated based on the schema selection logic. Before proceeding further, you must confirm that all the schema details are correctly populated.

   > **Note**
   >
   > You must not create any Oracle Argus Safety objects in custom schema.

7. Click **Next**.
8. Enter the path for Tablespaces and click **Next**.
9. Verify the Setup Parameters and click **Execute**.
10. To ignore any error due to customization, check **Ignore Error** checkbox in the DBInstaller user interface, and analyze it later when the upgrade is done.
11. To validate the schema, from the *Argus Release Media*\Database\Argus Safety\Schema Validation folder, run the SchemaValidation.bat file.

    See Validate Oracle Argus Safety Database.

Post Upgrade Steps

1. Log in to ARGUS_APP schema.
2. Verify that the common profile switch DATABASE_TIMEZONE is not empty by executing the following script:

```
select key, value from cmn_profile where key = 'DATABASE_TIMEZONE';
```

Enable Local Locking in Oracle Argus Safety

Before enabling Local Locking in Oracle Argus Safety, you must make sure that you have upgraded your database to this release successfully.

1. Execute the batch file Enable_local_lock.bat from *Argus Release Media*\Database\Argus Safety\Utilities\Enable_local_lock directory.
2. Enter the response for *Do you wish to turn on the Local Locking feature for one or more enterprises (Yes/No)?*, enter **Yes** to continue.
3. Enter the log file name to record the results.

   This is the execution log that is created on the client workstation under the Enable_local_lock directory mentioned above.
4. Enter TNSNAMES Entry to Connect to the source SAFETY Database.
5. Enter SAFETY schema owner name in source Database.
6. Enter the password for safety schema name in source Database.
7. Enter comma separated list of enterprises where local locking feature is to be enabled or enter ALL for all enterprises in Source safety Database.

   If no value is entered script will run for enterprise 1 by default.
8. Enter the Agency name for PMDA reporting destination as configured in **Reporting Destination** codelist.
9. To enable local locking privileges for the Oracle Argus Safety Japan users, enter **Yes**.

   Follow the prompts for confirmation.

> **Note**
>
> If the agency entered is invalid for any of the enterprises, the utility will abort and no changes will be committed.
>
> In case of a multi-tenant environment, if this utility is re-run for any of the enterprises, it will display a list of the enterprises for which it has already executed and will continue to process rest of the enterprises.

Merge a Single Enterprise Safety Database into a Multi-tenant Database

In this section:

Prerequisites to Run the Merge Export Step

- The end user should not use the source database during the export process.
- Install Oracle Argus Safety 2026.1.01 on a computer where Oracle database is installed. Make sure the Oracle database is installed as per the System Requirements.
- The source databases should be schema validated at Oracle Argus Safety 2026.1.01.
- The source database should only be a single-tenant database.
- The source database data must contain only one ENTERPRISE.

Merge Export

1. From the Start menu, navigate to the following path:

   Argus Release Media\Database\Argus Safety\Utilities\Merge_to_Multitenant

2. Double-click the `merge_export.bat` file and follow the instructions on the sqlplus screen.
   a. Enter Log File Name to record results.

      This is the execution log that is created on the client workstation:

      Log file path: *Argus Release Media*\Database\Argus Safety\Utilities\Merge_to_Multitenant

   b. Enter TNSNAMES Entry to Connect to the Source SAFETY Database.
   c. Enter SYSTEM or DBA user name in source Database.
   d. Enter password for SYSTEM or DBA user in source Database.

e. Enter SAFETY schema owner name in source Database.

f. Enter password for Oracle Argus Safety schema owner in source Database

g. Enter Oracle Argus Interchange schema owner name in Oracle Argus Safety Database

h. Enter password for Oracle Argus Interchange schema owner in source Database.

i. Enter the full directory Path to create the Source Oracle Argus Safety database export dump file:

   This is the Path on the **Source Database Server** where the Oracle Argus Safety Database resides. The batch file will create an export dump file (`SAFETY.DMP`) and an export log file (`SAFETY_EXPORT.LOG`) in the directory.

   Make sure that `SAFETY.DMP` file does not exist prior to the export.

3. Make sure that no error has occurred during the database export, by checking the following log files:

   - Log file name entered as parameter 1 during export step execution.
   - Following Oracle Export log files are created on database server. The path is the value entered on “Enter Directory including full Path to create Source safety database export dump file" during export step:

     `SAFETY_EXPORT.log`

Export the dmp File Copy to the Target Database Server

Move the export dmp file created in Merge Export from the source database server to the target database server.

Prerequisites to Run the Merge Import Step

- Create a cold backup of the target database before starting the Merge Import step.
- The end user should not use the target database during the import process.
- Only one Merge Import process can run on the target database at a time.
- Auto extend should be set on for all database files in the target database.
- Sufficient space should be available on the target database server to import the new enterprise data. The amount of space depends on the number of cases in source Oracle Argus Safety database.
- Install the Oracle Argus Safety 2026.1.01 application. Make sure that Oracle Client version is same as the database server.
- The target databases should be Schema Validated at Oracle Argus Safety 2026.1.01.
- The target database must be a multi-tenant database.
- All source database dictionaries should be available in target database. If the dictionary does not exist then install missing dictionaries on the target database.
- All existing AG service users on the source database must exist on the target database.
- All source database LDAP configured server names should be available in target database.

Merge Import

1. From the Start menu, navigate to the following path:

   Argus Release Media\Database\Argus Safety\Utilities\Merge_to_Multitenant

2. Click `merge_import.bat` and enter the following parameters for the target database:

   a. Log File Name to record results.

      This is the execution log that will be created on the client workstation.

      Log file path: *Argus Release Media*\Database\Argus Safety\Utilities\Merge_to_Multitenant

   b. TNSNAMES entry to connect to the target Safety database.

   c. SYSTEM or DBA user name.

   d. Password of the DBA user.

   e. VPD schema owner name.

   f. Password of the VPD schema owner.

   g. SAFETY schema owner name.

   h. Password of the Oracle Argus Safety schema owner.

   i. Oracle Argus Interchange schema owner name.

   j. Password of the Oracle Argus Interchange schema owner.

   k. Directory location where the export dmp file is copied for the import process.

      This is the path on the Target Database Server where the Oracle Argus Safety database is installed. The batch file creates an import log file in this directory.

   l. Name of the new enterprise.

   m. Abbreviation of the new enterprise.

   n. SAFETY schema owner name in the source database.

   o. Oracle Argus Interchange schema owner name in source database.

3. This batch file imports the data from the dump file into the target database.

4. Make sure that no error has occurred during import by checking the following log files:

   - Log file name entered as parameter 1 during Import step execution.
   - The following Oracle Import log files are created on database server. The path is the value entered in “Enter Directory including full Path on target database server where export dmp file copied for import process" during import step.
     - `SAFETY_IMPORT_safety.log`
     - `SAFETY_IMPORT_interchange.log`
     - `SAFETY_IMPORT_SAFETY_DUP_SEARCH_DATA.log`
     - `SAFETY_IMPORT_SAFETY_DUP_LAM_SEARCH_DATA.log`

5. Validate the schema of the database using the **SchemaValidation.bat** file.

Synchronize Dictionary Manually

The merge process synchronizes the dictionary information based on the dictionary name in the source and target database. If the source dictionary name is not available in target database, then manual synchronization is required.

To synchronize the dictionary data manually on the target database:

1. Log in as the Oracle Argus Safety schema owner using sqlplus on the target safety database.
2. Locate the new ENTERPRISE_ID value created from import process using the following sql:

   ```
   SELECT VALUEFROM cmn_profile_globalWHERE section = 'DATABASE' AND KEY =
   'MERGING_TO_MULTITENANT';
   ```

3. Set the context value to new Enterprise_id

   ```
   Exec pkg_rls.set_context('admin',< Value of New Enterprise ID>,'ARGUS_SAFETY');
   ```

4. Locate the list of Dictionaries ID's where Dictionary synchronization pending due to missing Dictionaries on Target database. If the following sql results in NO ROWS, then no further action is required.

   ```
   Select dict_idFrom cfg_dictionaries_enterpriseWhere enterprise_id = <Value of New
   Enterprise ID>And global_dict_id = -1;
   ```

5. Log in as the Oracle Argus Safety schema owner using sqlplus on the source safety database.
6. Locate the dictionary name of each Dictionary ID where the dictionary does not exist on the target database using the following sql:

   ```
   Select name from cfg_dictionaries_global where dict_id in (<List of Dict ID values
   (comma separated) from Step 4);
   ```

7. Load the missing dictionaries on the target database.
8. Set the context to new enterprise_id using following sql on target database.

   ```
   Exec pkg_rls.set_context('admin',<Value of new ENTERPRISE_ID> ,'ARGUS_SAFETY');
   ```

9. Update GLOBAL_DICT_ID data in the target database using the following SQL:

   ```
   UPDATE CFG_DICTIONARIES_ENTERPRISE
   SET GLOBAL_DICT_ID = <Dictionary Global Dict ID value from target database>
   WHERE ENTERPRISE_ID = <New ENTERPRISE_ID created in Target Database>
   AND DICT_ID = <Value of Dict ID in New ENTERPRISE with Dictionary name>
   AND GLOBAL_DICT_ID =-1;
   ```

15

Create the Oracle Argus Insight Data Mart Structure

The Oracle Argus Insight data mart structure is created while installing Oracle Argus Insight through Liquibase in silent-mode.

Besides, it also creates a link between the source Oracle Argus Safety database and the new Oracle Argus Insight data mart. The Extract Transform and Load (ETL) process uses this link to transfer data from Oracle Argus Safety database to the Oracle Argus Insight data mart for reporting purposes.

Liquibase is a refactoring tool that enables Oracle Argus Insight to be in synchronization with the closest major release, and subsequently upgrades the product to the required minor versions of the product.

> **Note**
>
> The Oracle Argus Insight database must be created with the same character set as the Oracle Argus Safety database. Make sure you have installed the requisite software as per System Requirements.

For more information, see:

- Before You Run the Oracle Argus Insight Installation
- Configure dbinstaller.properties file
- Create Oracle Argus Insight Database Schema
- Create Database Links
- Run Initial ETL
- Run Additional Grant Scripts for Single DB Instance

Before You Run the Oracle Argus Insight Installation

The `GLOBAL_NAMES` and `NLS_LENGTH_SEMANTICS` database parameters must be configured properly in order for the Oracle Argus Insight installation to run. You must check those settings *before* you run the Oracle Argus Insight Installation. If the parameters are not set properly, the installation will fail.

For more information, see:

- Review and Modify the Database Settings
- Create a DBA user

Review and Modify the Database Settings

1. Contact your database administrator (DBA).

2. Verify that the database configuration file for the Oracle Argus Insight database defines the following database parameter values:
   - `GLOBAL_NAMES`

     Value of parameter GLOBAL_NAMES must be same in Oracle Argus Safety and Oracle Argus Insight (either TRUE for both or FALSE for both).

     If GLOBAL_NAMES is set to TRUE, the Database Name reflected in the table GLOBAL_NAME, must have the same domain for both Oracle Argus Safety and Oracle Argus Insight databases (like, us.example.com).
   - `NLS_LENGTH_SEMANTICS` = CHAR
   - `TNS Name` for Oracle Argus Safety Database must be present in the Oracle Argus Insight Database Server (and vise-versa) > tnsnames.ora file at the following path: `...\network\admin\tnsnames.ora`
3. Restart the database instance to reflect the changes.

Create a DBA user

To use a different user than SYSTEM user to execute the installation, then create a DBA user by executing the DBA User Creation script:

Build path`\Database\Argus Insight\Utilities\Create_Dba_User\ai_create_dba_user.bat`

For more details on creating this user, see Create the DBA User.

Besides creating the DBA user, this batch file also provides minimum necessary privileges required for executing the installation.

Configure dbinstaller.properties file

Open the DBInstaller\dbinstaller.properties file, and view or modify the following parameters to make sure that Liquibase runs properly.

Parameter	Description	Modify	Default or Sample Value
`db_connect_string`	Database instance details	Yes	db_connect_string=<host>:<port>/<service name>
`dba_user`	Name of the Target Database DBA user	Yes	dba_user=AI_DBA_USER
`log_level`	Log level setting related to liquibase for smooth run. Possible values: • DEBUG • INFO	Yes	log_level=info
`argus_securekey_path`	Complete directory path of Oracle Argus Safety Secure Key ini file on the middle-tier.	Yes	argus_securekey_path=c:/windows
`appschema_mart_user`	Oracle Argus Insight Mart schema Owner	No	appschema_mart_user=APR_MART/pwd
`appschema_stage_user`	Oracle Argus Insight Staging schema Owner	Yes	appschema_stage_user=APR_STAGE/pwd

Parameter	Description	Modify	Default or Sample Value
appschema_ai_link_user	Oracle Argus Insight Link User	Yes	appschema_ai_link_user=APR_LINK/pwd
appschema_rls_user	Oracle Argus Insight VPD schema Owner	Yes	appschema_rls_user=RLS_USER/pwd
appschema_mart_app_user	Oracle Argus Insight Application schema Owner	Yes	appschema_mart_app_user=APR_APP/pwd
appschema_mart_hist_user	Oracle Argus Insight History schema Owner	Yes	appschema_mart_hist_user=APR_HIST/pwd
appschema_ai_apr_user	Oracle Argus Insight apr User Name	No	appschema_ai_apr_user=APR_USER/pwd
appschema_ai_login_user	Oracle Argus Insight Login User Name	Yes	appschema_mart_user=APR_LOGIN/pwd
ai_role	Oracle Argus Insight Mart Role	Yes	ai_role=MART_ROLE
ai_app_role	Oracle Argus Insight Mart App Role	Yes	ai_app_role=APP_ROLE
ai_link_role	Oracle Argus Insight Mart Link Role	Yes	ai_link_role=LINK_ROLE
safety_db	Oracle Argus Safety database instance name	Yes	• safety_db=SAF2026101DB, or • safety_db=SAF2026101DB.US.EXAMPLE.COM
safety_ro_user	Oracle Argus Insight read only user in Safety DB	Yes	safety_ro_user=INSIGHT_RO_USER
#Default Datafiles Directory	Default location of the datafiles. on the Database Server	Yes	default_datafile_destination =<c:/app/oradata/2026101DB>
#Insight Stage Normal Datafiles	Location of Oracle Argus Insight normal datafiles.	Yes	• ai_stage_data_01_datafile=APR_STAGE_DATA_01.DBF • ai_stage_ind_01_datafile=APR_STAGE_INDEX_01.DBF • ai_stage_lob_01_datafile =APR_STAGE_LOB_01.DBF
#Insight Stage ESM Datafiles	Location of Oracle Argus Insight ESM datafiles.	Yes	• apr_sesm_data_01_datafile =APR_SESM_DATA_01.DBF • apr_sesm_ind_01_datafile=APR_SESM_INDEX_01.DBF • apr_sesm_lob_01_datafile=APR_SESM_LOB_01.DBF
#Insight Stage WHO Datafiles	Location of Oracle Argus Insight WHO datafiles.	Yes	• stage_who_01_datafile=APR_SWHOC_DATA_01.DBF

Parameter	Description	Modify	Default or Sample Value
#Insight Mart Case/Rpt Datafiles	Location of Oracle Argus Insight Mart case and report datafiles.	Yes	• mart_case_rpt_data_01_datafile=APR_MCAS_DATA_01.DBF • mart_case_rpt_ind_01_datafile=APR_MCAS_INDEX_01.DBF • mart_case_rpt_lob_01_datafile=APR_MCAS_LOB_01.DBF
#Insight Mart Non-Case/Rpt Datafiles	Location of Oracle Argus Insight Mart non-case and report datafiles.	Yes	• mart_non_case_data_01_datafile=APR_MCFG_DATA_01.DBF • mart_non_case_ind_01_datafile=APR_MCFG_INDEX_01.DBF • mart_non_case_lob_01_datafile=APR_MCFG_LOB_01.DBF
#Insight Mart EDM Datafiles	Location of Oracle Argus Insight Mart EDM datafiles	Yes	• mart_edm_data_01_datafile=APR_MEDM_DATA_01.DBF • mart_edm_ind_01_datafile=APR_MEDM_INDEX_01.DBF • mart_edm_lob_01_datafile=APR_MEDM_LOB_01.DBF
#Insight Mart WHO Datafiles	Location of Oracle Argus Insight Mart WHO datafiles	Yes	• mart_who_01_datafile=APR_MWHOC_DATA_01.DBF
#Insight Hist Case/Rpt Datafiles	Location of Oracle Argus Insight case or report History datafiles	Yes	• hist_case_rpt_data_01_datafile=APR_MCAS_HIST_DATA_01.DBF • hist_case_rpt_ind_01_datafile=APR_MCAS_HIST_INDEX_01.DBF • hist_case_rpt_lob_01_datafile=APR_MCAS_HIST_LOB_01.DBF
#Insight Hist Non-Case/Rpt Datafiles	Location of Oracle Argus Insight non-case and report History datafiles.	Yes	• hist_non_case_data_01_datafile=APR_MFACT_HIST_DATA_01.DBF • hist_non_case_ind_01_datafile=APR_MFACT_HIST_INDEX_01.DBF • hist_non_case_lob_01_datafile=APR_MFACT_HIST_LOB_01.DBF
#Insight Apr Datafiles	Location of Oracle Argus Insight APR datafiles	Yes	• apr_user_data_01_datafile=APR_USER_DATA_01.DBF • apr_user_ind_01_datafile=APR_USER_INDEX_01.DBF • apr_user_lob_01_datafile=APR_USER_LOB_01.DBF
Default and Temporary tablespaces	Defines default and temporary tablespace name	Yes	• default_ts=USERS • temp_ts=TEMP

Parameter	Description	Modify	Default or Sample Value
Tablespace Encryption	Specifies the logic used for default encryption	Yes	tablespace_encryption=<blank> or <text>, where • blank—No encryption • text—like encryption using 'AES256' default storage (encrypt)
Tablespace Parameters	Specifies the details of the tablespace	Yes	• tablespace_initial_size=10M • tablespace_autoextend=ON • tablespace_next_size=10M • tablespace_block_size=8K

Create Oracle Argus Insight Database Schema

Follow these steps:

- Prerequisites
- Create Users in the Oracle Argus Safety Database
- Create the DBA User
- Create Fresh Oracle Argus Insight Schema
- Validate the Schema
- Create Oracle Argus Insight Read-only User

Prerequisites

Make sure:

- an Oracle client with Administrator option is installed on the server.
- database TNS entry is be added in the `TNSNAMES.ora` file.
- PRMART connection entry is added in the `TNSNAMES.ora` file.
- login machine user should have administrative privileges.

For more information, see:

- Install Java
- Set Java Installation Path

Install Java

1. Download the **jce_policy-8.zip** file on your local machine from the following link:

   http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html (download jce_policy-8.zip).
2. Unzip the jce_policy-8.zip.
3. Replace **local_policy.jar** and **US_export_policy.jar** files present in all the Java JRE installation security folders with the local_policy.jar and US_export_policy.jar shipped in **jce_policy-8.zip**.

   For example:

Location of Java JRE 64-bit.

`C:\Program Files\Java\jre1.8.0_161\lib\security`

4. From the command prompt verify that Java is properly installed by executing:

   java -version

   If no Java version appears, check the environment variables settings and path system variables have correct Java installation path set.

Set Java Installation Path

1. Right-click the My Computer (or Computer) icon, and from the drop-down menu select **Properties**.
2. From the left-pane, select **Advanced system settings**.

   The System Properties dialog box with Advanced tab appears.
3. In the Startup and Recovery section, click **Environment Variables**.
4. From the System variables section, scroll-down to **Path** variable, and double-click.

   The Edit System Variable dialog box appears.
5. In the **Variable value:** field, enter the location where Java will be installed, and end it with a semi-colon (;).
6. Click **OK** to close the Edit System Variable dialog box.
7. Click **OK** to close the System Properties dialog box.

Create Users in the Oracle Argus Safety Database

1. To create the Oracle Argus Safety Read-only user for Oracle Argus Insight, execute the following script from the folder *`Argus Release Media`*`\Database\Argus Insight\Utilities\Create_Safety_Ro_User:`
   - For Windows—Use the batch script ai_argus_read_only{user}.bat
   - For Linux—Use the shell script ai_argus_read_only{user}
2. When prompted, enter the following parameters:
   - Name of the Oracle Argus Safety Database instance
   - Name of DBA User in Oracle Argus Safety Database
   - DBA user password in Oracle Argus Safety Database
   - Name of the Oracle Argus Safety Read Only User to be created for Oracle Argus Insight
   - Password of the Oracle Argus Safety Read Only User
   - Default Tablespace for Oracle Argus Safety Read-only User—For example, USERS
   - Temporary Tablespace for Oracle Argus Safety Read-only User—For example, TEMP

   The process of creating a Oracle Argus Safety Read-only user begins.
3. Review the log file from the following path, and check for any errors, when a confirmation message appears.

   `Argus Release Media``\Database\ArgusInsight\Utilities\Create_Safety_Ro_User\AI_AS_RO_User_MMDDYYYY_HH24MISS.log`

Create the DBA User

> **Note**
>
> You must execute this script to install Oracle Argus Insight database, even if you are using the SYSTEM user. This script provides additional grants to the existing user.

To create a DBA user that has privileges same as the SYSTEM user for installation:

1. Execute the following script from the folder *Argus Release Media*\Database\ArgusInsight\Utilities\Create_Dba_User:
   - For Windows—Use the batch script ai_create_dba_user.bat
   - For Linux—Use the shell script ai_create_dba_user

   A prompt appears as `Do you want to use SYSDBA to run the script? (Y/N):`. Enter **Y** to run as SYSDBA.
2. When prompted, enter the following parameters:
   - Oracle Argus Insight Database instance name
   - SYS or an equivalent SYSDBA user on this database
   - SYSDBA user password
   - Name of the DBA User—For example, AI_DBA_USER
   - DBA user password

   If you provide a non-existing user name, then the script creates this as a new user, and provides the necessary grants to this user.

   If you provide an already existing user name, then the script provides the necessary additional grants to the existing user.

   When done, a message appears as:

   ```
   Created DBA user &dba_user
   ```
3. Press **Exit**.
4. Verify the log files for status information from:

   Argus Release Media\Database\ArgusInsight\Utilities\Create_Dba_User\AI_DBA_User_MMDDYYYY_HH24MISS.log

> **Note**
>
> For security reasons, Oracle recommends to drop the DBA user from the database after successful installation of Oracle Argus Insight as this user will have DBA privileges.
>
> To drop this user, connect to the respective database as a privileged user, and execute the following command:
>
> ```
> DROP USER <INSTALL_USER> CASCADE;
> ```

Create Fresh Oracle Argus Insight Schema

1. Log in to the Oracle Argus Insight Transaction Server.
2. Navigate to *`Argus Release Media`*`\Database\Argus Insight`.
3. Open the **dbinstaller.properties** file.
4. Modify the following parameters:
   - **Insight Database**:
     - db_connect_string—connects to the Oracle Argus Insight database.

       Syntax: db_connect_string=<host>:<port>/<service name>

       For example, server.us.xx.com:1521/AI2026101MT
     - dba_user—specifies the name of the DBA user to run Oracle Argus Insight Liquibase Install.

       See Create the DBA User.
     - default_datafile_directory—default location on the database server, where datafiles will be created.
   - **Insight User** of each schema, where password is optional:
     - appschema_mart_user
     - appschema_stage_user
     - appschema_mart_app_user
     - appschema_mart_hist_user
     - appschema_ai_link_user
     - appschema_rls_user
     - appschema_ai_login_user

     > **Note**
     >
     > The appschema_ai_apr_user parameter should not be modified in the **dbinstaller.properties** file.
   - **Insight Roles:**
     - ai_role—specifies Mart User roles
     - ai_app_role—specifies App User roles

- ai_link_role—specifies Link User roles

- **Secure Key:**
  - argus_securekey_path—path of the file insight.ini in the middle-tier machine from where the DBInstaller.bat is executed.
- **Safety Database:**
  - safety_db—Oracle Argus Safety database instance name
  - safety_ro_user—Oracle Argus Insight Read-only user created in Oracle Argus Safety

> **Note**
>
> For more information on these parameters, see Configure dbinstaller.properties file.
>
> It is recommended that you preserve the default names for tablespaces and roles.

5. From the command prompt, go to DBInstaller directory.
6. Type dbinstaller.bat, and press **Enter**.

   The Liquibase install begins, and the parameters (as entered) appear on the command prompt screen with password in the hidden mode (****).
7. Keep monitoring the Liquibase progress by querying the Liquibase Log table insight_dbchangelog, created in APR_MART schema.

> **Note**
>
> For Oracle Argus Insight 2026.1.01 Fresh Schema creation on 19c, if you encounter the error `Could not release lock`, follow the workaround:
>
> a. Clear/Release the liquibase lock (login as as_dba_user)
> b. Truncate apr_mart.insight_dbchangeloglock table
> c. Rerun installer.

8. When the process is complete, a confirmation message appears with the latest version of Oracle Argus Insight.

   The following is created as per the values specified in the `dbinstaller.properties` file:

   - **Users**
     - MART_USER
     - STAGE_USER
     - MART_APP_USER
     - MART_HIST_USER
     - AI_LINK_USER
     - RLS_USER
     - AI_APR_USER

  - AI_LOGIN_USER
- **Roles**
  - AI_ROLE
  - AI_APP_ROLE
  - AI_LINK_ROLE
- **Factory Data**
  - Out of the box Factory data is loaded into tables such as ETL_PROCEDURES, CMN_PROFILE_GLOBAL, etc.
- **Database Links**, DB_LINK_ARGUS:
  - From STAGE_USER of Argus Insight to INSIGHT_RO_USER of Safety
  - From MART_USER of Argus Insight to INSIGHT_RO_USER of Safety
  - From MART_APP_USER of Insight to INSIGHT_RO_USER of Safety
- **Tablespaces**
  Note that the tablespace names begin with APR. The Argus Power Reports (APR) product was renamed to Oracle Argus Insight.

STAGE Schema Tablespaces	MART Schema Tablespaces	HIST Schema Tablespaces	APR User Tablespaces
APR_STAGE_DATA_01	APR_MCAS_DATA_01	APR_MCAS_HIST_DATA_01	APR_USER_DATA_01
APR_STAGE_INDEX_01	APR_MCAS_INDEX_01	APR_MCAS_HIST_INDEX_01	APR_USER_INDEX_01
APR_STAGE_LOB_01	APR_MCAS_LOB_01	APR_MCAS_HIST_LOB_01	APR_USER_LOB_01
APR_SESM_DATA_01	APR_MCFG_DATA_01	APR_MFACT_HIST_DATA_01	--
APR_SESM_INDEX_01	APR_MCFG_INDEX_01	APR_MFACT_HIST_INDEX_01	--
APR_SESM_LOB_01	APR_MCFG_LOB_01	APR_MCFG_HIST_LOB_01	--
APR_SWHOC_DATA_01	APR_MEDM_DATA_01	--	--
--	APR_MEDM_INDEX_01	--	--
--	APR_MEDM_LOB_01	--	--
--	APR_MWHOC_DATA_01	--	--

9. Press **Exit**.

Validate the Schema

1. Navigate to *`Argus Release Media`*`\Database\ArgusInsight\ValidateSchema`.
2. Run the batch script **validate_schema.bat**.
3. When prompted, enter the following parameters:
   - Enter instance name: <Oracle Argus Insight Database Instance name>

- Enter DBA User Name: <DBA user of Oracle Argus Insight>
- Enter Password for DBA User: <DBA User password in Oracle Argus Insight>
- Enter Validation Data File Name: The validation control file name:

  <VLDN_APR_AI_8.4.5.CTL>
- Enter the destination where the log file is to be placed:

  `Argus Release Media\Database\ArgusInsight\ValidateSchema`
- Enter the log file name for recording the schema differences:

  <VLDN_APR_AI_8.4.5_diff.log>
- Enter Validation Output File Name: The validation output file name to record the validation progress:

  <VLDN_APR_AI_8.4.5.log>

4. Enter the password for the Oracle Argus Insight SYSTEM or DBA user, and press **Enter**.
5. When the validation process is complete, a confirmation message appears.

   The log files are created at the following location:

   `Argus Release Media``\Database\ArgusInsight\ValidateSchema\`

   - To view any schema discrepancies, such as missing objects, use the Difference Log File.
   - To view the list of errors, which occurred during schema validation, use the Output Log File.

> **Note**
>
> - If Oracle Argus Insight read-only user is created, then ignore the schema validation differences, where
>   - Objects are RO% views/columns
>   - GRANTEE is Oracle Argus Insight Read-only user
> - If Oracle Argus Insight and Oracle Argus Mart are installed on the same Database server, ignore the differences due to grants from APR_MART/RLS_USER of Oracle Argus Insight to AM_MART_USER/AM_APP_USER of Oracle Argus Mart.

Create Oracle Argus Insight Read-only User

1. Open *`Argus Release Media`*`\Database\ArgusInsight\Utilities\Create_Insight_Ro_User` file.
   - For Windows—execute the batch script ai_ro_user.bat
   - For Linux—execute the shell script ai_ro_user
2. When prompted, enter the following parameters:
   - Enter TNSNAME Entry to connect to the ARGUS INSIGHT Database: <ARGUS INSIGHT Database name>
   - Enter the name of Custom DBA user in Oracle Argus Insight Database: <Argus Insight Install user>

- Enter password for install user in Oracle Argus Insight Database: <Install user password>
- Enter Oracle Argus Mart schema owner name in Oracle Argus Insight Database: <Mart User of Insight>
- Enter Oracle Argus Insight History schema owner name in Insight Database: <Mart Hist User of Insight>
- Enter Read Only user to be created in Oracle Argus Insight Database: <Read-only user to be created in Insight>
- Enter password for Read Only user of Oracle Argus Insight Database: <Insight Read-only user password>

3. Press **Exit**.
4. Verify the log files for status information from:

   Argus Release Media\Database\Argus Insight\Utilities\Create_Insight_Ro_User\AI_RO_User_MMDDYYYY_HH24MISS.log

Create Database Links

In this section:

From Oracle Argus Safety to Oracle Argus Insight Database

This link allows real-time updates of some of the values from Oracle Argus Safety Console to Oracle Argus Insight data mart.

1. Create the reverse DB Link by executing the script file from *Argus Release Media*\Database\Argus Insight\Utilities\Database_Links\argus_to_mart.
   - For Windows—execute the batch script ai_argus_db_link_setup.bat
   - For Linux—execute the shell script ai_argus_db_link_setup
2. When prompted, enter the following parameters:
   - Enter the Oracle Argus Safety Database Tns Name: <Safety Database Instance Name>
   - Enter the Oracle Argus Safety DBA owner in <Safety Database Instance Name>, for example AS_DBA_USER)
   - Enter the password for user AS_DBA_USER
   - Enter the name of Oracle Argus Safety schema owner in Oracle Argus Safety Database Instance: <user account that owns the Oracle Argus Safety schema, for example: ARGUS_APP>
   - Enter the password for Oracle Argus Safety schema owner: <password of Oracle Argus Safety owner>
   - Enter the name of Oracle Argus Safety Role: <Oracle Argus Safety role>

- Enter the name of Read only user in Oracle Argus Safety Database: <Oracle Argus Insight Read-only user, created in Oracle Argus Safety>

  For example, <*INSIGHT_RO_USER*>
- Enter the Oracle Argus Insight Database Tns Name: <Oracle Argus Insight database>
- Enter the name of link user in Oracle Argus Insight Database.: <link user of Oracle Argus Insight for example: APR_LINK_USER>
- Enter the password for user Link user: <link user password>

3. Verify that the script is successfully connected as <Oracle Argus Safety schema owner/ Oracle Argus Safety schema password>@<Oracle Argus Safety Database Name>, and press **Enter**.
4. When the confirmation message appears, press **Enter**.

   Wait until a message `Created <Insight DB Global Name> @ARGUS_TO_MART` appears. This link name gets stored in the key DB_LINK_ARGUS_TO_MART of CMN_PROFILE_GLOBAL of the Oracle Argus Safety database.
5. Press **Exit** to close the window.
6. Verify the log files for status from:

   `*Argus Release Media*\Database\Argus Insight\Utilities\Database_Links\argus_to_mart\ ARGUS_TO_MART_DB_LINK_MMDDYYYY_HH24MISS.log`

From Oracle Argus Insight to Oracle Argus Safety (manually)

During Fresh installation, the database link from Oracle Argus Insight to Oracle Argus Safety (DB_LINK_ARGUS) is created as a part of the installation process. However, you can manually recreate the link DB_LINK_ARGUS.

1. Navigate to `*Argus Release Media*\Database\Argus Insight\Utilities\Database_Links\db_link_argus`.
   - For Windows—execute the batch script ai_create_db_link_argus.bat
   - For Linux—execute the shell script ai_create_db_link_argus
2. When prompted, enter the following parameters:
   - Enter the name of the Oracle Argus Safety Database instance: <SaOracle Argus Safetyfety Database Instance Name>
   - Enter the name of the Oracle Argus Insight Database instance: <Oracle Argus Insight Database Instance Name>
   - Enter the name of DBA User in Oracle Argus Insight DB: <Oracle Argus Insight dba user>
   - Enter the password for user &dba_user: <Oracle Argus Insight dba user pwd>
   - Enter the name of the Read Only User in Oracle Argus Safety DB: <Oracle Argus Safety Read Only user for Oracle Argus Insight, for example: INSIGHT_RO_USER>
   - Enter the password for Read Only user in Oracle Argus Safety: <Read-only user pwd>
   - Enter the name of the stage owner in Oracle Argus Insight: <Stage user of Oracle Argus Insight>
   - Enter the password for Oracle Argus Insight user: <Stage user password>

- Enter the name of the mart owner in Oracle Argus Insight: <Oracle Argus Mart user of Oracle Argus Insight>
- Enter the password for Oracle Argus Mart owner: <Oracle Argus Mart user password>
- Enter the name of the mart app owner in Oracle Argus Insight: <App user of Oracle Argus Insight>
- Enter the password for app owner: <App user password>

3. Verify that the script is successfully connected as <Oracle Argus Insight DBA user/Oracle Argus Insight DBA user pwd>@<Oracle Argus Insight>, and press **Enter**.

   Wait until a message `Created <Safety DB Global Name> @DB_LINK_ARGUS` appears for each Stage, Mart, and App user. This link name is stored in the key DB_LINK_ARGUS of CMN_PROFILE_GLOBAL in the Oracle Argus Insight database.

   For example, a typical DB link is:

   - SAF2026101DB@DB_LINK_ARGUS
   - SAF2026101DB.US.CORP.COM@DB_LINK_ARGUS

4. Press **Exit** to close the Oracle Argus Insight to Argus Database Link Creation window.
5. Verify the log files for status from:

   `Argus Release Media\Database\Argus Insight\Utilities\Database_Links\db_link_argus\DB_LINK_ARGUS_MMDDYYYY_HH24MISS.log`

Run Initial ETL

1. Navigate to DBInstaller folder.
2. Double click **dbinstaller.exe**.
3. Click **Initial ETL**.
4. Enter the parameters, and click **OK**.
5. Click **Start ETL**.
6. To monitor the ETL progress, execute query on tables:
   - staging_data_insert_log
   - mart_data_insert_log

For more details on ETL, see Extract, Transform, and Load Data.

Run Additional Grant Scripts for Single DB Instance

If Oracle Argus Insight and Oracle Argus Mart are running on the same database, provide additional grants for this database instance.

1. Navigate to `Argus Release Media\Database\Argus Insight\Utilities\am_grants`.
   - For Windows—execute the batch script am_grants.bat
   - For Linux—execute the shell script am_grants
2. When prompted, enter the following parameters:

- Enter the TNS name to connect to SDM database: <Oracle Argus Insight Database Instance name>
- Enter the name of dba user in Oracle Argus Insight Database: <DBA user of Oracle Argus Insight Database>
- Enter Password for User install user: <DBA user password>

3. Press **Exit** when a status message appears as:

   ```
   Execution of grants from Insight to Mart User and Mart App User completed
   ```

4. Verify the log files for status from:

   ```
   Argus Release Media\Database\Argus Insight\DBInstaller\Utilities\am_grants\AM_GRANTS_MMDDYYYY_HH24MISS.log
   ```

> **Note**
>
> After execution of the utility, Oracle Argus Insight schema validation file will reflect additional privileges.

16

Upgrade the Oracle Argus Insight Data Mart Structure

Oracle Argus Insight upgrade process has been moved from Schema Creation Tool to Liquibase for silent installation.

For more information, see:

- Prepare for Database Upgrade
- Upgrade Database

Prepare for Database Upgrade

Before upgrading, make sure:

1. Take the latest Liquibase build for this release.
2. Recreate the DBA User.

   (See Create the DBA User.)
3. Recreate the Oracle Argus Safety RO User of Oracle Argus Insight.
4. Recreate the DB_LINK_ARGUS from Oracle Argus Insight to Oracle Argus Safety.

   (See From Oracle Argus Insight to Oracle Argus Safety (manually))

Upgrade Database

1. Log in to Oracle Argus Insight Transaction Server.
2. Navigate to *`Argus Release Media`*`\Database\Argus Insight`.
3. Open the **dbinstaller.properties** file.
4. Modify the following parameters:
   - `Insight Database`:
     - **db_connect_string**—connects to the Oracle Argus Insight database.

       Syntax: db_connect_string=<*host*>:<*port*>/<service name>

       For example, db_connect_string=Dbname.us.xx.com:1521/AI2026101MT

       Or, db_connect_string=Dbname.us.xx.com:1521/AI2026101MT.us.xx.com
     - **dba_user**—specifies the name of the DBA user to run Oracle Argus Insight Liquibase Install.

       See Create the DBA User.
   - `Insight User` of each schema, where password is optional:
     - appschema_mart_user
     - appschema_stage_user

  - appschema_mart_app_user
  - appschema_mart_hist_user
  - appschema_ai_link_user
  - appschema_rls_user
  - appschema_ai_apr_user
  - appschema_ai_login_user
- `Insight Roles:`
  - ai_role—specifies Mart User roles
  - ai_app_role—specifies App User roles
  - ai_link_role—specifies Link User roles
- `Secure Key:`
  - argus_securekey_path—path of the file insight.ini in the middle-tier machine from where the `DBInstaller.bat` is executed.
- `Safety Database:`
  - safety_db—Oracle Argus Safety database instance name
  - safety_ro_user—Oracle Argus Insight Read-only user created in Oracle Argus Safety

> **Note**
>
> For more information on these parameters, see Configure dbinstaller.properties file.

5. From the command prompt, go to DBInstaller directory.
6. Type dbinstaller.bat, and press **Enter**.

   The Liquibase upgrade begins, and the parameters (as entered) appear on the command prompt screen with password in the hidden mode (****).
7. Keep monitoring the Liquibase progress by querying the Liquibase Log table insight_dbchangelog, created in APR_MART schema.
8. When the process is complete, a confirmation message appears with the latest version of Oracle Argus Insight.
9. Validate Schema using the schema validation control file `VLDN_APR_AI_8.4.5.CTL`.

   See Validate the Schema.

Part IV
Configure Other Products

This part lists the other products that are installed and configured through Oracle Argus Safety or Oracle Argus Insight, and are required to complete the installation.

During the installation, the information in this manual may differ from what you see on your monitor if additional modules were selected during the Oracle Argus Safety Web Installation.

Prerequisites:

- Obtain a domain account with Local Administrator privileges.
- In case of application upgrade, make sure to Backup Configuration Files of the existing Oracle Argus Safety application before setting up the machines.

For more information, see:

- Configure and Enable Oracle Argus Dossier
- Install and Configure Axway B2Bi
- Install and Configure Oracle B2B
- Configure Oracle Analytics Server or Oracle Analytics Publisher
- Configure the Oracle Analytics Publisher Environment for Oracle Argus Insight
- Configure the Oracle Analytics Server Environment for Oracle Argus Insight
- Configure Argus Centralized Coding
- Extract, Transform, and Load Data

17

Configure and Enable Oracle Argus Dossier

In this chapter:

Prerequisites

1. Set Up Argus Middle and Client Tiers.
2. Install or Upgrade Oracle Argus Safety Database Tier .

Configure Oracle Argus Dossier

1. On the server where Dossier is installed, from the installation folder, open the file **service.config**. By default, the installation folder is:

   `C:\Program Files\Oracle\ArgusWeb\ASP\Argus.NET\bin`

2. Uncomment the entries for **DossierBuilder** in the section:

   <ServiceConfiguration>/<ServiceComponents>

3. From the installation folder, open the file **RelsysWindowsService.exe.config**.
4. Make sure that the *DatabaseConfiguration* section is configured for the following attributes:

Attribute	Description
DBName (Mandatory)	TNS of the Database to which the RelsysWindowsService should connect to. Example: DBName="GOLDDEMO"
DBUser	AGService Username. The RelsysWindowsService logs into the database using this login name. This has to be a user of type AGSERVICE. Example: DBUser="agservice_user1"
GeneralEmailTo	The e-mail address to which the e-mails will be sent by the Intake Service, using the General Email feature of Oracle Argus Safety. Example: GeneralEmailTo ="recepient@oracle.net"
GeneralEmailFrom	The email address from which the e-mails will be sent by the Intake Service, using the General Email feature of Oracle Argus Safety. Example: GeneralEmailFrom ="admin@oracle.net"
GeneralEmailCc	This email address will be added to the Cc line when e-mails are sent by the Intake Service, using the General E-mail feature of Oracle Argus Safety. Example: GeneralEmailCc ="recepient@oracle.net"

Attribute	Description
GeneralEmailBcc	The email address will be added to the Bcc line when e-mails are sent by the Intake Service, using the General E-mail feature of Oracle Argus Safety. Example: GeneralEmailBcc ="recepient@oracle.net"
Recurrence (Optional)	The value for this attribute specifies the frequency of instantiation of the associated Service Component. The value is specified in seconds. For example: `<add Name="DossierBuilder" Assembly="DossierServiceComponent" Type="DossierBuilder" Recurrence="600" Metadata="InvokeDirect=true" />` The value of 600 for Recurrence above means, the "DossierBuilder" service is instantiated every 600 seconds (10 minutes) to perform the job.

Enable Oracle Argus Dossier

1. Go to **Argus Safety** > **Argus Console** > **System Configuration** > **Enabled Modules**.
2. Select **Dossier**.
3. Click **Save**.

18

Install and Configure Axway B2Bi

This chapter describes the steps required to install and configure the Axway B2Bi EDI (Electronic Data Interchange) Gateway so it can operate correctly with Oracle Argus Interchange.

> **Note**
>
> Either Oracle B2B or Axway B2Bi is required for E2B reports exchange. You can choose any one of the software, as required.
>
> You may install EDI Gateway and Interchange Service in any order.

For more information, see:

- Create an Axway B2Bi Database Instance
- Install Axway B2Bi
- Configure Axway B2Bi
- Test Communication

Create an Axway B2Bi Database Instance

1. Log in to the database server as an Admin user.
2. Create a blank Axway B2Bi instance, if it does not already exist.
3. Connect to the Axway B2Bi instance created in Step 2.
4. Create an Axway B2Bi DB User identified by the Axway B2Bi DB password.
5. Provide the following grants to the Axway B2Bi DB user:
   - Grant CREATE PROCEDURE
   - Grant CREATE SESSION
   - Grant CREATE TABLE
   - Grant CREATE VIEW
   - Grant UNLIMITED TABLESPACE (Optional)
   - Grant CREATE SEQUENCE
   - Alter user Axway B2Bi DB User default tablespace USERS.
   - Grant CONNECT
   - Grant RESOURCE

Install Axway B2Bi

For more information, see the *Axway B2Bi installation documentation*.

Configure Axway B2Bi

1. Log in to a client computer.
2. From the browser, go to (Sender or Receiver) http://<*AxwayB2BiServer*>:6080/ui/.
3. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
4. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Recent Communities** > **Manage Trading Configuration** from the menu.
5. In the Pick a community screen, click **Add a community**.
6. In the Choose the source screen:
   a. Click **Next** to continue.
   b. Click the **Manually create a new community profile** option button.
   c. Enter the parameters.
   d. Click **Yes** to add a certificate.

   > **Note**
   >
   > This information is entered for both the sender and the receiver, but initially for the sender.

   e. Click **Finish**.
7. In the Add a certificate screen, click **Create a self-signed certificate** and click **Next**.
8. In the Enter the certificate information screen, click **Next**.
9. In the Review request screen, click **Next**.
10. In the View certificate details screen:
    a. Check **Make this the default encryption certificate**.
    b. Check **Make this the default signing certificate**.
    c. Click **Finish**.
11. Hover over the **Trading Configuration** icon, from the drop-down menu, select the recent **Communities** > <**community**>.
12. In the Summary screen, click the **Setup up a pickup for receiving messages from partners**.
13. In the Choose message protocol screen, select the **EDIINT AS2 (HTTP)** option and click **Next**.
14. In the Choose HTTP transport type screen, click **Next**.
15. In the Configure URL screen, click **Next**.
16. In the Exchange Name screen, enter the **Exchange Name** and click **Finish**.

17. In the Summary screen, click **Application Delivery** and add an application delivery.
18. In the Choose transport protocol screen, select the **File system** option and click **Next**.
19. In the Configure the file system settings screen, click **Next**.
20. In the Exchange Name screen, enter the **Exchange Name** and click **Finish**.
21. Go to the Summary Page and click **Configure the settings for application delivery**.
22. In the Select application delivery screen, select **Name**, enter **Friendly Name**, and click **Finish**.

For more information, see:

- Configure Axway B2Bi for Binary File Transmission
- Configure Axway B2Bi Community
- Add a Node
- Configure Axway B2Bi Certificates
- Configure EVENTS.XML
- Configure Message Processing Settings

Configure Axway B2Bi for Binary File Transmission

1. Log in to a client computer.
2. From the browser, go to (Sender or Receiver): http://<*AxwayB2BiServer*>:6080/ui.
3. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
4. In the Getting Started screen, hover over the **Trading Configuration** icon and from the drop-down menu, select **Recent Communities** > <**community**>.
5. In the Summary screen, click the **Application Pickup** icon and add an application pickup.
6. In the Choose transport protocol screen, click **File system** option and click **Next**.
7. In the From address and To address screens, click **Next**.

   Address must be determined by either message attribute configuration or by protocol address only.
8. In the Configure the file system settings screen, on the Sender's Axway B2Bi Server, locate Common/Out folder and create the following folder structure:
   `Common\Out\Sender's Routing ID\Receiver's Routing ID`
9. In the Exchange Name screen, enter the **Exchange Name** and click **Finish**.
10. In the Change this application pickup exchange screen, click the **Message attributes** tab.
11. In the Message attribute directory mapping tab:
    a. The system moves them to the **Selected attributes** list.
    b. Select **From routing ID** and **To routing ID** and click **Add**.
    c. Locate the **Available Attributes** list.
    d. Click the **From address** tab.
12. Click **To address** tab, select the **Address determined by message attribute configuration** option or by protocol address only and click **Save Changes**.

13. On the Sender's Axway B2Bi Server, locate Common/Out folder and create the following folder structure: `Common\Out\Sender's Routing ID\Receiver's Routing ID`

> **Note**
>
> This completes the folder configuration for outgoing binary transmissions. Since binary file transmission configuration is based on these folder names, each combination of Sender and Receiver Routing ID must be unique for binary file transmission to different trading partners.
>
> The Binary file should be dropped in the RECEIVER's Routing ID Folder which is the last folder. Although in the Axway B2Bi GUI the Application Pickup folder will show up only ..\common\out.

For incoming binary transmissions, repeat steps 5 - 8 for Application Delivery.

Repeat steps 1 - 12 for setting up the Receiver Axway B2Bi.

Configure Axway B2Bi Community

In this section:

Register with the Axway B2Bi Community

1. From the browser, go to http://<*Receiver Axway B2BiServer*>:6080/ui/.
2. In the Axway B2Bi Login screen, enter Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting started screen, hover over the **Trading Configuration** icon and from the drop-down menu, select **Recent Communities** > <**community**>.
4. In the Summary screen, click **Export this community as a partner profile** at the bottom of the page.
5. Enter the password and save the file to your local hard drive and close the Save dialog box.
6. Click **Logout** in the upper right corner of the page.

Add a Partner to the Axway B2Bi Community

1. From the browser, go to http://<*Sender AxwayB2BiServer*>:6080/ui/.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Recent Communities** > <**community**> from the menu.
4. In the Summary screen, click the **Add a Partner to this community** link.
5. In the Choose the source screen, select the **Import the profile information from a file** option and click **Next**.

6. In the Enter profile path screen, click **Browse** to navigate to the saved file, enter the same password used at the time of exporting this community as a partner profile, and click **Finish**.
7. In the Successful profile import screen, click **Close**.

> **Note**
>
> If you receive a summary where the Routing ID is not displayed, you must add the sender's Routing ID manually, as listed from Steps 9 - 12.

8. In the Summary screen:
   a. Click the **Partners** menu item and select the newly imported partner.
   b. Click the **Routing IDs** icon.
9. In the Routing IDs screen:
   a. Click **Add**.
   b. Type the partner (sender) routing ID in the **Routing ID** field.
   c. Verify that the partner **does not** have a routing ID.

      The new routing ID is added to the page.
   d. Hover over the **Trading Configuration** icon.
   e. Select **Recent Communities** > <**community**> from the menu.
10. In the Summary screen, select the sender partner.
11. In the Summary: Sender screen, click the **Default delivery exchange** link.
12. In the Change this delivery exchange screen, click the **HTTP Settings** tab, and verify that the URL is correct and that the correct routing ID for the send is appended to the end of the URL.

Register the Receiver's Community on the Sender Server

Repeat the procedures of the Create an Axway B2Bi Database Instance.

Add a Node

1. From the browser, go to http://<*Sender Axway B2BiServer*>:6080/ui/.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting started screen, click the **System Management** icon.
4. In the System Management screen, click **Add a Trading engine node**.
5. In the Add a node screen:
   a. Click **Add**.
   b. Select the machine to add the node to from the **Computer name** drop-down.
   c. Click the **Trading Engine** option.
6. When the System management page opens with the newly created node: Click **Start** to start the trading engine node.

   The system updates System management page.

The status of the node changes to **Starting**.

The system updates the System management page.

The status of the node changes to **Running**.

7. Click **Home** and verify that the node status is **Running**.
8. Repeat the procedure to set up the Receiver Axway B2Bi.

Configure Axway B2Bi Certificates

In this section:

Configure Receiver Axway B2Bi Certificates

1. From the browser, go to http://<*Receiver Axway B2BiServer*>:6080/ui/.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Manage trading configurations** from the menu.
4. In the Community screen, click the **Community name**.
5. In the Summary screen, click the **Certificates** link.
6. In the Certificate screen, click the **Certificate** listed on the **Personal certificates** tab.

> **Note**
>
> Click the Trusted root certificates tab to verify that no certificates exist for the Sender or Receiver Axway B2Bi.
>
> Skip this section if a valid trusted root certificate already exists in the Name section on the Trusted root certificates tab.

7. In the View certificate screen, in the General tab, locate the **Related task** section and click **Export this certificate**.
8. In the Choose the format you want to use for the certificate export screen, retain the default configurations.
   a. Click **Export certificate**.
   b. Click the **Cryptographic Message Syntax Standard PKCS #7** option button.
   c. Select the **Include all certificates in the certification path if possible** checkbox.
9. Save the file to the Sender's local hard drive and click **Logout** in the upper right corner of the page.

Configure Sender Axway B2Bi Certificates

1. From the browser, go to http://<*Sender Axway B2BiServer*>:6080/ui/.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.

3. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Manage trading configurations** from the menu.
4. In the Community screen, click the **Community name**.
5. In the Summary screen, click the **Certificates** link.
6. In the Certificate screen, click the **Trusted root certificates** tab and click the **Add a trusted root certificate** link.

> **Note**
>
> It is possible that the Trusted Root Certificates for the Receiver Axway B2Bi Server may already be on the Sender Axway B2Bi Server.

7. In the Add a certificate screen, click **Next**.
8. In the Locate the certificate file screen, click **Browse** to locate the P7B certificate file saved for the Receiver Axway B2Bi Server and click **Next**.
9. In the View certificate details screen, click **Finish**.
10. In the Pick a certificate screen, click the **Trusted root certificates** tab.
11. Verify that the certificate you added appears on the list.
12. Log out of the Sender Server.

    Repeat the procedure to register the Sender's certificate on the Receiver Server as a Trusted Root Certificate.

Configure EVENTS.XML

In this section:

Configure Event.xml on client machine

1. Log in to a client computer.
2. Using Windows Explorer, go to the local directory containing the Oracle Argus Safety installation files and navigate to `..\DBInstaller\Utilities\Cyclone`.
3. Locate and double-click the **cyclone_setup.bat** file to open a DOS command prompt window.
4. In the Oracle SQL+ screen:
   a. Enter the Axway B2Bi instance in the **TSNAMES entry**.
   b. Enter the Axway B2Bi DB User Name in the **Axway B2Bi User Name**.
   c. Enter the Axway B2Bi User Password in the **Password for User Axway Synchrony_USER**.
   d. Enter the Axway B2Bi Schema User in the **[USERS]**.
5. When SQL+ connects to the specified database, enter the Directory name and the log file name.

When the process is complete, the SQL+ window and DOS command prompt window close.

Configure Event.xml on receiver machine

1. Log in to the Receiver Server.
2. Using Windows Explorer, navigate to `<Axway B2Bi Install Folder>\conf folder\`.
3. Take a backup of the `Events.xml` file and rename it Events.xml.bak.
4. Right-click the `Events.xml` file and select **Edit** to display it in **Notepad**.
5. Locate the `<EventRouters>` section and add the following code:

```
<EventRouter id="ARGUS Events" class =
"com.cyclonecommerce.relsys.router.GetEventInfo" active="true">
<Parameters file="../logs/ARGUS.log" rollOnStart= "true" autoFlush="true"
maxFileSize="2M" maxBackupFiles="5"/>
<MetadataProcessorListRef ref="Messaging"/>
<EventFilterRef ref="ARGUS"/>
</EventRouter>
```

6. Add the following section in the Events.xml file in the `<EventFilters>` section:

```
<EventFilter id="ARGUS">
<OrFilter>
<EventFilterRef ref="Message Milestones"/>
<EventLevelFilter level="Warning"/>
<EventLevelFilter level="Error"/>
<EventLevelFilter level="High"/>
</OrFilter>
</EventFilter>
```

7. Copy the `ArgusRouter.jar` file from Oracle Argus Safety local directory: `\SUPPORT\AxwayB2Bi\2.6` to Axway B2Bi directory: `<Axway B2Bi Install folder>/b2bi/shared/local_te/jars/`.

> **Note**
>
> Make sure that the `ArgusRouter.jar` available from the previous versions is removed before replacing with new one. There must only be the latest `ArgusRouter.jar` present.
>
> In case Axway Interchange is upgraded to Axway B2Bi, then the old `ArgusRouter.jar` can be found at `<Axway Install Folder>\jars\`.

8. From the browser, go to http://*<Receiver Axway B2BiServer>*:6080/ui/.
9. In the Getting Started screen, hover over the **Trading Configuration** icon and from the drop-down menu select **Recent Communities** > **Community**.
10. In the Summary screen and click the **Application Pickup** icon.
11. In the Application pickup exchange screen, click the link in the **Name** column.
12. Click the **Inline Processing** tab.
13. In the Inline processing rules screen, enter the following parameters:

a. `Class name`—`com.cyclonecommerce.relsys.router.GetMessageInfo`

b. `Parameter`—**Relsys Argus**

c. `Description`–GetMessagesInformation

14. Click **Save changes**.
15. When the Pick an integration pickup exchange screen appears, click **Logout**.
16. Repeat the preceding steps for the Sender Server.

Configure Message Processing Settings

1. From the browser, go to http://<*Sender Axway B2BiServer*>:6080/ui/.
2. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
3. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Recent Communities** > <**community**> from the menu.
4. In the Summary screen, click the **Application Pickup** icon.
5. In the Application pickup exchange screen, click a link in the **Name** column.
6. Click the **Advanced** tab and from **Message processing**, select **Limited - only use message handler and collaboration settings**.
7. In the Getting Started screen, hover over the **Trading Configuration** icon and select **Recent Communities** > <**community**> from the menu.
8. In the Summary screen and click the **Trading Pickup** icon.
9. In the Trading pickup exchange screen, click a link in the **Name** column.
10. Click the **Advanced** tab, and from **Message processing**, select **Limited - only use message handler and collaboration settings**.
11. Go to `<AxwayB2Bi Install folder>\B2Bi`, and execute the following command to stop the server:

    ./B2Bi stop

12. Go to `<AxwayB2Bi Install Folder>\B2Bi`, and execute the following command to start the server:

    ./B2Bi start

13. To verify that the Trading engine node in Running state and the Integration engine node in Started state, and the Trading engine node is assigned to the Integration engine node:

    a. From the browser, go to http://<*Sender Axway B2BiServer*>:6080/ui/

    b. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.

    c. In the Getting started screen, click the **System Management** icon.

> **Note**
>
> If the **Trading engine node** is not in **Running** state then click **Start**.

Test Communication

1. From the Sender Axway B2Bi Server, configure an XML file to transmit from the Sender server to the Receiver server.

   > **Note**
   >
   > The file must be an E2B file that contains the correct routing IDs for the sender and the receiver.

2. Make sure that the Axway B2Bi servers on both sender and receiver are running.
3. Drop the E2B XML file into the out bound folder of the Axway B2Bi Sender server.
4. Log in to a machine where Axway B2Bi is installed.
5. From the browser, go to http://<*Sender Axway B2BiServer*>:6080/ui/.
6. In the Axway B2Bi Login screen, enter the Axway B2Bi User ID and Password, and click **Login**.
7. In the Getting started screen, hover over the **Message Tracker** icon and select the **Message Searches** > **All Messages** from the menu.

   From the Search results screen, verify that the transmission is in progress by locating the Custom Search section and click **Find** until Delivered appears on the screen.

   > **Note**
   >
   > The system does not display this screen if it has already transmitted the file.

8. When the file is transmitted successfully, click **Logout**.
9. Go to the Axway B2Bi Receiver server and verify that the E2B file has been received.
10. To verify that the file has been transmitted:
    a. Log in to the receiver Axway B2Bi server.
    b. Select the All Messages option.
    c. View the message payload.
11. Compare the E2B file on the receiving machine (payload version displayed) with the file from the sending machine.

    These files should be identical.
12. To verify delivery on the Receiver Server, repeat the procedure.

    Verify that the E2B XML file is configured with proper routing IDs for both the send and the receiver before dropping the file into the Axway B2Bi outbound folder.

19

Install and Configure Oracle B2B

You can install either Oracle B2B or Axway B2Bi for E2B reports exchange.

Install Oracle B2B

Refer to *Oracle B2B Installation Guide*.

Integrate Oracle B2B with Oracle Argus Safety

The entire integration process can broadly be categorized under the following steps:

1. Creation of integration tables in Oracle B2B Schema through provided scripts
2. Oracle B2B UI Configuration
    a. General Configuration
    b. Document Configuration
3. Oracle Enterprise Manager Configuration
    a. SOA Composites Deployment
    b. SOA Composites Configuration
4. Web Logic Console Configuration
    a. Data Sources and JNDI Configuration
5. Large Payload Configuration
6. Configuration on Oracle Argus Safety side

Create Integration tables in Oracle B2B Schema

There are a few database objects which are created in the ESM Schema for outbound file integration as part of the Oracle Argus Safety installation. However, a few database objects need to be created in Oracle B2B Schema for inbound files integration.

After Oracle Argus Safety is installed, locate DB Script B2B_setup.bat under *`Argus Install Folder`*`\Oracle\Argus\DBInstaller\Utilities\B2B_Setup\`.

Double-click it to provide database details of Oracle B2B. This is recommended to be installed under SOA_INFRA Schema of Oracle B2B database instance.

This script creates the following database objects required to integrate incoming files data:

1. B2B_ARGUSSAFETY_INBOUND (table)
2. S_B2B_ARGUSSAFETY_INBOUND (sequence)

Configure Oracle B2B User Interface

Log in to Oracle B2B UI as an admin user.

For more information, see:

- General Configuration > Administration > Configuration
- Document Configuration > Administration > Document

General Configuration > Administration > Configuration

1. Under the **Non Purgeable** section, set **Use JMS Queue as default** to **True**.
2. Under the **Miscellaneous** section, set **Additional MIME Types** to **application/octet-stream : application/pdf**.
3. Under the **Performance** section, set **Large Payload Directory** to the desired location.

   It is recommended to set it, even if large payloads are not likely to be received.

Document Configuration > Administration > Document

There can be one document type configured for each of the following categories, as transmitted and received from Oracle Argus Safety:

1. XML—for E2B Message and Acknowledgments
   a. SGML files with no EDI Header and Footer are also categorized under this category.
2. Zip—for PMDA E2B Message files
3. PDF—for E2B R2 Attachments
   a. The Zip and PDF may be combined together under one category since both are binary documents. One common doc type may be sufficient for them.
4. EDI files—for those E2B Reporting Destinations in Oracle Argus Safety Console for which EDI Header and footer is checked. If there is no such Reporting Destination, this document type need not be created. Identification Types for EDI Files can be given as:
   a. Identification Start Position = 1
   b. Identification End Position = 3
   c. Identification Value = UNB

Besides this, XML, EDI, and Binary should be created as separate document types rather than as different document definitions under one document type.

Configure Web Logic Console

Log in to Web Logic Console to create the following data sources and JNDI configuration.

For more information, see:

- Data source with JNDI Name as 'eis/DB/ArgusSafety_Outbound'
- Data source as 'jdbc/ArgusSafety_Inbound'
- Data source with JNDI Name as 'eis/DB/ArgusSafety_Inbound'
- DB Adapters for Data Source

Data source with JNDI Name as 'eis/DB/ArgusSafety_Outbound'

This is hard coded JNDI Identifier being used inside AS_BPEL_Outbound SOA Composite for outbound files. This should point to a data source which has all access to the Oracle Argus Safety database table **B2B_ARGUSSAFETY_OUTBOUND** under ESM Schema. This table is available as part of the Oracle Argus Safety installation.

The configuration is validated with xADataSource property filled with a data source using database driver as 'Oracle's Driver (Thin XA) for instance connection; Version: 9.0.1 and later'.

Data source as 'jdbc/ArgusSafety_Inbound'

This is a hard coded data source being used inside AS_BPEL_Inbound SOA composite for inbound files. This should point to a data source which has access "all access" on the integration database table B2B_ARGUSSAFETY_INBOUND and the sequence S_B2B_ARGUSSAFETY_INBOUND. These are created as part of the script.

Besides, the same data source can be used as an underlying data source under the following:

The configuration is validated with database driver chosen as "Oracle's Driver (Thin XA) for instance connection; Version:9.0.1 and later".

Data source with JNDI Name as 'eis/DB/ArgusSafety_Inbound'

This is hard coded JNDI Identifier being used inside sca_AS_BPEL_Inbound_rev1.0.jar for inbound files. This should point to a data source which has access "all access" on the Oracle B2B database table B2B_ARGUSSAFETY_INBOUND and for Sequence S_B2B_ARGUSSAFETY_INBOUND created under the step above "Creation of integration tables in B2B Schema".

The data source created in the above section "jdbc/ArgusSafety_Inbound" can be used as a data source here.

The configuration is validated with xADataSource property filled with a data source using database driver as "Oracle's Driver (Thin XA) for instance connection; Version: 9.0.1 and later".

DB Adapters for Data Source

Navigate to **Deployments** > **Summary of Deployments** > **DbAdapter** > **Configuration** > **Outbound Connection Pools**, and verify that the DB Adapters are present for the data sources created in the previous sections.

Make sure that the data source name (JNDI Name) has been configured in the property 'XADataSourceName'. If not present, then create a data source with the name '`eis/DB/ArgusSafety_Outbound`' and '`eis/DB/ArgusSafety_Inbound`' respectively for the corresponding data sources name populated in 'XADataSourceName'.

Configure Oracle Enterprise Manager

In this section:

Deploy SOA Composite

The Oracle Argus Safety build provide the following composites to integrate Oracle B2B:

- **sca_AS_BPEL_Outbound_rev1.0.jar**—for all outbound traffic from Consolidated Intake
- **sca_AS_BPEL_Inbound_rev1.0.jar**—for all inbound traffic from Oracle Argus Safety

The files are available in *`Install Directory`*`\Support\OracleB2B`.

To deploy SOA composites:

1. Log in to Oracle Enterprise Manager as Admin user.
2. Locate the domain under which composites are to be deployed.
3. Right-click and select **SOA Deployment** > **Deploy To This Partition**.
4. To deploy the **sca_AS_BPEL_Outbound_rev1.0.jar** file, under the `Archive or Exploded Directory > Archive is on the machine where this web browser is running`, select the `sca_AS_BPEL_Outbound_rev1.0.jar` file, and click **Next**.
5. To deploy the **sca_AS_BPEL_Inbound_rev1.0.jar**, under the `Archive or Exploded Directory > Archive is on the machine where this web browser is running`, select the `sca_AS_BPEL_Inbound_rev1.0.jar` file and under the `Configuration Plan > Configuration plan is on the machine where this web browser is running`, select the `AS_BPEL_Inbound_cfgplan.xml` file, and click **Next**.
6. Repeat the above process to deploy the other JAR file.

Configure SOA Composite

There are certain parameters for the deployed composites which need to be modified as per the Customer Environment.

For more information, see:

AS_BPEL_Outbound Composite

1. In the Oracle Enterprise Manager, under deployed domain, right-click **AS_BPEL_Outbound** and click **Service/Reference Properties**.
2. Select **AS_FileAdapter**.
   a. Change PhysicalDirectory and PhysicalArchiveDirectory to the desired location.

      Do not change other properties.

b. Oracle Argus Safety may create outbound files under the same or under any of the child directories of the above specified directory.

3. B2B_DBAdapter should NOT be changed for any of the properties.
4. B2B_JMSAdapter can be changed, but only if required.

AS_BPEL_Inbound Composite

In the Oracle Enterprise Manager, under deployed domain, right-click **AS_BPEL_Inbound** and click **Service/Reference Properties**.

1. Select **AS_FileAdapter**.
   - Set PhysicalDirectory as the top level folder under which all the incoming files are dropped by Oracle B2B.

     Do not change other properties.
2. Select **LargeFileReader**.
   - The PhysicalDirectory should be the same as Large Payload Directory under Oracle B2B UI > Administration > Configuration > Performance section.

     Do not change other properties.
3. B2B_DBAdapter should NOT be changed for any of the properties.
4. B2B_Inbound can be changed, but only if required.

Configure Large Payload Exchange

For Oracle B2B, a large payload is a file bigger than the configured size in **Oracle B2B UI** > **Administration** > **Configuration** > **Performance** section.

Oracle Argus Safety can send large files if E2B R2 Attachments are configured or E2B R3 or eVAERS files are exchanged. With other scenarios, generally, large payloads may not be applicable.

For more information, see:

- Outbound Files
- Inbound Files
- Transaction Time
- General Oracle B2B Settings for Large Payloads

Outbound Files

Select **Trading Partner** > **Channel** > **Channel Attributes** > **Ack Mode to be Async**.

This configuration is good even if large payloads are not supposed to be exchanged.

Inbound Files

1. Log in to the Oracle Enterprise Manager.
2. Go to **SOA** > **(Domain)** > **SOA Administration** > **B2B Server Properties**.
3. On the right side, under the Operation tab, click **addProperty** to add a new property called **b2b.setisLargePayloadPropertyForSmallMsg** with value as **True**.

4. The Large Payload Directory configuration should be the same for Oracle B2B Web UI > Administration > Configuration > Performance section, and also for Oracle Enterprise Manager > SOA > (Domain) > AS_BPEL_INBOUND > LargeFileReader PhysicalDirectory property.

Both these configurations are required, even if large payloads are not expected to be exchanged.

Transaction Time

Log in to Web Logic Console > (Domain) > Services > JTA > Timeout Seconds. Set the time to 720 seconds to allow processing of large pay loads. This has been tested with 20 MB files.

This may have to be tuned if transaction time-out errors occur for the same size or larger size files.

General Oracle B2B Settings for Large Payloads

If required, go through other general Oracle B2B configuration for large payload, available with Oracle B2B documentation.

Configurations for Oracle Argus Safety

In this section:

Configure Oracle B2B

1. Log in to ESM Mapping Utility as an ESM Admin user.
2. Go to **Administrator Menu** > **Setup INI file** > **EDI Section**.
3. Select Oracle B2B as the EDI Gateway.

   The Oracle B2B database details should be provided for a User who has all access on the following:

   - B2B_ARGUSSAFETY_INBOUND table (all access)
   - B2B_INSTANCEMESSAGE table (read access)

Update for Oracle B2B Documents

Manually update document in the Oracle Argus Safety database table **B2B_ARGUSSAFETY_DOC** under ESM Schema as mentioned in Oracle B2B UI > Configuration > Document.

The following table list the sample factory data:

Doc_ID	Doc_Type	Doc_Revision	Comments (Not a column)
1	AS_XmlDoc	ArgusSafety_1.0	Xml for E2B Message and Acknowledgments

Doc_ID	Doc_Type	Doc_Revision	Comments (Not a column)
2	AS_BinaryDoc	ArgusSafety_1.0	Zip for PMDA E2B Message files
3	AS_BinaryDoc	ArgusSafety_1.0	PDF for E2B Attachments
4	AS_EDIDoc	ArgusSafety_1.0	EDI files

- The Admin should update only Doc_Type and Doc_Revision columns from Oracle B2B UI.
- The Doc ID column must not be updated as new Doc ID is not supported.
- the mapping between Doc ID and other columns is assumed to be exactly as provided in the sample above. For example:
  - Doc_ID = 1 should not point to Binary Docs.
  - Doc ID = 2 and Doc ID = 3 can point to the same or different doc type and doc version but neither of these should be left blank.
  - Doc_ID=4 may be left blank, if there is no Reporting Destination with EDI Header and Footer configuration.

This information is picked up by outbound SOA Composite at run time to dynamically attach Document Type and Document Version properties to outgoing file via JMS.

Argus Console > Reporting Destination Code List

The Company Identifier under EDI Tab should contain Name Identifier as configured in Oracle B2B UI > Partners > Trading Partner > Profile > Identifier.

20

Configure Oracle Analytics Server or Oracle Analytics Publisher

The Oracle Analytics Server or Oracle Analytics Publisher is needed when Flexible Aggregate Reporting (FAR) or Japanese PMDA R3 Paper Forms is generated through Oracle Argus Safety. This chapter elaborates the steps needed to integrate the Oracle Analytics Server or Oracle Analytics Publisher with Oracle Argus Safety.

In the Oracle Argus Safety Enterprise Edition, Oracle Analytics Server or Oracle Analytics Publisher is also required for Oracle Argus Analytics and Oracle Analytics reporting on Oracle Argus Mart.

Prepare Oracle Analytics Publisher

To execute PMDA R3 Paper Forms or Oracle Analytics Publisher Periodic Reports, or a standalone Oracle Analytics Publisher on an Oracle Analytics Server must be prepared.

> **Note**
>
> Oracle Analytics Publisher Standalone Server is applicable only for the Oracle Argus Safety Standard Edition users. The Oracle Argus Safety Enterprise Edition users must install Oracle Analytics Server integrated with Oracle Analytics Publisher only.

When the Oracle Analytics Publisher /Oracle Analytics Server is successfully installed, make a note of:

- TNS Names details of the database where Oracle Analytics Publisher repository is created
- Oracle Analytics Platform User ID and Password
- Oracle Analytics Publisher Console login credentials
- Oracle Analytics Publisher Console URL along with the Port Number

Set Up Oracle Analytics Publisher for Oracle Argus Safety

In this section:

Enable a Local Superuser

Oracle Analytics Publisher enables you to define an administration Superuser. Using the Superuser credentials you can directly access the Oracle Analytics Publisher administrative functions without logging in through the defined security model. Set up this Superuser to ensure access to all administrative functions in case of failures with the configured security model. It is highly recommended that you set up a Superuser.

To enable a local superuser:

1. Click **Administration**.
2. Under **Security Center**, click **Security Configuration**.
3. Under Local Superuser, select the **Enable Local Superuser** checkbox and enter the credentials.
4. Restart the Oracle Analytics Publisher service.

Create a Database Connection

To establish a database connection with the Oracle Argus Safety database, create a new JDBC connection named **asbip** in the Oracle Analytics Publisher.

> **Note**
>
> It is recommended to provide the JDBC connection name, user name and database connection information in the lower case.

1. Log in to Oracle Analytics Publisher using the administrator credentials. This displays the Oracle Analytics Publisher Home Page.
2. Click **Administration**.
3. Click **JDBC Connection** under **Data Sources**.

   This displays the Data Sources screen.
4. Click **Add Data Source**.
5. In the **Add Data Source** section:
   a. Enter `asbip` in the **Data Source Name** field.

      Make sure that you enter this data source name in lowercase only.
   b. Select the database from the **Driver Type** drop-down.

This auto-populates the **Database Driver Class** field.

c. Enter either of the following connection strings in the **Connection String** field.

- `url="jdbc:oracle:thin:@[host]:[port]/[sid]"`
- `url="jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=host.com)(PORT=<port number>)))(CONNECT_DATA=(SID=orcl)))"`

d. Enter the Oracle Argus Safety Oracle Analytics Publisher schema username (for example, bip_owner) and the password.

This user is created as part of the Oracle Argus Safety database installation.

e. Click **Test Connection**.

If successful, this displays a confirmation message.

6. Click **Apply**. This displays the `asbip` Data Source in the list of already existing data source names.

This successfully creates a connection between Oracle Analytics Publisher and the Oracle Argus Safety database.

Set Up Runtime Oracle Analytics Publisher Time-out

1. Log in to Oracle Analytics Publisher.
2. Click **Administration**.
3. From Runtime Configuration section, click **Properties**.
4. Modify the following parameter values to **5000** seconds from 600 seconds:
   - Memory Guard > Process timeout for online report formatting
   - Data Model > SQL Query Timeout
5. Click on **Apply**.

These values can be increased as needed, for any Oracle Analytics Publisher custom reports that take longer to complete.

Configure Oracle Fusion Middleware Security Model

> **Note**
>
> If you are using the Oracle Analytics Publisher Security model, it is recommended to move to Oracle Fusion Middleware Security model.
>
> When moving from Oracle Analytics Publisher Security model, you must re-create the users, roles and policies through the Oracle Enterprise Manager.

Manage Users and Roles

In this section:

- Create Application Policies and Set Up Folder Privileges (Oracle Analytics Publisher Standalone only)
- Create Application Policies and Set Up Folder Privileges (Oracle Analytics Server and Oracle Analytics Integrated Installation only)

Configure Users, Groups and Roles

This section describes the steps to create users, groups and roles in Oracle Fusion Middleware Security model (recommended security model).

For more information, see:

- Create a Group
- Create a User
- Create an Application Role

Create a Group

> **Note**
>
> For detailed information, refer to Oracle Healthcare Translational Research Installation Guide, section Create Oracle Analytics Server groups and users.

1. Log in to Oracle Fusion Middleware Enterprise Manager.
2. Navigate to **WebLogic Domain** > **Security** > **Security Realms** > **myrealm** > **Users and Groups**.
3. From the Groups section, click **New**.

   The Create a New Group dialog box appears.
4. Create the following groups for Flexible Aggregate Reports by entering the **Name** and **Description**:
   - FARAdminGroup
   - FARSafetyAuthorGroup
   - FARSafetyConsumerGroup
5. Create the following groups for Expedited Reports by entering the **Name** and **Description**:
   - EXPAdminGroup
   - EXPSafetyAuthorGroup
   - EXPSafetyConsumerGroup

Create a User

1. Log in to Oracle Fusion Middleware Enterprise Manager.
2. Navigate to **WebLogic Domain** > **Security** > **Security Realms** > **myrealm** > **Users and Groups** >.
3. From the Users section, click **New**.

   The Create a New User screen appears.

4. Enter the parameters and click **OK**.
5. Assign a group to the user and click **Save**.

Create an Application Role

1. Log in to Oracle Fusion Middleware Control Enterprise Manager.
2. Go to **WebLogic Domain** > **Security** > **Application Roles**.

   The Application Roles dialog box appears.
3. From the **Application Stripe** drop-down, select **OBI** and click **Search**  .

   The default Role available in clean slate installation appears.
4. Click **Create**.

   The Create Application Role dialog box appears.
5. In the **Role Name** field, enter **FARAdminRole**.
6. From the Members section, click **+Add**.

   The Add Principal dialog box appears.
7. From the **Type** drop-down, select **Group** and click **Search**.

   A list of principals appears.
8. From the list of Searched Principals, select **FARAdminGroup** and click **OK**.
9. From the Members section, click **+Add**.

   The Add Principal dialog box appears.
10. From the **Type** drop-down, select **User** and click **Search**.

    A list of principals appears.
11. From the list, search Users, select **Weblogic** and click **OK.**
12. Repeat from Step 4 to Step 11 to create other FAR and Expedited Reports role and add Member to these roles as listed in the table below.

    Besides, make sure to add EXP Roles only for Expedited Reports (and not the FAR roles).

Role	Application Roles
FARAdminRole	FARAdminGroup
--	Weblogic
FARSafetyAuthorRole	FARSafety AuthorGroup
--	FARAdminGroup
FARSafetyConsumerRole	FARSafetyConsumerGroup
--	FARSafetyAuthorGroup
--	FARAdminGroup
EXPAdminRole	EXPAdminGroup
--	Weblogic
EXPSafety Author Role	EXPSafetyAuthorGroup
--	EXPAdminGroup
EXPSafety Consumer Role	EXPSafetyConsumerGroup

Role	Application Roles
--	EXPSafetyAuthorGroup
--	EXPAdminGroup

> **Note**
>
> For more details, refer to Oracle Analytics Managing Security for Oracle Analytics Server guide, section Manage Application Roles.

Create Application Policies and Set Up Folder Privileges (Oracle Analytics Publisher Standalone only)

For information, see:

- Create Application Policies
- Manage Folder Privileges

Create Application Policies

1. Log in to Oracle Fusion Middleware Control Enterprise Manager.
2. Go to **WebLogic Domain** > **Security** > **Application Policies**.

   The Application Policies screen appears.
3. To create a new application policy, click **Create**.

   The Create Application Grant dialog box appears.
4. From the Grantee section, click **+Add**.

   The Add Principal dialog box appears.
5. From the **Type** drop-down, select **Application Role** and click **Search**.
6. From the list of Searched Principals, select **FARAdminRole** and click **OK**.
7. From the Permissions section, click **+Add**.

   The Add Permission dialog box appears.
8. Select the **Resource Types** radio button.
9. From the **Resource Type** drop-down, select **oracle.bi.publisher.permission** and click **Search**.
10. From the Search Results, select **oracle.bi.publisher.permission** (Oracle Analytics Publisher Administer Server) and click **Continue**.

    The Add Permission dialog box appears.
11. For **Permission Actions**, select **All** (_all_) and click **Select**.
12. Add Resource Name as `oracle.bi.user` with **Impersonate** permission.

    The new FAR Admin policy has all the permissions.

> **Note**
>
> Make sure all the fields are either selected or entered manually.

13. Repeat from Step 4 to Step 12, to add the following:

Policy Name/Principal	Resource Type	Resource Name	Permission Actions
FARAdminRole	oracle.bi.user	oracle.bi.user	impersonate
--	oracle.bi.publisher.permission	oracle.bi.publisher.administerServer	_all_
FARSafetyAuthorRole	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
FARConsumerRole	oracle.bi.publisher.permission	oracle.bi.publisher.accessExcelReportAnalyzer	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.accessReportOutput	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.accessOnlineReportAnalyzer	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.scheduleReport	_all_

14. Similarly, create roles and policies for Expedited Reports for the following groups:
    - EXPAdminRole
    - EXPSafetyAuthorRole
    - EXPSafetyConsumerRole

> **Note**
>
> For more details, refer to *Section 2.8.3.2 Creating Application Policies Using Fusion Middleware Control* from https://docs.oracle.com/middleware/1221/bip/BIPAD.pdf

Manage Folder Privileges

To set Catalog Folder-level permissions:

1. Log in to Oracle Analytics Publisher application as a privileged user.

   For example, log in to http://<*hostname.domainname*>:<*port*>/xmlpserver, as WebLogic.
2. Go to **Catalog** > **Shared Folders** > **Argus Safety** > **Tasks** > **Permissions**.

   The Permissions dialog box appears.
3. Set the Permissions as follows and click **OK**.

Accounts	Permissions
FAR Admin Role	Write, Delete, Run Report Online, Schedule Report, View Report Output
FAR Safety Consumer Role	Read, Run Report Online
FAR Safety Author Role	Read, Write, Delete, Run Report Online, Schedule Report, View Report Output

> **Note**
>
> Make sure to select the **Apply permissions** option for the items within this folder.

4. Go to **Catalog** > **Shared folders** > **AS_Expedited** > **Tasks** > **Permissions**.

   The Permissions dialog box appears.

5. Set the Permissions as follows and click **OK**.

Accounts	Permissions
EXP Admin Role	Write, Delete, Run Report Online, Schedule Report, View Report Output
EXP Safety Consumer Role	Read, Run Report Online
EXP Safety Author Role	Read, Write, Delete, Run Report Online, Schedule Report, View Report Output

> **Note**
>
> Make sure to select the **Apply permissions** option for the items within this folder.

6. To add the Data Sources to Roles in Oracle Analytics Publisher:
   a. Log in to the Oracle Analytics Publisher with Administrator credentials.
   b. Go to **Administration** > **Roles and Permissions**.

      The Roles and Permissions screen appears.
   c. From the list of roles, select **FARAdminRole** and click the corresponding **Add Data Sources** icon.

      The Add Data Sources screen appears.
   d. From the Available Data Sources section, select **asbip** and click the **Move (>)** icon to move the **asbip** data source to the Allowed Data Sources section.
   e. Click **Apply**.
   f. Repeat the steps to add **asbip** data source for the following roles as well:

      - FARSafetyAuthorRole,
      - FARSafetyConsumerRole,
      - EXPAdminRole,
      - EXPSafetyAuthorRole
      - EXPSafetyConsumerRole

Create Application Policies and Set Up Folder Privileges (Oracle Analytics Server and Oracle Analytics Integrated Installation only)

For information, see:

- Create Application Policies
- Manage Folder Privileges

Create Application Policies

1. Log in to Oracle Fusion Middleware Control Enterprise Manager.
2. Go to **WebLogic Domain** > **Security** > **Application Policies**.
   The Application Policies screen appears.
3. From the **Application Stripe** drop-down, select **OBI**.
4. Click **Create**.
   The Create Application Grant dialog box appears.
5. From the Grantee section, click **+Add**.
   The Add Principal dialog box appears.
6. From the **Type** drop-down, select **Application Role** and click **Search**.
7. From the list of Searched Principals, select **FARAdminRole** and click **OK**.
8. From the Permissions section, click **+Add.**

   The Add Permission dialog box appears.
9. Select the **Resource Types** radio button.
10. From the **Resource Type** drop-down, select **<Resource Type>** and click **Search**.
11. From the Search Results, select **<Resource Name>** and click **Continue**.

    The Add Permission dialog box appears.

> **Note**
>
> If the Resource Name field is blank, enter it manually.
>
> For Principal, Resource Type, and Resource Name, see Table 20-1.

12. For **Permission Actions**, select **All** (_all_) and click **Select**.
13. When all the permissions are added, click **OK**.
14. Repeat Steps 5-13 for other principals and their permissions. (See Table 20-1)

Table 20-1 List of Policies and their Permissions

Policy Name/ Principal	Resource Type	Resource Name	Permission Actions
FARAdminRole/ EXPAdminRole	oracle.bi.catalog	*	manage

Table 20-1 (Cont.) List of Policies and their Permissions

Policy Name/ Principal	Resource Type	Resource Name	Permission Actions
--	oracle.bi.server.permission	oracle.bi.server.manageRepositories	_all_
--	oracle.bi.presentation.catalogmanager.permission	oracle.bi.presentation.catalogmanager.manageCatalog	_all_
--	oracle.bi.delivers.job	oracle.bi.delivers.job	manage
--	oracle.bi.publisher.permission	oracle.bi.publisher.administerServer	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
--	oracle.bi.repository	oracle.bi.repository	manage
--	oracle.bi.scheduler.permission	oracle.bi.scheduler.manageJobs	_all_
FARSafetyAuthorRole / EXPSafetyAuthorRole	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
--	oracle.bi.tech.visualanalyzer.permission	oracle.bi.tech.visualanalyzer.generalAccess	_all_
--	oracle.bi.delivers.job	*	schedule
FARSafetyConsumerRole/ EXPSafetyConsumerRole	oracle.bi.publisher.permission	oracle.bi.publisher.scheduleReport	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.runReportOnline	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.accessReportOutput	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.accessOnlineReportAnalyzer	_all_
--	ESSMetadataPermission	oracle.bip.ess.JobDefinition.EssBipJob	Read,Execute
--	oracle.bi.publisher.permission	oracle.bi.publisher.accessExcelReportAnalyzer	_all_

Manage Folder Privileges

1. Log in to the Oracle Analytics Server application as a privileged user.

   For example: Log in to *http://acme.oracle.com:port/analytics* with WebLogic user credentials.
2. Go to **Administration** > **Security** > **Manage Privileges**.
3. Add the following Catalog Roles:

> **Note**
>
> Do not remove any existing privileges, only append the additional privileges.

Component	Privilege	Default Role Granted
Access	Access to Dashboards	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Answers	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Oracle Analytics Composer	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Delivers	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Briefing Books	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Mobile	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Administration	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Access	Access to Segments	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Segment Trees	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to List Formats	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Metadata Dictionary	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Access	Access to Oracle Analytics for Microsoft Office	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Oracle Analytics Client Installer	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Catalog Preview Pane UI	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Access	Access to Export	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role

Component	Privilege	Default Role Granted
Actions	Create Navigate Actions	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Actions	Create Invoke Actions	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Actions	Save Actions containing embedded HTML	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: Catalog	Change Permissions	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Admin: Catalog	Toggle Maintenance Mode	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Manage Sessions	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Create Dashboards	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Admin: General	See sessions IDs	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Change Log Configuration	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Issue SQL Directly	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	View System Information	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Performance Monitor	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Manage Agent Sessions	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Manage Device Types	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Manage Map Data	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	See privileged errors	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	See SQL issued in errors	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role

Component	Privilege	Default Role Granted
Admin: General	Manage Global Variables	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: General	Diagnose Oracle Analytics Server Query	Denied: Authenticated User
Admin: Security	Manage Catalog Accounts	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: Security	Manage Privileges	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: Security	Set Ownership of Catalog Objects	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Admin: Security	User Population - Can List Users	Oracle Analytics Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role
Admin: Security	User Population - Can List Application Roles	Oracle Analytics Service Administrator, BI System, EXP Safety Consumer Role, FAR Safety Consumer Role,
Admin: Security	Access to Permissions Dialog	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Briefing Book	Add To or Edit a Briefing Book	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Briefing Book	Download Briefing Book	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Briefing Book	Add to Snapshot Briefing Book	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Catalog	Personal Storage (My Folders and My Dashboard)	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Catalog	Reload Metadata	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Catalog	See Hidden Items	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Catalog	Create Folders	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Catalog	Archive Catalog	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Catalog	Unarchive Catalog	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role

Component	Privilege	Default Role Granted
Catalog	Upload Files	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Catalog	Perform Global Search	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Conditions	Create Conditions	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Dashboards	Save Customizations	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Dashboards	Assign Default Customizations	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Dashboards	Create Bookmark Links	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Dashboards	Create Prompted Links	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Dashboards	Export Entire Dashboard To Excel	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Dashboards	Export Single Dashboard Page To Excel	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Formatting	Save System-Wide Column Formats	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Home and Header	Access Home Page	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Access Catalog UI	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Access Catalog Search UI	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Open Menu	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	New Menu	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Help Menu	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Dashboards Menu	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role

Component	Privilege	Default Role Granted
Home and Header	Favorites Menu	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	My Account Link	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Custom Links	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Home and Header	Access Administration Menu	Denied: Authenticated User
Home and Header	Access User & Role Admin	Denied: Authenticated User
Home and Header	Access Modeler	Denied: Authenticated User
My Account	Access to My Account	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
My Account	Change Preferences	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
My Account	Change Delivery Options	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Answers	Create Views	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Create Prompts	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Access Advanced Tab	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Edit Column Formulas	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Save Content with HTML Markup	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Answers	Enter XML and Logical SQL	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Edit Direct Database Analysis	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Answers	Create Analysis From Simple SQL	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Answers	Create Advanced Filters and Set Operations	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Save Filters	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role

Component	Privilege	Default Role Granted
Answers	Save Column	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Add EVALUATE_PREDICATE Function	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Answers	Execute Direct Database Analysis	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Answers	Upload Images	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Delivers	Create Agents	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Delivers	Publish Agents for Subscription	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Delivers	Deliver Agents to Specific or Dynamically Determined Users	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Delivers	Chain Agents	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Delivers	Modify Current Subscriptions for Agents	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
RSS Feeds	Access to RSS Feeds	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Mobile	Enable Local Content	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
Mobile	Enable Search	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access SOAP	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Impersonate as system user	Oracle Analytics System
SOAP	Access MetadataService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access MsgdbService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access ReportEditingService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role

Component	Privilege	Default Role Granted
SOAP	Access ConditionEvaluationService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access SecurityService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access Tenant Information	Oracle Analytics System
SOAP	Access SchedulerService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access DashboardService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access JobManagementService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access CatalogIndexingService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access UserPersonalizationService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access AnalysisExportViewsService Service	Oracle Analytics Service Administrator, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access CatalogService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access AdministrationSOAPService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access HtmlViewService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access XmlGenerationService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role
SOAP	Access IBotService Service	Oracle Analytics Service Administrator, Oracle Analytics System, EXP Safety Consumer Role, FAR Safety Consumer Role

Component	Privilege	Default Role Granted
View Canvas	Add/Edit Canvas View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Column Selector	Add/Edit Column Selector View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Compound Layout	Add/Edit Compound Layout View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Contribution Wheel	Add/Edit Contribution Wheel View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Graph	Add/Edit Graph View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Funnel	Add/Edit Funnel View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Gauge	Add/Edit Gauge View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Micro Chart	Add/Edit Micro Chart View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Filters	Add/Edit Filters View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Dashboard Prompt	Add/Edit Dashboard Prompt View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Performance Tile	Add/Edit Performance Tile View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Heat Matrix	Add/Edit Heat Matrix View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Static Text	Add/Edit Static Text View	BI Oracle Analytics Administrator, EXP Safety Author Role, FAR Safety Author Role
View Javascript view	Edit Javascript View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Legend	Add/Edit Legend View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Map	Add/Edit Map View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Narrative	Add/Edit Narrative View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role

Component	Privilege	Default Role Granted
View No Results	Add/Edit No Results View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Pivot Table	Add/Edit Pivot Table View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Generic Plugin View	Add/Edit Generic Plugin View View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Report Prompt	Add/Edit Report Prompt View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Create Segment	Add/Edit Create Segment View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Selection Steps	Add/Edit Selection Steps View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Logical SQL	Add/Edit Logical SQL View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Table	Add/Edit Table View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Create Target List	Add/Edit Create Target List View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Ticker	Add/Edit Ticker View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Title	Add/Edit Title View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Treemap	Add/Edit Treemap View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View Trellis	Add/Edit Trellis View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
View View Selector	Add/Edit View Selector View	Oracle Analytics Service Administrator, EXP Safety Author Role, FAR Safety Author Role
Write Back	Manage Write Back	Oracle Analytics Service Administrator, EXP Administrator Role, FAR Administrator Role
Write Back	Write Back to Database	Denied: Authenticated User

4. To set Catalog Folder-level Permissions:
   a. Log in to Oracle Argus Analytics with WebLogic user credentials.

      For example, Log in to *http://acme.oracle.com:port/analytics*.

   b. Go to **Catalog** > **Shared Folders** > **Tasks** > **Permissions**.

The Permissions dialog box appears.

c. To set the permissions, select **Apply Permissions** to sub-folders, select **Permission to items within folder**, and click **OK**.

Accounts	Permissions
FAR Administrator Role/EXP Administrator Role	Full Control
FAR Safety Author Role/EXP Safety Author Role	Full Control
FAR Safety Consumer Role/EXP Safety Consumer Role	Open (Read, and Traverse)
BI Service Administrator (Owner)	Full Control

5. To add the Data Sources to Roles in Oracle Analytics Publisher:
   a. Log in to the Oracle Analytics Publisher with Administrator credentials.

      The Oracle Analytics Publisher home page appears.

   b. Go to **Administration** > **Roles and Permissions**.

      The Roles and Permissions screen appears.

   c. From the list of roles, select **FARAdminRole** and click the corresponding **Add Data Sources** icon.

      The Add Data Sources screen appears.

   d. From the Available Data Sources section, select **asbip** and click the **Move (>)** icon to move the **asbip** data source to the Allowed Data Sources section.

   e. Click **Apply**.

   f. Repeat the steps to add **asbip** data source for the following roles as well:

      - FARSafetyAuthorRole

      - FARSafetyConsumerRole

      - EXPAdminRole

      - EXPSafetyAuthorRole- EXPSafetyConsumerRole

Upload Oracle Analytics Publisher Reports

For information, see:

- Flexible Aggregate Reports
- PMDA R3 Paper Reports

Flexible Aggregate Reports

To upload the Argus Safety.xdrz file to Oracle Analytics Publisher execute the following steps:

1. Copy the Argus Safety.xdrz file from the following location on the Argus Safety Web Server to the local file system: `<Argus Install Media>\SUPPORT\BIP`
2. Log in to Oracle Analytics Publisher using Oracle Analytics Admin User credentials.

3. From the left pane, click **Catalog**.

   This displays the Catalog screen with the **Folders** and **Tasks** sections.
4. Click **Shared Folders** under **Folders**.
5. Click **Upload** under **Tasks**.

   This displays the Upload dialog box.
6. Click **Browse** and navigate to the location where you have saved the **Argus Safety.xdrz** file on the local file system.
7. Click **Upload**. When done, an **Argus Safety** folder is created in **Shared Folders**.
8. Expand the **Argus Safety** folder to verify whether the data model and reports are present.

To set permissions for Oracle Argus Safety Shared Folders:

1. Log in to Oracle Argus Analytics.
2. Go to **Shared folders** > **Argus Safety** > **Tasks** > **Permissions**.

   The Permissions dialog box appears.
3. To set the permissions, select **Apply Permissions** to sub-folders, select **Permission to items within folder**, and click **OK**.

Accounts	Permissions
FAR Administrator Role/EXP Administrator Role	Full Control
FAR Safety Author Role/EXP Safety Author Role	Full Control
FAR Safety Consumer Role/EXP Safety Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
Oracle Analytics Service Administrator (Owner)	Full Control

PMDA R3 Paper Reports

For the Expedited Reports, log in to Oracle Analytics Publisher with Oracle WebLogic Server user credentials, and upload the `AS_Expedited.xdrz` file.

The steps to upload the file remains the same as Flexible Aggregate Reports.

Integrate Oracle Argus Safety with Oracle Analytics Publisher

For information, see:

- Configure AG Service
- Configure Web Service (Expedited Reports only)
- Add AG Service user to Oracle Analytics Publisher (Expedited Reports only)
- Update SSO Exclusion List

Configure AG Service

1. Log in to the server that hosts the AGService and the Batch Periodic Reports process.

2. Navigate to the ArgusInstallPath in the filesystem.
3. Open the file `AGProc.exe.config` for editing.
4. Navigate to the <*system.serviceModel*> tag in this file.
5. In the endpoint element that lies within the client element, enter the following text in the Address attribute:

   http://<host>:<port>/xmlpserver/services/v2/SecurityService where the *name* attribute is set to *SecurityService*

   http://<host>:<port>/xmlpserver/services/v2/ScheduleService where the *name* attribute is set to *SchedulingService*

   http://<host>:<port>/xmlpserver/services/v2/ReportService where the *name* attribute is set to *ReportService*

   In the above instances, <host> refers to the IP address or the Fully Qualified Domain name of the Oracle Analytics Publisher and <port> refers to the Oracle Analytics Publisher port number.

   If the Oracle Analytics Publisher has been configured over an Oracle Access Manager/SSO controlled port, then that port number to be used here.

Configure Web Service (Expedited Reports only)

1. Log in to the Oracle Argus Safety Web Server.
2. Navigate to the ArgusInstallPath in the filesystem.
3. Open the file `Argusvr2.exe.config` for editing.
4. Navigate to the <*system.serviceModel*> tag in this file.
5. In the endpoint element that lies within the client element, enter the following text in the Address attribute:

   http://<host>:<port>/xmlpserver/services/v2/SecurityService where the *name* attribute is set to *SecurityService*

   http://<host>:<port>/xmlpserver/services/v2/ScheduleService where the *name* attribute is set to *SchedulingService*

   http://<host>:<port>/xmlpserver/services/v2/ReportService where the *name* attribute is set to *ReportService*

   In the above instances, <host> refers to the IP address or the Fully Qualified Domain name of the Oracle Analytics Publisher and <port> refers to the Oracle Analytics Publisher port number.

   If the Oracle Analytics Publisher has been configured over an Oracle Access Manager/SSO controlled port, then that port number to be used here.

Add AG Service user to Oracle Analytics Publisher (Expedited Reports only)

This section is applicable for Expedited Reports only.

To auto-schedule the Expedited Reports through AG Services:

1. Navigate to the Oracle Argus Safety Transaction Server.
2. Open the AG Proc and note down the AG Service user, which is used for Batch Report Generation Service.

3. Create the same user (AG Service user) in the Oracle Analytics Publisher.

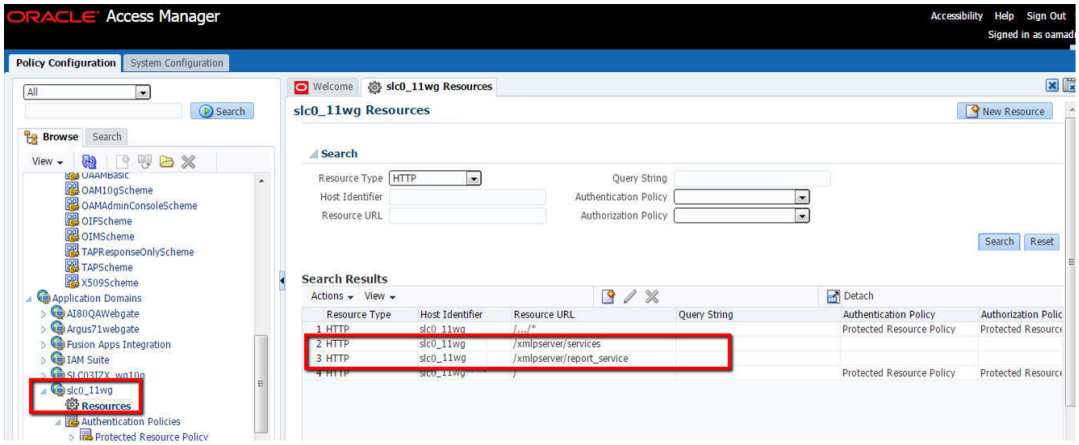
Update SSO Exclusion List

If SSO is enabled, exclude the following URLs from SSO:

- *http://<host>:<port>/xmlpserver/services/v2/ScheduleService* where the *name* attribute is set to *SchedulingService*
- *http://<host>:<port>/xmlpserver/services/v2/SecurityService* where the *name* attribute is set to *SecurityService*
- *http://<host>:<port>/xmlpserver/services/v2/ReportService* where the *name* attribute is set to *ReportService*

If Oracle Access Manager is the SSO being used, perform the following configuration:

1. Add excluded resource (/xmlpserver/services and /xmlpserver/report_service) on Oracle Access Manager Server for the Oracle Analytics Server/Oracle Analytics Publisher application domain.



2. Copy `mod_osso.conf` from the disabled directory to the moduleconf directory for editing. For example:

   From: `ORACLE_INSTANCE/config/OHS/<ohs_name>/disabled/mod_osso.conf`

   To: `ORACLE_INSTANCE/config/OHS/<ohs_name>/moduleconf/`

3. Add the following Web services in the `mod_osso.conf` file:

```
<Location /xmlpserver/services/>
require valid-user
AuthType Basic
Allow from All
Satisfy any
</Location>
```

4. Save the file and restart OHS Service.

Oracle Argus Safety Console—Oracle Analytics Publisher Common Settings

For information, see:

- Configure Oracle Analytics Publisher Reporting Admin User
- Enable Oracle Analytics Publisher Aggregate Reports and Configure Persistence Data (Flexible Aggregate Reporting only)
- Configure Code Lists

Configure Oracle Analytics Publisher Reporting Admin User

1. Navigate to **Argus Console** > **System Configuration** > **System Management (Common Profile Switches)**.
2. Expand the **Reporting** node on the tree that appears on the left pane.
3. Click **BIP Reporting**.
4. In **Common Settings** section, enter the Oracle Analytics Publisher Common username and password.

   This user is created in Oracle Analytics Publisher with administrator privileges. This user could be an actual Oracle Argus Safety user or a user who has No Access to Oracle Argus Safety.
5. Save the changes.

Enable Oracle Analytics Publisher Aggregate Reports and Configure Persistence Data (Flexible Aggregate Reporting only)

1. Navigate to **Argus Console** > **Enabled Modules**.
2. Enable the **BIP Aggregate Reports** module.
3. Navigate to **Argus Console** > **System Configuration** > **System Management (Common Profile Switches)**.
4. Expand the **Reporting** node on the tree that appears on the left pane.
5. Click **BIP Reporting**.
6. Set the Persist data in Oracle Analytics Publisher Aggregate Temp tables to **Yes** or **No**.

   The default value is **No**.
7. Set the Number of days to persist the Oracle Analytics Publisher Aggregate Temp table data. Defaulted to null.
8. Perform **iisreset** on Webserver to make sure that the changes made to enable the Oracle Analytics Publisher Aggregate Reports module are visible in the periodic report configuration.

> **Note**
>
> The Persist data parameters are used to logically retain the data from the Oracle Analytics Publisher temp tables and purge them after the specified number of days.

Configure Code Lists

For information, see:

Flexible Aggregate Reporting Code Lists

The REPORT_TEMPLATE Code list to be updated for executing Flexible Aggregate Reports through Oracle Analytics Publisher. Execute the following steps to configure the REPORT_TEMPLATE code list.

1. Navigate to **Argus Console** > **Code Lists** > **Flexible Data Re-categorization**.
2. Under the **Flexible Data Re-categorization** tree, navigate to **Flexible Re-categorization**.
3. Select the **Code List Name** as **REPORT_TEMPLATE** and click **Search**.
4. Update the **REPPATH** as follows:
   - For PBRER - `/Argus Safety/PBRER/Reports/pbrer.xdo`
   - For PMAR - `/Argus Safety/PMAR/Reports/pmar.xdo`
   - For DSUR - `/Argus Safety/DSUR/Reports/dsur.xdo`
5. Click **Save**.

> **Note**
>
> As the REPPATH is case sensitive, in Unix based Operating System, it must be same as that provided in Report.
>
> For example, in PBRER > Code List, the REPPATH is `/Argus Safety/PBRER/Reports/pbrer.xdo`
>
> The same path must be provided in the Reports and vice-versa.

PMDA R3 Paper Forms Code lists

1. Navigate to **Argus Console** > **Code Lists** > **Flexible Data Re-categorization**.
2. Under the **Flexible Data Re-categorization** tree, navigate to **Flexible Re-categorization**.
3. Select the **Code List Name** as **LM_REPORT_FORMS_EXPEDITED,** and click **Search**.
4. Check the **REPPATH** that is pre-configured with the report path of all the PMDA reports.

> **Note**
>
> Update this REPPATH only if the PMDA R3 reports are uploaded to a different folder than the one that is configured.

Configure Flexible Aggregate Reporting Database

> **Note**
>
> This section is applicable only if Flexible Aggregate Reporting is enabled.

Some database configurations need to be handled in order to enable the Flexible Aggregate Reporting in Oracle Argus Safety. These steps need to be handled from a machine where the Oracle Argus Safety database can be accessed (preferably the Oracle Argus Safety Web Server or the Oracle Argus Safety Transaction Server).

- Execute Argus_BIP_Enable
- Execute ETL Dashboard Utility

Execute Argus_BIP_Enable

1. From the command prompt, navigate to `<Argus Release Media>\DBInstaller\Utilities\BIP_Enable`.
2. Execute the batch file **Argus_BIP_Enable.bat**.
3. Enter the following parameters:
   a. TNSNAMES entry to connect to the Oracle Argus Safety database.

      For example, Oracle Argus Safety database SID.

   b. SYSTEM or DBA user name in SYSTEM or DBA user name in Argus database database.

   c. Password for SYSTEM or DBA user.

   d. FMW Database instance.

   e. Is FMW Database hosted on ADB? [Y/N]

   f. Name of DBA user in FMW DB.

      For DBaaS, use a user with SYSDBA privilege.

      For ADB, use ADMIN.

   g. Password for DBA user in FMW.

   h. Oracle Argus Safety schema owner name.

      For example: ARGUS_APP.

   i. Oracle Argus Safety schema password.

   j. Oracle Analytics Publisher Schema user.

      The Oracle Analytics Publisher Schema owner name created during the Oracle Argus Safety database installation. For example, BIP_OWNER.

   k. Password for the Oracle Analytics Publisher Schema user.

   l. Oracle Analytics Publisher Repository Service name.

      This is the database SID of the Oracle Analytics Publisher metadata repository.

m. Oracle Analytics Publisher Repository user name (Default DEV_BIPLATFORM).

   This is the BIPLATFORM user created in Oracle Analytics Publisher metadata repository.

n. Oracle Analytics Publisher Repository password.

o. Host name of the Oracle Analytics Publisher Repository instance.

   For example, <*hostname*>.<*domain name*>.

p. Oracle Analytics Publisher Repository instance listener port.

When the execution is complete, the database objects needed for enabling and integrating the Flexible Aggregate Reporting are created.

> **Note**
>
> If you are using Oracle Argus Mart with Oracle Analytics Publisher enabled in Oracle Argus Safety, make sure that you re-create the Oracle Argus Safety RO user.

Execute ETL Dashboard Utility

1. The `TNSNAMES.ORA` file present on the Argus Safety Database host must have an entry of each of the following:
   - Argus Safety database
   - Argus Insight database
   - Argus Mart database
   - ODI repositary DB for Argus Mart and Argus Analytics
2. All TNS entry must be present on the server where the utility is being invoked.
1. From the command prompt, navigate to *`Argus Release Media`*`\DBInstaller\Utilities\Create_ETL_dashboard_infra`.
2. Execute the `create_etl_dashboard_infra.bat` batch file.
3. 5. Enter the following parameters:
   a. Argus Safety instance, like *TNS of Safety DB*
   b. Argus Safety application user, like *ARGUS_APP*.
   c. Password of the Argus Safety application user.
   d. Do you want to configure ETL Dashboard for Argus Insight (Y/N).

      Skip the following Argus Insight parameters, if the Argus Insight configuration is selected as N.

   e. Argus Insight instance. like *TNS of Insight DB*.
   f. Name of the Argus Insight Mart user, like *APR_MART*.
   g. Password of the Argus Insight Mart user.
   h. Do you want to configure ETL Dashboard for Argus Mart (Y/N).

      Skip the following Argus Mart parameters, if the Argus Mart configuration is selected as N.

   i. Argus Mart instance, like *TNS of Mart DB*.

j. Name of the Argus Mart user in instance, like *AM_MART_USER*.

k. Password of *AM_MART_USER* in instance.

l. Name of the Argus Mart ODI Repository instance, like `TNS of Mart ODI Repository DB`.

m. Name of the Argus Mart ODI repository user in ODI, like *AM_ODI_REPO*.

n. Password of *AM_ODI_REPO* in ODI.

o. Name of the Argus Mart ODI DBA user in ODI, like SYSTEM or any user with similar privilege.

p. Password of the system in ODI.

q. Do you want to configure ETL Dashboard for Argus Analytics (Y/N).

   Skip the Argus Analyics parameters, if the Argus Analytics configuration is selected as N.

r. Name of the Argus Analytics ODI Repository instance, like *TNS of Analytics ODI Repository DB*.

s. Name of the Argus Analytics ODI repository user in ODI, like *AN_ODI_REPO*.

t. Password of *AN_ODI_REPO* in ODI DB.

u. Name of the Argus Analytics ODI DBA user in ODI, like SYSTEM or any user with similar privilege.

v. Password of SYSTEM in ODI.

Upgrade Oracle Analytics Publisher Reports

If you have enabled the Oracle Argus Safety Flexible Aggregate Reporting and you are upgrading from 8.1.x or 8.2.x:

> **Note**
>
> You can upgrade Oracle Analytics Publisher reports only from Oracle Argus Safety 8.1. Upgrade from previous versions of Oracle Argus Safety is not supported.
>
> Besides, any customization done to the Aggregate Reports must be taken care after upgrading.

To upgrade the Oracle Analytics Publisher report to this release:

1. For Oracle Analytics Publisher Flexible Aggregate Reporting, repeat the instructions of Execute Argus_BIP_Enable to recreate the AS_TO_BIPREP DB link.

   > **Note**
   >
   > Skip this step, if you are using ONLY PMDA R3 Paper reports.

2. Log in to the Oracle Analytics Publisher console as administrator (or any user who has Oracle Analytics Admin User access).
3. Back up the existing `.xdrz` files.

a. From the left pane, click **Catalog**.

   The Catalog screen with the Folders and Tasks sections appears.

b. Click **Folders** > **Shared Folders**.

c. Click **Tasks** > **Download**.

d. Click **Browse** and navigate to the location where the backup will be saved.

4. To upload the latest xdrz files (`Argus Safety.xdrz` and `AS_Expedited.xdrz`), see Flexible Aggregate Reports.

   While uploading, click **Overwrite existing files**.

21

Configure the Oracle Analytics Publisher Environment for Oracle Argus Insight

When you have installed the Oracle Analytics Publisher (OAP), you need to configure certain settings to be able to view the available reports in Oracle Analytics Publisher. This chapter introduces you with the steps to make those configuration changes using Oracle Analytics Publisher:

- Create PRMART JDBC Connection
- Manage Users and Roles: Oracle Analytics Publisher Standalone Installation with Oracle Fusion Middleware Security
- Configure Oracle Analytics Publisher Users and Roles: Oracle Fusion Middleware Security Model

Create PRMART JDBC Connection

If you are installing Oracle Analytics Publisher on a Windows machine, the TNS entry of Oracle Argus Insight must be added in `TNSNAMES.ora` file of the Oracle Analytics Publisher Web Server.

If Oracle Analytics Publisher is installed on a Linux machine, no modifications to the `TNSNAMES.ora` file are required.

When you have uploaded the `Argus Insight.xdrz` file to Oracle Analytics Publisher, you also need to create a connection between the Oracle Analytics Publisher and the database.

To connect the Oracle Analytics Publisher and the database:

1. Log on to Oracle Analytics Publisher using the administrator credentials.

   The Oracle Analytics Publisher home page appears.
2. From top-menu, click **Administration**.
3. In the Data Sources section, click **JDBC Connection**.

   The Data Sources screen appears.
4. Click **Add Data Source**.
5. In the Add Data Source section:
   a. In the **Data Source Name** field, enter **PRMART**.
   b. From the **Driver Type** drop-down list, select the database.

      The Database Driver Class field is auto-populated based on the selected Driver Type.
   c. In the **Connection String** field, enter the connection string.

      You must enter all the details in lower case in this field.
   d. In the **Username** field, enter the username (Oracle Argus Insight application DB user, for example, apr_app) to connect to the database.
   e. In the **Password** field, enter the password for the user.

f. Click **Test Connection**.

If successful, a confirmation message appears.

6. Click **Apply**.

The PRMART Data Source in the list of already existing data source names appears.

A connection between Oracle Analytics Publisher and the database is successfully created.

Manage Users and Roles: Oracle Analytics Publisher Standalone Installation with Oracle Fusion Middleware Security

This section introduces you with the steps that you need to execute to create users, assign the roles and permissions to those users, and configure server settings for the Oracle Fusion Middleware (OFM) Security Model:

- Create Users and Assign Roles to Users
- Oracle Analytics Publisher Standalone Installation in Oracle Fusion Middleware Security
- Create Roles, Adding Data Sources, and Assign Roles in WebLogic Oracle Enterprise Manager
- Create Application Policy
- Upload the Argus Insight.xdrz file to Oracle Analytics Publisher

Create Users and Assign Roles to Users

Creating users for LDAP or SSO users is done using the LDAP servers which is beyond the scope of this manual.

For the list of users that need to be configured, refer to the Configure Oracle Analytics Publisher Users and Roles: Oracle Fusion Middleware Security Model.

Oracle Analytics Publisher Standalone Installation in Oracle Fusion Middleware Security

This section provides the steps to create roles, policies, users, and groups in Oracle Fusion Middleware Security for Oracle Analytics Publisher Standalone Installation.

- Create Users and Groups
- Create Roles and Policies

Create Users and Groups

1. Open the WebLogic Administration Console.
2. Navigate to **Security Realms** > **myrealm** > **Users and Groups** > **Groups** tab.
3. From the Groups section, and click **New**.

   The Create a New Group dialog box appears.
4. Create the following groups by entering the **Name** and **Description**, and click **OK**.
   - AIAdminGroup
   - AIAuthorGroup

- AIConsumerGroup

To create users in the Oracle Fusion Middleware Control:

1. Open the WebLogic Administration Console.
2. Navigate to **Security Realms** > **myrealm** > **Users and Groups** > **Users**.
3. From the Users section, and click **New**.

   The Create a New User dialog box appears.
4. Enter the parameters, and click **OK**.
5. To assign a group to the user, from the Groups tab, select a Group, and click **Save**.

> **Note**
>
> For more details, refer to *Oracle Healthcare Translational ResearchInstallation Guide, section Create Oracle Analytics Server groups and users*.

Create Roles and Policies

To create new application roles:

1. Login to Oracle Fusion Middleware Control Enterprise Manager.
2. Go to **WebLogic Domain** > **Security** > **Application Roles**.

   The Application Roles dialog box appears.
3. From the **Application Stripe** drop-down list, select **OBI**, and click **Search**  .

   The default role available in clean slate installation appears.
4. Click **Create**.

   The Create Application Role dialog box appears.
5. In the **Role Name** field, enter **AIAdminRole**.
6. From the Members section, click **+Add**.

   The Add Principal dialog box appears.
7. From the **Type** drop-down list, select **Group**, and click **Search**.

   A list of principals appears.
8. From the list of Searched Principals, select **AIAdminGroup**, and click **OK**.
9. From the Members section, click **+Add**.

   The Add Principal dialog box appears.
10. From the **Type** drop-down list, select **Application Role**, and click **Search**.

    A list of principals appears.
11. From the list of Searched Principals, select **BIServiceAdministrator**, and click **OK.**

    The Membership for **AIAdminRole** appears.
12. To add **AIAuthorRole**, repeat from Step 4 to Step 11.
13. To add **AIConsumerRole**, repeat from Step 4 to Step 11.

> **Note**
>
> For more details, refer to *Oracle AnalyticsManaging Security for Oracle Analytics Server guide, section Manage Application Roles*.

To create new application policy:

1. Login to Oracle Fusion Middleware Control Enterprise Manager.
2. Go to **WebLogic Domain** > **Security** > **Application Policies**.

   The Application Policies screen appears.
3. To create a new application policy, click **Create**.

   The Create Application Grant dialog box appears.
4. From the Grantee section, click **+Add**.

   The Add Principal dialog box appears.
5. From the **Type** drop-down list, select **Application Role**, and click **Search**  .
6. From the list of Searched Principals, select **AIAdminRole**, and click **OK**.
7. From the Permissions section, click **+Add.**

   The **Add Permission** dialog box appears.
8. Select the **Resource Types** radio button.
9. From the **Resource Type** drop-down list, select **oracle.bi.publisher.permission**, and click **Search**.
10. From the Search Results, select **oracle.bi.publisher.permission** (Oracle Analytics Publisher Administer Server), and click **Continue**.

    The Add Permission dialog box appears.
11. For **Permission Actions**, select **All** (_all_), and click **Select**.
12. Add Resource Name as **oracle.bi.user** with **Impersonate** permission.

    The new AI Admin policy has all the permissions.

> **Note**
>
> Make sure all the fields are either selected or entered manually.

13. Repeat from Step 4 to Step 12, to add the following:

Name	Grantee	Resource Permissions
AI Author	AIAuthorRole	BIP Develop Report BIP Develop Data Model
AI Consumer	AIConsumerRole	BIP Access Excel Report Analyzer BIP Access Online Report Analyzer BIP Access Report Output BIP Schedule Report

Create Roles, Adding Data Sources, and Assign Roles in WebLogic Oracle Enterprise Manager

To create roles, add data sources, and assign roles in WebLogic Oracle Enterprise Manager, execute the following procedure:

1. Log on to the Oracle Enterprise Manager.

   The Enterprise Manager home page appears with a list of folders in the left pane.
2. Expand the **Weblogic_Domain** > **Security** folder, and click **Application Roles**.
3. In the Application Policies and Roles section, click **Configure and Manage Application Roles**.

   The Application Roles screen appears.
4. From the **Application Stripe** drop-down list, select the OBI as application stripe.
5. Select any existing role (for example, AIConsumerRole), and click **Create Like**.

   The Create Application Role screen appears.
6. In **Role Name** field, enter the name of the role.
7. Optionally, enter the **Display Name** and **Description** for the role.
8. To add any existing application role/group/user to the new role, click **Add**.
9. To display the list of all the roles, groups, and users that are created in LDAP server, click the **>** icon next to the **Display Name** field.
10. Select the name of the role, group, or user that you want to add to the new role, and click **OK**.
11. Repeat steps 8 to 10 to add more roles, users, and groups to the new role.
12. On Create Application Role screen, click **OK** to save the changes.

    When you have created the role and added the required list of users, roles, and groups to the new role, you must add the **PRMART** data source to the new role.
13. Log on to Oracle Analytics Publisher using the administrator credentials.

    The Oracle Analytics Publisher home page appears.
14. From top-menu, click **Administration**.

    Refer to Section 6.2 > Step 2.
15. In Security Center section, click **Roles and Permissions**.

    The Roles and Permission screen appears.

    You can view the name of the new role which you have just created in the list of role names.
16. Click the **Add Data Sources** icon corresponding to the name of the new role.

    The Add Data Sources screen appears.
17. From the Available Data Sources section, select **PRMART**, and click the **Move (>)** icon to move the PRMART data source to the Allowed Data Sources section.
18. Click **Apply** to save the changes.

    For more information, refer to the Oracle BIP Administrator's Guide > Creating Application Roles Using Fusion Middleware Control section.

For the list of roles that need to be configured, refer to the Configure Oracle Analytics Publisher Users and Roles: Oracle Fusion Middleware Security Model.

Create Application Policy

Once you have created the new role and assigned the required roles, users, and data sources to the role, you also need to create the application policy for the new role.

Before creating a Oracle Analytics Publisher policy, you must have created an empty role in the Enterprise Manager.

To create the application policy for the new role, execute the following steps:

1. Log on to the Oracle Enterprise Manager.

   The Enterprise Manager home page appears with a list of folders in the left pane.
2. Expand the **Weblogic_Domain** > **Security** folder, and click **Application Policies**.
3. In the Application Policies and Roles section, click **Configure and Manage Application Policies**.

   The Application Policies screen appears.
4. From the **Application Stripe** drop-down list, select **obi**.
5. Select the **BIAuthor** policy, and click **Create Like**.

   The Create Application Grant Like screen appears with the **Grantee** and **Permissions** sections.
6. In the Grantee section, click **Add**.

   This displays the Add Principal Screen.
7. To retrieve the list of all the available application roles, click the **>** icon next to the **Principal Name** field.
8. From the Searched Principals section, select the name of the role (for example, BIReportWriter), and click **OK**.

   The Create Application Grant Like screen appears.
9. From the list of Permission Classes, select the **developDataModel** resource name, and click **Delete**.
10. Click **OK** to apply the changes.

Upload the Argus Insight.xdrz file to Oracle Analytics Publisher

> **Note**
>
> You must be logged in to Oracle Analytics Publisher with the Oracle Analytics Admin User credentials to be able to upload the `Argus Insight.xdrz` file.

1. Copy the `Argus Insight.xdrz` file from the release media to the local file system:

   `<Argus Install Media>\SUPPORT\BIP`
2. Log on to Oracle Analytics Publisher using the Oracle Analytics Admin User credentials.

   The Oracle Analytics Publisher home page appears.

3. From the menu bar, click **Catalog**.

   The Catalog screen with the **Folders** and **Tasks** sections appears.

4. From Folders section in the left pane, click **Shared Folders**.
5. Navigate to **Shared Folders** > **Argus Insight** > **General** > **Reports** > **Remove/Delete Generic Line Listing Report – LE**.
6. From Folders section in the left pane, click **Shared Folders**.
7. From Tasks section in the left pane, click **Upload**.

   The Upload dialog box appears.

8. Click **Browse** and navigate to the location where you have saved the `Argus Insight.xdrz` file on the local file system.
9. Click **Upload**.

   After successful upload, an **Argus Insight** folder is created in **Shared Folders**.

10. Expand the **Argus Insight** folder to verify that the **Generic Line Listing Data Model** exists in the **Data Models** sub-folder and the **Generic Line Listing Report** in **RTF** format exists in the **Reports** sub-folder.

Configure Oracle Analytics Publisher Users and Roles: Oracle Fusion Middleware Security Model

This section lists the names of the <Admin Users> and roles that you need to configure using the steps given in Manage Users and Roles: Oracle Analytics Publisher Standalone Installation with Oracle Fusion Middleware Security.

Table 21-1 Configuring Oracle Analytics Publisher Users: Oracle Fusion Middleware Security Model

User	Description
Oracle Analytics Admin User	An Admin user refers to the user who has Oracle Analytics Publisher administrative rights. This user should belong to the **BIAdministration** functional role.
Data Modeler Users	An Oracle Argus Insight Data Model user refers to the user who should have access to both **Data Models** and **Reports** in the **Argus Insight** folder. This user should belong to **AIDataModeler** custom role. There are Oracle Enterprise Manager specific Modeler users, who have access to **Data Models** and **Reports** in Enterprise specific folders and **Argus Insight** folder. These users should have Oracle Enterprise Manager specific Modeler roles assigned to them. This user should belong to Oracle Enterprise Manager specific Modeler roles.
Users	An Oracle Argus Insight Role (AIRole) user refers to the user who should have access to **Reports** only, and should have Read-only access to the Data Model which is required to create the reports. This user should belong to **AIRole**. There can be users who have access to reports of specific Enterprises. These users can Read/Write reports in **Enterprise specific Report** folder and **Argus Insight Report** folder. However, these users have Read-only access to the Data Models in the Enterprise specific **Data Model** and Oracle Argus Insight **Data Model** folder. This user should belong to Enterprise specific Report roles.

Table 21-1 (Cont.) Configuring Oracle Analytics Publisher Users: Oracle Fusion Middleware Security Model

User	Description
Global Admin Users	An AI Admin Role user should have full access to the **Argus Insight** folder (Read/Write/Delete). An Enterprise specific Admin user should have full access to the Enterprise specific folders (Read/Write/Delete) and **Argus Insight folder** (Read/Write/Delete).

For more information, see:

- Configure Oracle Analytics Publisher Roles
- Folder Level Permissions

Configure Oracle Analytics Publisher Roles

The following table illustrates the roles that you need to configure using Oracle Analytics Publisher:

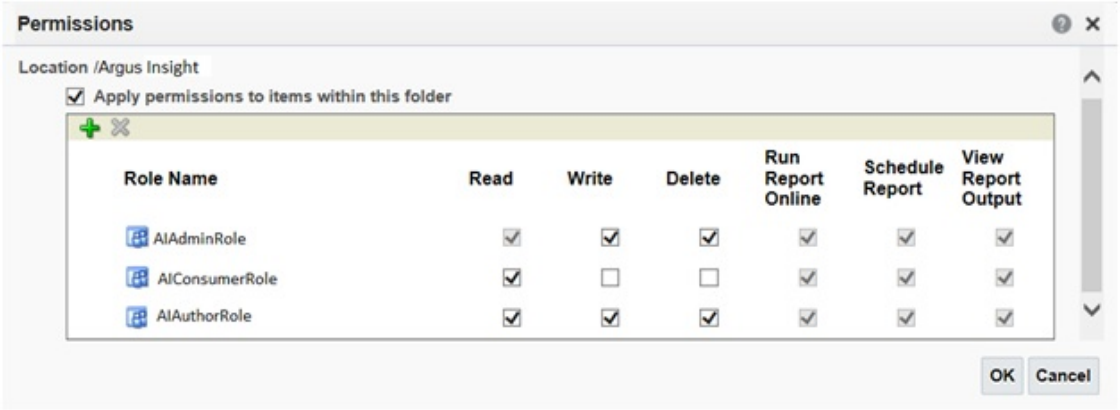
Table 21-2 Configuring Oracle Analytics Publisher Roles

Role	Users/Roles to be added
BIAdministration (Functional Role)	Super user who has full access to any folder and Oracle Analytics Publisher Administration access
AIRole	All Oracle Argus Insight role users, **AIDataModelerRole**, and All Enterprise Report Roles (for specific enterprises)
AIDataModelerRole	All AI Data Modeler Users, All Enterprise Modeler Roles, and **AIAdminRole**
Enterprise Report Role	Users that belong to a specific Enterprise with **Reports** access and Enterprise Modeler Role
Enterprise Modeler Role	Users that belong to a particular Enterprise with both **Data Models** and **Reports** access
Enterprise Admin Role	Enterprise specific Admin users. These users should have full access to the Enterprise specific folders.
AIAdminRole	Any User with this role should have full access to the Oracle Argus Insight Folder. The Enterprise Admin Role should be added to this role.
BIAdministrator (Functional Role)	Oracle Analytics Admin User
BIAuthor (Functional Role)	**AIDataModelerRole**
BIReportWriter (create this role using the steps given in section 8.4.3 and create an Application Policy for this role using the steps given in section 8.4.4)	**AIRole**

Folder Level Permissions

View folder level permissions for Oracle Analytics Publisher Standalone Installation:

You cannot see the permissions of shared folder for Oracle Analytics Publisher Stand-Alone installation. Besides, the Oracle Argus Insight permissions folder appears.



To assign folder level permissions for Oracle Analytics Publisher Integrated Installation (Oracle Analytics Server+Oracle Analytics Publisher):

1. Login to Oracle Analytics Server Analytics with the WebLogic user credentials.
2. Go to **Catalog** > **Shared Folders** > **Tasks** > **Permissions**.

   The Permissions dialog box appears.
3. Set the Permissions as follows, and click **OK**.

Accounts	Permissions
Oracle Argus Insight Admin Role	Open (Read, and Traverse)
Oracle Argus Insight Author Role	Open (Read, and Traverse)
Oracle Argus Insight Consumer Role	Open (Read, and Traverse)
Oracle Analytics Service Administrator (Owner)	Full Control

4. Go to **Shared Folders** > **Argus Insight** > **Permissions**.

   The Permissions dialog box appears.
5. Set the Permissions as follows, and click **OK**.

Accounts	Permissions
Oracle Argus Insight Admin Role (Owner)	Full Control
Oracle Argus Insight Author Role	Full Control
Oracle Argus Insight Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
Oracle Analytics Service Administrator	Full Control

22

Configure the Oracle Analytics Server Environment for Oracle Argus Insight

In this chapter:

Pre-installation Configuration

Before integrating Oracle Analytics Server with Oracle Argus Insight, make sure to complete the following tasks:

1. Install JDK on the machine where Oracle Argus Insight is installed.
2. Since the data for analysis is based on Oracle Argus Mart schema and not the Oracle Argus Insight Mart schema, the TNS entry for the Oracle Argus Mart schema should be present in the Oracle Analytics Server 12c home at the following path:

   oas_home\user_projects\domains\bi\config\fmwconfig\bienv\core\

   > **Note**
   >
   > In this chapter, **bi** is referred as the domain name. This domain name may differ based on your configuration.
   >
   > *oas_home*/user_projects/domains/bi

3. Set up the TNS for Oracle Client Home in the PATH variable.
4. Install Oracle Argus Mart.

   When the installation is complete, the new tables, indexes, packages and all the objects required for Oracle Analytics Server are created in the Oracle Argus Mart schema.

   Additionally, a read only user AM_BI_USER with read-only privileges on Oracle Analytics Objects is created.

   For detailed information on installing and upgrading Oracle Argus Mart schema, refer to *Oracle Argus Mart Installation and Administration Guide*.

Configure the Oracle Analytics Server Repository and Web Catalog using the BAR File

Oracle Analytics Application Archive (BAR) file is a compressed archive file that contains a cohesive set of Oracle Analytics metadata artifacts (data model, content model, and authorization model). When deploying Oracle Analytics application from one server to another you can use these BAR files to transfer the metadata instead of transferring the RPD, Catalog, and the Security Model separately.

A BAR file contains the following Oracle Analytics application module artifacts:

- Data model metadata for the Oracle Analytics Server. This metadata is xml-based but functionally equivalent to an .RPD file.
- Presentation Services catalog metadata for a service instance.
- Security policy metadata containing application role and application role memberships, and permission and permission set grants for a service instance.
- A manifest file declaring the dependencies of the BAR file.

> **Note**
>
> Importing a BAR file replaces all the Catalog files, RPD files, and the Security Model in an existing Oracle Analytics Server instance with any customization.
>
> It is recommended that the BAR file import is done on a new Oracle Analytics Server instance.

For more information, see:

- Import the BAR file in an existing Oracle Analytics Server instance
- Import the BAR file to create a new Oracle Analytics Server Instance

Import the BAR file in an existing Oracle Analytics Server instance

Before importing the BAR File, make sure:

- Oracle Analytics Server compatible version is installed
- The Administrator Console is up and running

  (validate it from *http://machinename.port/console*)
- The Oracle Enterprise Manager (Oracle Fusion Middleware Control) is up and running

  (validate it from *http://machinename.port/em*)

To import the BAR File:

1. Copy the BAR file from `<AI HOME>OAS\BAR File\ssi.bar` to a local folder on the machine where the Oracle Analytics Server is installed.

   For example, copy the file at `C:\AIOAS`.
2. Login to the Oracle Enterprise Manager with the Oracle WebLogic Server credentials.

3. Click **Target Navigation**.

The Target Navigation drop-down menu appears.

4. Go to **Business Intelligence** > **biinstance**.

The Business Intelligence Instance screen appears.

5. From the Availability tab, select **Processes**, and click **Stop All**.

A confirmation dialog box appears.

6. Click **Yes**.

All the running processes are stopped.

7. Go to the command prompt, and start the WebLogic Scripting Tool (using **wlst.cmd** on Windows, and **wlst.sh** on Unix/Linux) from the following path:

OracleBI Home\Middleware\oracle_common\common\bin

8. To know the **BI Service Instance key**, type the following command, and press Enter.

```
> listBIServiceInstances(domainHome)
```

where, Domain Home is the directory of the Oracle Analytics Install domain, the default path is:

oas_home/user_projects/domains/bi

The Key appears at the end of the command.

For example, **ssi** appears as the Key.

9. Exit WLST using the **exit ()**command.

10. To import the BAR file:

    a. Go to the Domain Home path:

    oas_home/user_projects/domains/bi/bitools/bin

    b. Execute the following command:

    importarchive.cmd Oracle Analytics Service Instance key <*complete path of bar file to import*>

    For example, importarchive.cmd ssi C:\ai841\ssi.bar

11. Go to Oracle Enterprise Manager, from the Availability tab, select **Processes**, and click **Start All**.

A confirmation dialog box appears.

12. Click **Yes**.

The BAR file imports the RPD, Catalog and the Security model.

To check if the BAR File has imported RPD, Catalog, and the Security Model:

1. To verify the Roles and Policies imported by BAR file in the Oracle Enterprise Manager, go to **Business Intelligence Instance** > **Security** > **Application Roles and Application Policies**.

   The following roles are imported as default application roles:

   - AI Admin Role
   - AI Author Role
   - AI Consumer Role

   For a list of privileges assigned to these roles, refer to Oracle Analytics Server Default Application Roles.

2. To modify the Connection Pool Settings:

   a. From the following path, right click the **admintool.cmd** file, and click **Run as Administrator**.

      oas_home\user_projects\domains\bi\bitools\bin

      The Oracle Analytics Admin Tool opens.

   b. To open the RPD, select the online mode, and enter the Oracle WebLogic Server user credentials.

      > **Note**
      >
      > To open the RPD in online mode, you must set the Open Database Connectivity (ODBC). Refer to the Create ODBC Connection for OAS Administration Tool for Oracle Argus Insight.
      >
      > If Oracle Analytics Server is installed on the Unix or Linux machine, set up the Oracle Analytics Developer Client Tool on any Windows machine to access the Oracle Analytics Administration Tool.

   c. Click the **Connection Pool**, and modify the **Data source name**, **User name**, and **Password**.

      Modify both the connection pools: AI80OAS_CP and AI80OAS_CP_InitBlocks.

3. Check-in the changes, and save the RPD.

   Ignore the warning messages that appear during the consistency check.

4. Create Oracle Analytics Server Groups and Users. (See Create Users and Groups in Oracle Analytics Server)

5. Go to Catalog, and set the folder level permissions for the Oracle Analytics Server Groups. (See Oracle Analytics Server Catalog Folder-level Permissions)

6. To view and administer privileges for the Oracle Analytics components, login to Oracle Analytics Server Analytics with Oracle WebLogic Server user credentials.

   Go to **Administration** > **Security** > **Manage Privileges**.

   For a list of privileges assigned to these roles, refer to Oracle Analytics Server Default Application Roles.

7. Go to **Administration** > **Maintenance and Troubleshooting**, and click **Reload Files and Metadata**.

8. To use the AI Aggregate Analysis Subject area and Dashboard, login with a valid user credentials.

Import the BAR file to create a new Oracle Analytics Server Instance

1. Copy the BAR file from `<AI HOME>OAS\BAR File\ssi.bar` to a local folder on the machine where the Oracle Analytics Server is installed.
2. When creating an instance in Oracle Analytics Server, enter the BAR file path in the **Path** field of the OAS Initial Application wizard screen.
3. When the installation is completed successfully, and all the processes are up, open the RPD in online mode, and change the **Connection Pool Settings**. (See Import the BAR file in an existing Oracle Analytics Server instance > Step 2)
4. Check-in the changes, and save the RPD.

   Ignore the warnings that appear during the consistency check
5. From the **Enterprise Manager** > **Stop and Start the BI processes**.
6. Create Oracle Analytics Server Groups and Users. (See Create Users and Groups in Oracle Analytics Server)
7. Go to Catalog, and set the folder level permissions for the Oracle Analytics Server Groups. (See Oracle Analytics Server Catalog Folder-level Permissions)
8. To view and administer privileges for the Oracle Analytics components, login to Oracle Analytics Server Analytics with Oracle WebLogic Server user credentials.

   Go to **Administration** > **Security** > **Manage Privileges**.

   For a list of privileges assigned to these roles, refer to Oracle Analytics Server Default Application Roles.
9. Go to **Administration** > **Maintenance and Troubleshooting**, and click **Reload Files and Metadata**.
10. To use the AI Aggregate Analysis Subject area and Dashboard, login with a valid user credentials.

Configure Oracle Analytics Server Repository and Web Catalog Manually

1. Copy the RPD, and Catalog files from `<AI HOME>OAS\RPD\` and `<AI HOME>OAS\Catalog` folders to a machine where the Oracle Analytics Server is installed.
2. Open the RPD Admin tool in offline mode from the following path:
   oas_home`\user_projects\domains\bi\bitools\bin\admintool.cmd`

   The default Repository Password is **insight123**.
3. Change the **Connection Pool Settings**.

   See Import the BAR file in an existing Oracle Analytics Server instance > Step 2
4. Save the changes, and close the RPD.
5. From the command prompt:
   a. Navigate to the *oas_home*`\user_projects\domains\bi\bitools\bin`
   b. Run the following command:

```
datamodel.cmd uploadrpd -I <RPDname> [-W <RPDpwd>] -U <cred_username> [-P
<cred_password>] -SI <service_instance>
```

For example, `datamodel.cmd uploadrpd -I C:\AIOAS\RPD\ArgusInsight.rpd -W insight123 -U weblogic -P weblogic1 -SI ssi`

6. Login to the Oracle Enterprise Manager with the Oracle WebLogic Server credentials.
7. Click **Target Navigation**.

The Target Navigation drop-down menu appears.

8. Go to **Business Intelligence** > **biinstance**.

   The Business Intelligence Instance screen appears.

9. From the Availability tab, select **Processes**, and click **Stop All**.

   A confirmation dialog box appears.

10. Click **Yes**.

    All the running processes are stopped.

11. Go to `Catalog\argusinsight\root\shared` folder:
    a. Copy **argus+insight** folder, and **argus+insight.atr** file.
    b. Paste in *oas_home*`\user_projects\domains\bi\bidata\service_instances\ssi\metadata\content\catalog\root\shared` folder.
12. Go to Oracle Enterprise Manager, from the Availability tab, select **Processes**, and click **Start All**.

    A confirmation dialog box appears.

13. Click **Yes**.
14. Create User Groups and Users manually in Admin Console. (See Create Users and Groups in Oracle WebLogic Server.).
15. Create Roles and policies manually in Oracle Enterprise Manager. (See Create Roles and Policies with Oracle Fusion Middleware Control.)
16. To view and administer privileges for the Oracle Analytics components, login to Oracle Analytics Server Analytics with Oracle WebLogic Server user credentials.
17. Go to **Administration** > **Security** > **Manage Privileges**.

    For a list of privileges assigned to these roles, refer to Oracle Analytics Server Default Application Roles.

18. Go to Catalog, and set the folder level permissions for the Oracle Analytics Server Groups. (See Oracle Analytics Server Catalog Folder-level Permissions)
19. Go to **Administration** > **Maintenance and Troubleshooting**, and click **Reload Files and Metadata**.
20. To use the AI Aggregate Analysis Subject area and Dashboard, login with a valid user credentials.

> **Note**
>
> All the WLST commands are case sensitive.
>
> To start the WebLogic Scripting Tool on Unix or Linux, use wlst.sh command, rest all of the commands mentioned in the procedure remains same.
>
> While executing the WLST commands on Windows server, you must use forward slash (/) to avoid any error messages. For example:
>
> `C:/AIOAS/instance/import/ssi.bar`

Create Users and Groups in Oracle Analytics Server

In this section:

Create Users and Groups in Oracle WebLogic Server

To create users and groups in Oracle Analytics Server

1. Open the Oracle WebLogic Server Administration Console.
2. Navigate to **Security Realms** > **myrealm** > **Users and Groups** > **Groups** tab.
3. From the Groups section, and click **New**.

   The Create a New Group dialog box appears.
4. Create the following groups by entering the **Name** and **Description**, and click **OK**.
   - AIAdminGroup
   - AIAuthorGroup
   - AIConsumerGroup

To create users in the Oracle Fusion Middleware Control:

1. Open the Oracle WebLogic Server Administration Console.
2. Navigate to **Security Realms** > **myrealm** > **Users and Groups** > **Users**.
3. From the Users section, and click **New**.

   The Create a New User dialog box appears.
4. Enter the parameters, and click **OK**.
5. To assign a group to the user, from the Groups tab, select a Group, and click **Save**.

Create Roles and Policies with Oracle Fusion Middleware Control

> **Note**
>
> This section is applicable only when you manually upload the RPD file and Catalog. For more details, refer to Configure Oracle Analytics Server Repository and Web Catalog Manually..

To create new application roles:

1. Login to Oracle Fusion Middleware Control Enterprise Manager.
2. Go to **WebLogic Domain** > **Security** > **Application Roles**.

   The Application Roles dialog box appears.
3. From the **Application Stripe** drop-down list, select **OBI**, and click **Search** .

   The default role available in clean slate installation appears.
4. Click **Create**.

   The Create Application Role dialog box appears.
5. In the **Role Name** field, enter **AIAdminRole**.
6. From the Members section, click **+Add**.

   The Add Principal dialog box appears.
7. From the **Type** drop-down list, select **Group**, and click **Search**.

   A list of principals appears.
8. From the list of Searched Principals, select **AIAdminGroup**, and click **OK**.
9. From the Members section, click **+Add**.

   The Add Principal dialog box appears.
10. From the **Type** drop-down list, select **Application Role**, and click **Search**.

    A list of principals appears.
11. From the list of Searched Principals, select **BIServiceAdministrator** , and click **OK.**

    The Membership for **AIAdminRole** appears.
12. Repeat from Step 4 to Step 11 to create other Roles and add Member to these roles as listed in the table below.

Role	Application Roles
AI Admin Role	AI Admin Group
--	Weblogic
AI Author Role	AI Author Group
--	AI Admin Group
AI Consumer Role	AI Consumer Group
--	AI Author Group

Role	Application Roles
--	AI Admin Group

> **Note**
>
> For more details, refer *Oracle Analytics Managing Security for Oracle Analytics Server guide, section Manage Application Roles*.

To create new application policy:

1. Login to Oracle Fusion Middleware Control Enterprise Manager.
2. Go to **WebLogic Domain** > **Security** > **Application Policies**.

   The Application Policies screen appears.
3. To create a new application policy, click **Create**.

   The Create Application Grant dialog box appears.
4. From the Grantee section, click **+Add**

   The Add Principal dialog box appears.
5. From the **Type** drop-down list, select **Application Role**, and click **Search**.
6. From the **Type** drop-down list, select **Application Role**, and click **Search**.
7. From the list of Searched Principals, select **AIAdminRole**, and click **OK**.
8. From the Permissions section, click **+Add**

   The Add Permission dialog box appears.
9. Select the **Resource Types** radio button.
10. From the **Resource Type** drop-down list, select **oracle.bi.publisher.permission**, and click **Search**.
11. From the Search Results, select **oracle.bi.publisher.permission** (Oracle Analytics Publisher Administer Server), and click **Continue**.

    The Add Permission dialog box appears.
12. For **Permission Actions**, select **All** (_all_), and click **Select**.
13. Repeat from Step 4 to Step 11, to add the following:

Policy Name/ Principal	Resource Type	Resource Name	Permission Actions
AI Admin Role	oracle.bi.catalog	*	manage
--	oracle.bi.server.permission	oracle.bi.server.manageRepositories	_all_
--	oracle.bi.presentation.catalogmanager.permission	oracle.bi.presentation.catalogmanger.manageCatalog	_all_
--	oracle.bi.delivers.job	oracle.bi.delivers.job	manage
--	oracle.bi.publisher.permission	oracle.bi.publisher.administerServer	_all_

Policy Name/ Principal	Resource Type	Resource Name	Permission Actions
--	oracle.bi.repository	oracle.bi.repository	manage
--	oracle.bi.scheduler.permission	oracle.bi.scheduler.manageJobs	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
AI Author Role	oracle.bi.publisher.permission	oracle.bi.publisher.developReport	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.developDataModel	_all_
--	oracle.bi.tech.visualanalyzer.permission	oracle.bi.tech.visualanalyzer.generalAccess	*
--	oracle.bi.delivers.job	*	schedule
AI Consumer Role	oracle.bi.publisher.permission	oracle.bi.publisher.scheduleReport	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.runReportOnline	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.accessReportOutput	_all_
--	oracle.bi.publisher.permission	oracle.bi.publisher.accessOnlineReportAnalyzer	_all_
--	ESSMetadataPermission	oracle.bip.ess.JobDefinition.EssBipJob	READ,EXECUTE
--	oracle.bi.publisher.permission	oracle.bi.publisher.accessExcelReportAnalyzer	_all_

Oracle Analytics Server Catalog Folder-level Permissions

1. Login to Oracle Analytics Server Analytics with the Oracle WebLogic Server user credentials.
2. Go to **Catalog** > **Shared Folders** > **Tasks** > **Permissions**.

   The Permissions dialog box appears.
3. Set the Permissions as follows:

Accounts	Permissions
AI Admin Role	Full Control
AI Author Role	Full Control
AI Consumer Role	Open (Read, and Traverse)
BI Service Administrator (Owner)	Full Control

   a. Select **Apply Permissions to sub-folders**.
   b. Select **Permissions to items within folder**.
   c. Click **OK**.

4. Go to **Shared Folders** > **Argus Insight** > **Permissions**.

   The Permissions dialog box appears.

5. Set the Permissions as follows:

Accounts	Permissions
AI Admin Role (Owner)	Full Control
AI Author Role	Full Control
AI Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
BI Service Administrator	Full Control

   a. Select **Apply Permissions to sub-folders**.

   b. Select **Permissions to items within folder**.

   c. Click **OK**.

- Setup the Permissions through the Catalog Manager

Setup the Permissions through the Catalog Manager

1. Open the catalog manager from the following path, right-click **runcat.cmd**, and click **Run as administrator**: `<oas_home >\user_projects\domains\<instance_name>\bitools\bin\runcat.cmd`

2. Open the catalog in offline mode from the catalog path.

   For example:
   `C:\Oracle\Middleware\Oracle_Home\user_projects\domains\bi1\bidata\service_instances\ssi\metadata\content\catalog\`

3. Click the **'/'** folder.

   In the right pane, the Shared folder appears.

   a. Right-click the Shared folder, and select **Permissions**.

      The Permissions dialog box appears.

   b. Set the Permissions as follows:

Accounts	Permissions
AI Admin Role (Owner)	Full Control
AI Author Role	Full Control
AI Consumer Role	Custom (Read, Traverse, Run Publisher Report, Schedule Publisher Report, and View Publisher Output)
BI Service Administrator	Full Control

   c. Select **Apply Permissions to sub-folders**.

   d. Select **Permissions to items within folder**.

   e. Click **OK**.

4. Right-click the Shared folder > **Properties**, set the owner as **BiServiceAdministrator**, and click **OK**.

5. From the tree structure (on the left side), click Shared folder.

   Oracle Argus Insight folder appears on the right side.

   Right-click Oracle Argus Insight folder, and click **Permissions**.

   Set the permissions as in Step 3 b to 3 d.

   The Permissions dialog box appears.
6. Right-click Oracle Argus Insight folder > **Properties**, set the owner as **AIAdminRole**, and click **OK**.
7. Login to Oracle Analytics Server Analytics, and check the folder level permissions.
8. Go to **Administration** > **Maintenance and Troubleshooting**, and click **Reload Files and Metadata**.

Oracle Analytics Server Default Application Roles

To view and administer privileges of Oracle Analytics components:

1. Login to Oracle Analytics Server Analytics with Oracle WebLogic Server user credentials.
2. Go to **Administration** > **Security** > **Manage Privileges**.

> **Note**
>
> Create these privileges only when you manually upload the RPD and Catalog.
>
> You do not need to create these privileges when you import the BAR file.

Component	Privilege	Default Role Granted
Access	Access to Dashboards	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Access	Access to Answers	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Access	Access to BI Composer	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Access	Access to Delivers	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Access	Access to Briefing Books	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Access	Access to Mobile	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Access	Access to Administration	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Access	Access to Segments	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Access	Access to Segment Trees	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Access	Access to List Formats	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Access	Access to Metadata Dictionary	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
Access	Access to Oracle Analytics for Microsoft Office	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Access	Access to Oracle Analytics Client Installer	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Access	Catalog Preview Pane UI	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Access	Access to Export	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Actions	Create Navigate Actions	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Actions	Create Invoke Actions	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Actions	Save Actions containing embedded HTML	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: Catalog	Change Permissions	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Admin: Catalog	Toggle Maintenance Mode	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	Manage Sessions	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	Create Dashboards	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Admin: General	See sessions IDs	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	Change Log Configuration	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	Issue SQL Directly	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	View System Information	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	Performance Monitor	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	Manage Agent Sessions	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	Manage Device Types	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	Manage Map Data	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	See privileged errors	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	See SQL issued in errors	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Admin: General	Manage Global Variables	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: General	Diagnose BI Server Query	Denied: Authenticated User
Admin: Security	Manage Catalog Accounts	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
Admin: Security	Manage Privileges	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: Security	Set Ownership of Catalog Objects	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Admin: Security	User Population - Can List Users	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
Admin: Security	User Population - Can List Application Roles	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
Admin: Security	Access to Permissions Dialog	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Briefing Book	Add To or Edit a Briefing Book	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Briefing Book	Download Briefing Book	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Briefing Book	Add to Snapshot Briefing Book	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Catalog	Personal Storage (My Folders and My Dashboard)	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Catalog	Reload Metadata	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Catalog	See Hidden Items	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Catalog	Create Folders	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Catalog	Archive Catalog	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Catalog	Unarchive Catalog	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Catalog	Upload Files	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Catalog	Perform Global Search	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Conditions	Create Conditions	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Dashboards	Save Customizations	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Dashboards	Assign Default Customizations	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Dashboards	Create Bookmark Links	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Dashboards	Create Prompted Links	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Dashboards	Export Entire Dashboard To Excel	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Dashboards	Export Single Dashboard Page To Excel	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
Formatting	Save System-Wide Column Formats	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Home and Header	Access Home Page	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	Access Catalog UI	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	Access Catalog Search UI	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	Open Menu	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	New Menu	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	Help Menu	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	Dashboards Menu	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	Favorites Menu	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	My Account Link	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	Custom Links	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Home and Header	Access Administration Menu	Denied: Authenticated User
Home and Header	Access User & Role Admin	Denied: Authenticated User
Home and Header	Access Modeler	Denied: Authenticated User
My Account	Access to My Account	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
My Account	Change Preferences	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
My Account	Change Delivery Options	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Answers	Create Views	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Answers	Create Prompts	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Answers	Access Advanced Tab	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Answers	Edit Column Formulas	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Answers	Save Content with HTML Markup	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Answers	Enter XML and Logical SQL	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Answers	Edit Direct Database Analysis	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Answers	Create Analysis From Simple SQL	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
Answers	Create Advanced Filters and Set Operations	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Answers	Save Filters	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Answers	Save Column	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Answers	Add EVALUATE_PREDICATE Function	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Answers	Execute Direct Database Analysis	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Answers	Upload Images	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Delivers	Create Agents	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Delivers	Publish Agents for Subscription	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Delivers	Deliver Agents to Specific or Dynamically Determined Users	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
Delivers	Chain Agents	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Delivers	Modify Current Subscriptions for Agents	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator
RSS Feeds	Access to RSS Feeds	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Mobile	Enable Local Content	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
Mobile	Enable Search	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
SOAP	Access SOAP	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Impersonate as system user	Oracle Analytics System
SOAP	Access MetadataService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access MsgdbService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access ReportEditingService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access ConditionEvaluationService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access SecurityService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access Tenant Information	Oracle Analytics System

Component	Privilege	Default Role Granted
SOAP	Access SchedulerService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access DashboardService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access JobManagementService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access CatalogIndexingService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access UserPersonalizationService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access AnalysisExportViewsService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator
SOAP	Access CatalogService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access AdministrationSOAPService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access HtmlViewService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access XmlGenerationService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
SOAP	Access IBotService Service	Oracle Argus Insight Consumer Role, Oracle Analytics Service Administrator, Oracle Analytics System
Subject Area: "AI-Aggregate Analysis"	Access within Oracle Analytics Answers	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Canvas	Add/Edit Canvas View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Column Selector	Add/Edit Column Selector View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Compound Layout	Add/Edit Compound Layout View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Contribution Wheel	Add/Edit Contribution Wheel View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Graph	Add/Edit Graph View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Funnel	Add/Edit Funnel View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Gauge	Add/Edit Gauge View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Micro Chart	Add/Edit Micro Chart View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
View Filters	Add/Edit Filters View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Dashboard Prompt	Add/Edit Dashboard Prompt View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Performance Tile	Add/Edit Performance Tile View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Heat Matrix	Add/Edit Heat Matrix View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Static Text	Add/Edit Static Text View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Javascript view	Edit Javascript View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Legend	Add/Edit Legend View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Map	Add/Edit Map View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Narrative	Add/Edit Narrative View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View No Results	Add/Edit No Results View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Pivot Table	Add/Edit Pivot Table View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Generic Plugin View	Add/Edit Generic Plugin View View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Report Prompt	Add/Edit Report Prompt View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Create Segment	Add/Edit Create Segment View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Selection Steps	Add/Edit Selection Steps View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Logical SQL	Add/Edit Logical SQL View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Table	Add/Edit Table View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Create Target List	Add/Edit Create Target List View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Ticker	Add/Edit Ticker View	Oracle Argus Insight Author Role, BI Service Administrator
View Title	Add/Edit Title View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Treemap	Add/Edit Treemap View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View Trellis	Add/Edit Trellis View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
View View Selector	Add/Edit View Selector View	Oracle Argus Insight Author Role, Oracle Analytics Service Administrator
Write Back	Manage Write Back	Oracle Argus Insight Admin Role, Oracle Analytics Service Administrator

Component	Privilege	Default Role Granted
Write Back	Write Back to Database	Denied: Authenticated User

23

Configure Argus Centralized Coding

You must execute the following batch files to set up the Argus Centralized Coding Interface schema and to migrate encoded terms for all cases to the Interface schema:

- setup_centralized_coding_interface_schema.bat
- dms_migration.bat

setup_centralized_coding_interface_schema.bat

This batch file creates the schema objects for the Argus Centralized Coding Interface schema.

This script also updates the coding status field with the current status for existing cases for the following fields. The code status fields displays whether all events are encoded and are in a coding state or if the case has items that can be coded but are not coded.

- LM_LAB_TEST_TYPES.CODE_STATUS
- LM_LABELED_TERMS.CODE_STATUS
- LM_PRODUCT.IND_CODE_STATUS
- CASE_EVENT.CODE_STATUS
- CASE_DEATH_DETAILS.CAUSE_CODE_STATUS
- CASE_PROD_INDICATIONS.IND_CODE_STATUS
- CASE_PAT_HIST.ITEM_CODE_STATUS
- CASE_ASSESS.DIAGNOSIS_CODE_STATUS

For more information, see:

- Execute the Batch File

Execute the Batch File

1. Double-click the **setup_centralized_coding_interface_schema.bat** file and enter:
   a. Log folder name
   b. Database name
   c. DBA user credentials, such as system and password
   d. RLS schema owner name and password

      Execute the following query to get the RLS schema owner name:

      ```
      SELECT owner
      FROM all_objects
      WHERE object_name = PKG_RLS AND object_type = PACKAGE;
      ```

   e. Argus schema owner name, such as ARGUS_APP and password
   f. Argus Safety role name

   The script creates two users, ARGUS_DMS and DMS_LOGIN, and their tablespaces.

The Interface schema object is present in the ARGUS_DMS schema.

2. Enter the following:
   a. Password for user ARGUS_DMS.
   b. Password for user DMS_LOGIN.
   c. Temporary tablespace name.

      If no input is provided, TEMP tablespace is taken by default.

      The script creates two tablespaces: DMS_DATA_01.DBF, and DMS_INDEX_01.DBF.
   d. Path and data file name of the tablespaces, such as:

      C:\APP\ORADATA\DBNAMD\DMS_DATA_01.DBF

      C:\APP\ORADATA\DBNAMD\DMS_INDEX_01.DBF
   e. A log file name
3. Press Enter when the Users and Roles are located.
4. Check the log file to validate the successful completion of the script.
5. Log in to the application and enable the Centralized Coding module.

   Configure Centralized Coding from the dictionary selection page in the Console.

dms_migration.bat

Execute this script to populate the already encoded terms from all cases to the Interface schema table. This script supports two types of migration:

- Single Enterprise Migration in One Execution
- All Enterprise Migration in One Execution

Single Enterprise Migration in One Execution

To migrate encoded terms for case data for a particular enterprise, enter an enterprise_id such as *1*.

All Enterprise Migration in One Execution

When you have multiple enterprises in the Oracle Argus Safety multi-tenant environment:

- To migrate encoded terms of case data for one enterprise only, enter only one enterprise_id such as 1 when prompted.
- To migrate encoded terms of case data for all enterprises in one go, enter input as ALL when prompted.
- To migrate encoded terms of case data for some enterprises (but not all), the number of executions of `dms_migration.bat` = Migration of encoded terms of case data for the number of enterprises.

> **Note**
>
> This migration script does not check whether the Argus Centralized Coding module is enabled for any specific enterprise. You must verify that module is enabled and then migrate data for enterprises.
>
> To populate terms to the Interface table, you must load MedDRA into the Argus schema.
>
> The migration script populates already encoded terms from all cases to the Interface table. Any open cases in the application are processed during migration.

Execute the batch file `dms_migration.bat` and enter the following:

1. Log folder name
2. Log file name
3. TNSNAMES of the Oracle Argus Safety database when the Interface schema was created
4. Oracle Argus Safety schema owner name and password
5. Based on whether you want to migrate coded terms for all cases, one enterprise or for multiple enterprises:

   i. Enter the enterprise_id of one enterprise to migrate data for that particular enterprise.

   ii. Enter ALL as Input to migrate data for all enterprises.

   iii. To migrate coded terms of cases for more than one enterprise, execute step (i) multiple times and provide different enterprise_ids.
6. Application user name

   If no input is provided, *admin* is taken as user input.
7. Check the log file to validate successful completion of the script.

24

Extract, Transform, and Load Data

This chapter describes the steps required to run and work with the initial extract, transform, and load (ETL) process:

Prerequisites, Cautions, and Warnings

Before running the Initial ETL, make sure:

- The Auto extend is set to ON for all the data files in the database that are related to staging and Oracle Argus Insight Mart.
- The POPULATE CASE/CONFIGURATION DATA profile switch is configured to the desired value.

In addition, note that:

- Since the initial ETL requires a huge amount of temporary space, set the temporary space to 100 GB to prevent data errors. After completing the Initial ETL, reduce the temporary space to 30 GB.
- After the Initial ETL completes, the balancing log may show differences between the Oracle Argus Safety (Stage) and Oracle Argus Insight Mart table counts. This is because of the derivation rules applied to the Oracle Argus Insight data mart.
- The system may display the following message:

  `Warning !!! - Could not locate MedDRA-J User in the Argus Database.`

  Ignore this warning for all MedDRA tables.
- **Do not** run incremental ETL for more than 50,000 cases. Run the Initial ETL again if the number of cases exceeds 50,000.
- The Oracle Argus Insight Insight ETL will not populate the Oracle Argus Mart database.

  Refer to the *Oracle Argus Mart Installation and Administration Guide* for more information on the Oracle Argus Mart ETL.

Run the Initial ETL

1. Log in to the Oracle Argus Insight Web Server as a user with administrator privileges.
2. Click **Start**.
3. Navigate to **Oracle** > **Argus Insight**, and then select **Insight ETL Tool**.
4. Click **Initial ETL**.

The Oracle Database Connect dialog box appears.

5. To connect to the Oracle Database:
   a. In the **User** field, enter the user name (AI_APR_MART user name in the AI database).
   b. In the **Password** field, enter the password for the user.
   c. In the **Database** field, enter the name of your Oracle Argus Insight database.
   d. Click **OK**.

   The Initial ETL Status dialog box opens.
6. Click **Start ETL**.

   The initial process of extracting, transforming, and loading data begins. A message confirming that you have completed the required configuration steps appears.
7. Click **Yes** if these items have already been configured.

   The Initial ETL Status dialog box appears stating the ETL start time, the progress bar, and the current process in execution.

   While the ETL is in progress, you can:

   - To close the dialog box, and exit from the Insight ETL Tool, click **Close**.

     Closing the dialog box does not affect the execution of the ETL process.
   - To halt the ETL process, click **Stop ETL**.

     For more information about this option, see Stop the Execution of ETL.

   A status message appears when the initial ETL process is completed.

For more information, see:

- Generate the Balance Logs
- Close the Initial ETL Status Dialog Box
- Stop the Execution of ETL

Generate the Balance Logs

When the system successfully completes the Initial ETL process, you should generate and check the logs.

To generate the balance logs:

1. Wait until the dialog box that reports the initial ETL completed successfully appears.
2. Click **Balancing Logs**.

   A dialog box appears to confirm that you want to generate balancing logs for the completed Initial ETL appears.
3. Click **OK**.

   The command prompt screen appears.
4. Enter the password for the **APR_MART** user, and press **Enter**.
5. Verify that the script is successfully connected as *APR_MART User Name@Argus Insight Database Name*, and press **Enter**.

   The command prompt screen appears and the balancing logs are generated.

When the logs are generated, a dialog box with the location and name of the log files appears.

6. Click **OK** to close the dialog box.
7. Open and verify the contents of each Balancing Report.

   The Balancing Reports are located at:

   drive:`\VSS SOURCE\Argus Insight\Main Source\Database Source\DBInstaller`

   The log files are named as:

   - `etl_ini_atos_bal_lm_cfg_rep.log`
   - `etl_ini_atos_bal_rep.log`
   - `etl_ini_stom_bal_lm_cfg_rep.log`
   - `etl_ini_stom_bal_rep.log`

Close the Initial ETL Status Dialog Box

1. Click **Close**.

   A message to confirm that you want to close the Oracle Argus Insight ETL Tool application appears.
2. Click **OK**.

Stop the Execution of ETL

You may choose to stop an ETL in progress.

To halt the execution of the initial ETL process:

1. Click **Stop ETL**.

   A message to confirm that you want to stop the ETL currently in progress appears.
2. Click **OK**.

   The ETL process is stopped and returns to the Initial ETL Status dialog box.

   At this point, you can select one of the following options:

   - To continue extracting, transforming, and loading the data that was in progress, click **Continue**.
   - To start the initial ETL from the beginning, click **Restart ETL**.
   - To exit from the Oracle Argus Insight ETL Tool application, click **Close**.

Run the Initial ETL Again

To start the ETL process from the beginning:

1. Click **Run ETL**.

   A message to confirm whether you want to start the initial ETL from the beginning appears.
2. Click **OK**.

   The Database Connect dialog box appears.

3. Enter the password for the APR_MART user, and then click **OK**.

The initial ETL process starts from the beginning.

Process a Failed ETL

The initial ETL may fail due to an error. If an error occurs, the system stops processing the ETL and displays error message.

You may choose any of the following options for the failed Initial ETL process:

- To continue the failed Initial ETL process, click **Continue**.
- To ignore the failed Initial ETL process, click **Ignore**.
- For ETL Data Exclusion, click **Modify Attributes**, if PRE_REQ_CHECK_FLAG switch is set to ABORT.

> **Note**
>
> These modifications must be done before running the Initial ETL process.

For more information, see:

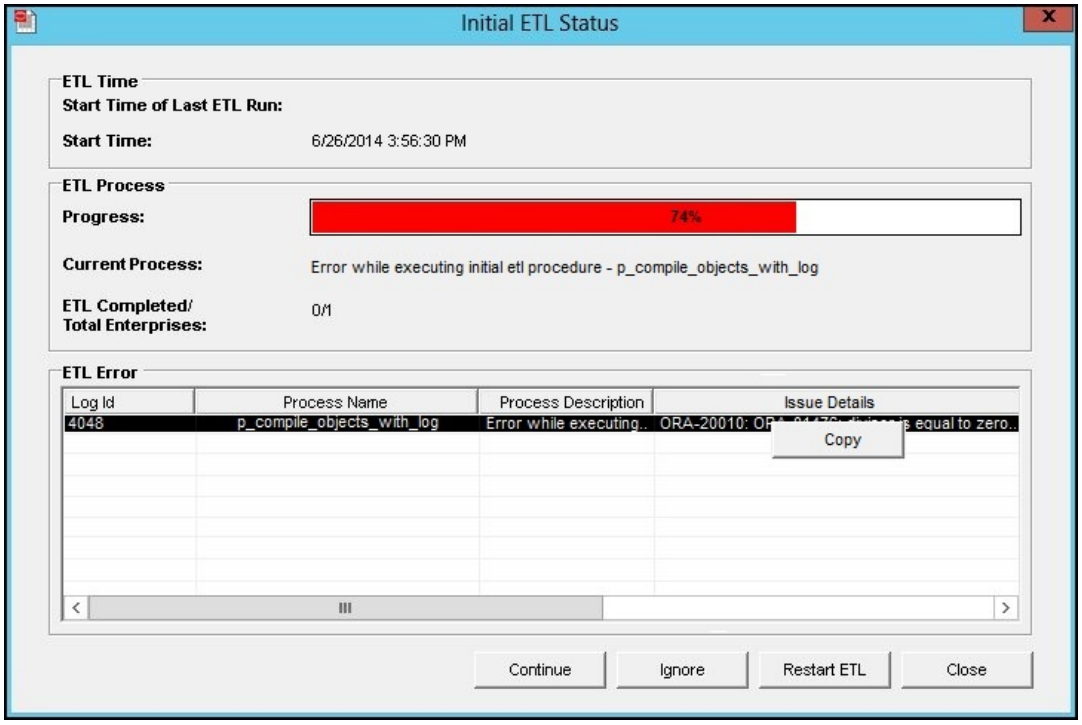
- Continue the Failed Initial ETL Process
- Ignore the Failed Initial ETL Process
- Modify the Attributes of ETL Data Exclusion

Continue the Failed Initial ETL Process

To continue the Initial ETL process from the failed ETL procedure:

1. Double-click on the ETL error.

   The Error Data dialog box appears with details of the error.
2. Review the error information, and then click **OK**.
3. Right-click on the ETL Error, and click **Copy** to copy the error data.



4. Click **Continue** to continue the failed ETL process.

   A message to confirm that you want to start the initial ETL from the stopped process appears.

5. Click **OK**.

   The ETL process continues (if no errors are found).

Ignore the Failed Initial ETL Process

To ignore a failed ETL process and continue with the next process in the ETL:

1. Click **Ignore**.

   A message to confirm that you want to skip the failed process and continue executing the Initial ETL with the next process appears.

2. Click **OK**.

The Initial ETL begins from the next process and continues with the ETL process (if no errors are found).

Modify the Attributes of ETL Data Exclusion

You must modify these attributes before ETL execution.

1. Log in to the Oracle Argus Insight application as a user with administrator privileges.
2. On Oracle Argus Insight home page, from the upper-right corner, click the **Tools** tab.

   The Administration Tools screen appears.

3. Click the **List Maintenance** tab.
4. Select **Profile Switches** from the List Maintenance Items group.

   The Attributes group is updated with the profile switches that you can modify.

5. Select **ETL Data Exclusion**, and click **Modify**.

   The Modify Attribute dialog box appears.

6. Click the **Value** field, and enter one of the following values:

   - If you want the ETL process to skip cases with erroneous data and continue processing all other cases, enter **IGNORE**.
   - If you want the ETL process to abort when it encounters cases with erroneous data, enter **ABORT**.

7. Click **OK** to save the changes and return to the List Maintenance tab.

Restart the Initial ETL Process

To restart the Initial ETL process starting from after the confirmation message and APR_MART password input:

1. Click **Restart ETL**.

   A message to confirm that you want to start the initial ETL from the beginning appears.

2. Click **OK**.

   The Oracle Database Connect dialog box appears.

3. Enter the APR_MART user password, the Oracle Argus Insight Database name, and click **OK**.

4. Click **Start ETL** to start the initial process of extracting, transforming, and loading data.

   A message to confirm that you have completed the required configuration steps appears. See Section 5.2 > Step 6.

5. Click **Yes** if these items have already been configured.

   The Initial ETL Status dialog appears with the ETL start time, the progress bar, and the current process in execution.

   When the system finishes the ETL process, click **Close**.

Part V
Secure Oracle Argus Safety

In this chapter:

25

Oracle Argus Safety Password Management—Cryptography Tool

Oracle Argus Safety uses dynamically generated encryption keys for passwords within the system. The Cryptography Key Editor allows you to generate a dynamic key and then encrypt passwords using the said key. The generated key must be installed on each application server and must be common to allow all servers to communicate with the Oracle Argus Safety database.

The key is stored in the `ArgusSecureKey.ini` file located in the .\Windows folder.

IMPORTANT: During a new environment installation, a key will need to be generated **prior to** creating a database.

During an upgrade, a key will need to be generated prior to upgrading or an existing key from the existing setup can be used to perform the database upgrade. Make sure that the password information specified in the database is consistent with the information provided in the `ArgusSecureKey.ini` file.

> **Note**
>
> When the `ArgusSecureKey.ini` file is generated, there is no need to run this tool again while launching the Oracle Argus Safety Crypto Tool. The tool should only be run again:
>
> - if you are resetting passwords or keys
> - if you have lost the ArgusSecureKey.ini file
> - if you are setting the Argus Bridge schema password

When the key file is created, copy it to the .\Windows folder on all application servers (web, transaction, etc.).

> **Note**
>
> Do not run the Cryptography Key Editor on each application server to generate passwords. It need only be run once during the initial system setup. Subsequent server installations must have the key manually copied to each .\Windows folder.

For more information, see:

- Cryptography Key to Install or Upgrade Oracle Argus Safety
- Reset Password or Change the Cryptography Key
- Manage Oracle Argus Insight Cryptographic Key

Cryptography Key to Install or Upgrade Oracle Argus Safety

Whether you are upgrading to the latest Oracle Argus Safety or installing a fresh instance of it, you must generate new key using the Cryptography Key Editor.

> **Tip**
>
> Install the Oracle Argus Safety Crypto Tool and Oracle Argus Insight Crypto Tool on the Transaction Server.

Generate New Cryptography Key

You must generate the `ArgusSecureKey.ini` key file before running the Oracle Argus Safety Crypto Tool.

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.

2. Click **New**.

   The Generate Key screen appears.

3. In the **Note to be added as comment** field, enter a comment that will be saved in the `ArgusSecureKey.ini`.

   This can be any form of metadata, such as the reason why this key was generated or for what environments it is used.

4. Enter ARGUSUSER password and Confirm password.

5. (Optional) Enter APR_USER password and Confirm password.

   This field applies to the Oracle Argus Insight user. If Oracle Argus Insight is not installed along with Oracle Argus Safety, leave this field blank.

6. Click **OK**.

   The `ArgusSecureKey.ini` file is created in the <*Install folder*>\CryptoKeyEditor\output\<DateTimeStamp>\.

7. Click the link in the **Argus Secure Key Path** dialog box to open the folder in Windows Explorer.

8. Click **Close, I will copy it manually** and copy the file manually from the window that gets opened by clicking on the link mentioned above.

9. To move the generated `ArgusSecureKey.ini` file to the .\Windows folder, click **Copy to windows folder**.

Create or Upgrade Oracle Argus Safety Database

Run the Oracle Argus Safety Crypto Tool to create or upgrade the database. If you run the Oracle Argus Safety Crypto Tool before creating the key, a warning message appears that the cryptography key is required.

Oracle Argus Safety Application Servers

After the application servers are set-up:

1. From the server where the database is created or upgraded, go to the `.\Windows` folder, and copy the `ArgusSecureKey.ini` file.
2. Paste this file in the `.\Windows` folder of each installed application server.

Reset Password or Change the Cryptography Key

Reset the ARGUSUSER Password

If the password for the database user ARGUSUSER has changed, you will need to reset the password in the `ArgusSecureKey.ini` file on all the servers.

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.
2. Click **Existing**.

   The Key Editor Login or Re-encrypt ARGUSUSER screen appears.
3. Enter the ARGUSUSER password.
4. Enter the APR_USER password.

   This field appears only when you have installed Oracle Argus Insight along with Oracle Argus Safety.
5. Enter the database name.
6. Click **Re-encrypt**.

   A confirmation dialog appears.
7. Click **Yes**.
8. Copy the updated `ArgusSecureKey.ini` file from the `.\Windows` folder to all the `.\Windows` folder of all the application servers.
9. Verify that you can Log in to the Oracle Argus Safety application.

Edit Keys

An administrator might want to change a key due to various reasons like a policy to change key every few days, or to avoid network compromise, etc.

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.

2. Click **Existing**.

   The Key Editor Login or Re-encrypt ARGUSUSER screen appears.

3. Enter the ARGUSUSER password.

4. Enter the APR_USER password.

   This field appears only when you have installed Oracle Argus Insight along with Oracle Argus Safety.

5. Enter the database name.

6. Click **Login**.

   The Key Editor Options for Existing Installation screen appears.

7. Enter the DBA User Name and User Password.

8. Click **Validate**.

9. Select the **Edit Key** checkbox.

   This enables the child checkboxes of **User Key** and **Cookie Key**.
   The **User Key** is used for all the encrypted strings which are persisted in the database or file server.

   The **Cookie Key** is only used to encrypt and decrypt the key.

   The user has the option to change either one or both keys.

10. Select the checkboxes in front of the key that you want to change.

11. Change the Key Size drop-down value, if you wish to change the key size. Key Size is measured in bits of the key used in a cryptographic algorithm.

12. Click **Re-Generate**.

    This will change the value of the checked items and the new value will be visible in the textbox.

13. Click **Execute**.

    The Reason for this Action dialog box appears, prompting the user to add a reason for his action.
    The text entered here is visible in the Audit Log in the Oracle Argus Safety application.

14. Click **OK**.

15. Check the status box to verify if the operation has been successful.

16. If the operation is successful and the Cryptography key is checked, then the changed key is now stored in the `ArgusSecureKey.ini`.

    You should now copy this file from the .\Windows folder of the current machine and paste it to the `.\Windows` folder of all web servers.

17. When the user key is changed, all the encrypted strings in the database are re-encrypted using the new key.

However, there are still some other file server locations where this key change must also be applied manually. The following is a list of places where the changes must be done manually:

18. Items to be changed from the User Interface:

String	Description
Argus Services	Open Argus Safety Service Configuration: Open all the processes and enter password again.
Cyclone	Open ESM Mapping utility and re-enter the Cyclone password.
ESM Common User	Open ESM Mapping utility and re-enter the ESM Common User password.

Re-encrypt Common User Passwords

The Key Editor Options for Existing Installation screen can also be used to change the common user (ARGUS_LOGIN, ARGUS_LOGIN_I, and ARGUS_LOGIN_IPS) passwords.

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.
2. Click **Existing**.

   The Key Editor Login or Re-encrypt ARGUSUSER screen appears.
3. Enter the ARGUSUSER password.
4. Enter the APR_USER password.

   This field appears only when you have installed Oracle Argus Insight along with Oracle Argus Safety.
5. Enter the database name.
6. Click **Login**.

   The Key Editor Options for Existing Installation screen appears.
7. Enter the DBA User Name and User Password.
8. Click **Validate**.
9. Check the **Re-encrypt** checkbox.
10. Enter the passwords for the common users.
11. Click **Execute**.

    The Reason for this Action dialog box appears, prompting the user to add a reason for his action.
12. The text entered here is visible in the **Audit Log** in the Oracle Argus Safety application.
13. Click **OK**.
14. Check the status box to verify if the operation has been successful.

Generate Encrypted String

Generate the encrypted string from clear text, using the configured UserCryptoKey in `ArgusSecureKey.ini`.

1. Launch the **Cryptography Key Editor**.

The Key Editor Utility screen appears.

2. Click **Existing**.

   The Key Edit Login screen appears.

3. Enter the ARGUSUSER password.
4. Enter the APR_USER password.

   This field appears only when you have installed Oracle Argus Insight along with Oracle Argus Safety.

5. Enter the database name.
6. Click **Login**.

   The Key Editor Options for Existing Installation screen appears.

7. Enter the DBA User Name and User Password.
8. Click **Validate**.
9. Check the **Generate Encrypted** checkbox.
10. Enter the password in the **Clear text** field.
11. Click **Execute**.

    The Reason for this Action dialog box appears, prompting the user to add a reason for his action.

12. The text entered here is visible in the **Audit Log** in the Oracle Argus Safety application.
13. Click **OK**.
14. Check the status box to verify if the operation has been successful. If the operation is successful, the encrypted script gets displayed in the **Encrypted String** field.

Create Argus Bridge Keys

To generate bridge keys on all Web and Transaction servers, see Configure Argus Bridge.

Reset Administrator and System Application User Password

1. Launch the **Cryptography Key Editor**.

   The Key Editor Utility screen appears.

2. Click **Existing**.

   The Key Editor Login screen appears.

3. Enter the ARGUSUSER password.
4. Enter the APR_USER password.

   This field appears only when you have installed Oracle Argus Insight along with Oracle Argus Safety.

5. Enter the database name.
6. Click **Login**.

   The Key Editor Options for Existing Installation screen appears.

7. Enter the DBA User Name and User Password.
8. Click **Validate**.

9. Check the **Reset password for the default Administrator and System Accounts** checkbox.
10. To set **Administrator** password, select the respective checkbox, and enter the parameters.
11. To set **System** user password, select the respective checkbox and enter the parameters.
12. Click **Execute**.

    The Reason for this Action dialog box appears, prompting the user to add a reason for his action.
    The text entered here is visible in the **Audit Log** in the Oracle Argus Safety application.
13. Click **OK**.
14. Check the status box to verify if the operation has been successful.

Reset the Environment if ArgusSecureKey.ini is Lost

1. To generate a new key and copy it to the Windows folder, follow the steps listed in the Reset the ARGUSUSER Password.
2. To re-encrypt common user passwords, follow the steps listed in the Re-encrypt Common User Passwords.
3. Re-encrypt strings in the following locations:

String	Description
LDAP	Clear column LDAP_SEARCH_PASSWORD in all rows from table CFG_LDAP_SERVERS. Now open **Argus Console** > **System Configuration** > **System Management** > **LDAP** and re-enter passwords for all configurations.
SMTP	Clear column USER_PASSWORD in all rows from table CFG_SMTP. Now open **Argus Console** > **System Configuration** > **SMTP Configuration** and re-enter passwords for SMTP account.
Argus Services	Open Argus Safety Service Configuration: Open all the processes and enter password again.
Cyclone	Open ESM Mapping utility and re-enter the Cyclone password.
ESM Common User	Open ESM Mapping utility and re-enter the ESM Common User password.

Manage Oracle Argus Insight Cryptographic Key

- Update APR_USER Password
- Copy Initialization Files to Other Servers
- Restart IIS and Run ETL

Update APR_USER Password

When Oracle Argus Insight is installed and you have an If you have the `ArgusSecureKey.ini` file, updated the APR_USER password in `ArgusSecureKey.ini`

1. Log in to **Argus Insight Client**.
2. Click **Start**.

3. Navigate to **Programs > Oracle > Argus Crypto Tool**.

   Or, go to: `C:\Program Files\Oracle\Argus\ArgusCrypto`
   The Argus Key Editor Utility screen appears.
4. Click **Existing**.
5. Select the **Re-encrypt** option.
6. From the drop-down list, select **APR_USER**, enter the parameters, and click **Re-encrypt**.

   The system updates the password for APR_USER.

Copy Initialization Files to Other Servers

After you change the cryptography key using the Key Management tool, you must manually copy the `ArgusSecureKey.ini` initialization file from the `C:\Windows` folder of the Oracle Argus Insight Web Server to the following folders:

- C:\Windows of all Oracle Argus Insight Web Servers

You must copy the `ArgusSecureKey.ini` file to keep the cryptography key and the APR_USER password in sync on all the servers. In case these files are not copied or any other Oracle Argus Insight Web Server will not function.

Restart IIS and Run ETL

After you change the cryptography key, you must complete the following steps on the Oracle Argus Insight Web Server to reflect the changes:

1. Restart the **Internet Information Services (IIS)**.
2. Run the incremental ETL.

A

Create ODBC Connection for OAS Administration Tool for Oracle Argus Insight

This appendix comprises the steps to create ODBC connection for OAS Administration tool.

1. Navigate to **Control Panel** > **All Control Panel Items** > **Administrative Tools**.
2. Double-click **Data Sources (ODBC) (64-bit)**.
   The ODBC Data Source Administrator (64-bit) dialog box appears.
3. From the System DSN tab, and click **Add**.
   The Create New Data Source dialog box appears.
4. From the list of the available drivers, select **Oracle BI Server**, and click **Finish**.
   The Oracle BI Server DSN Configuration dialog box appears.
5. Enter the following fields:
   a. **Name**—AIOAS (or any name)
   b. **Description**—Oracle Argus Insight OAS (or any description)
   c. **Server**—OAS Server Name
6. Click **Next**.
   a. **Login ID**—weblogic
   b. **Password**—<password for weblogic>
   c. **Port**—The port must be same as mentioned in the Managed Server port list for OAS Server.
      To retrieve this port, go to **Enterprise Manager** > **BI Instance** > **Availability** tab.
7. Click **Next**.
   The Oracle BI Server DSN Configuration dialog box appears.
8. From the list of database, select **AI80_SRC**.
9. Click **Finish**.