Oracle Life Sciences Safety One Argus

Cloud Service Administration Guide

Release 2026.1.01
G53134-01
March 2026

ORACLE

Oracle Life Sciences Safety One Argus Cloud Service Administration Guide, Release 2026.1.01

G53134-01

Contents

Preface

Intended Audience i
Related resources i

1 Get started with Oracle Cloud Service Administration

About Oracle Argus Cloud Service 1
How Oracle Argus Cloud Service differs from the on-premise version 2
Begin with Oracle Argus Cloud Service subscriptions 3
Components of your Oracle Argus Cloud Service subscription 3
Oracle Argus Cloud Service architecture 6
Get your administrator account credentials 6
What you do as an administrator 8
Sign in for the first time 8
Environments you can access 9

2 Manage sites, groups, and users

Manage sites 1
- Add user sites 1
- User sites fields descriptions 3
- Site configuration printout 3

Manage groups 3
- Groups included with the Oracle Argus Cloud Service 4
- About user groups 4
- Add Argus user groups 4
- Add local affiliate user groups 6
- User groups fields description 7
- Users belonging to multiple groups 7
- Print a group configuration list 8
- Group configuration printout 8

Manage users 9
- Manage users with Oracle Identity Cloud Service (IDCS) 9
  - Create users in IDCS 10

Create groups in IDCS 10
Assign groups to user accounts in IDCS 12
Deactivate users in Argus Cloud Service 13
Reset a user password 13
Print a user configuration list 14
User migration in Oracle Identity Cloud Service (IDCS) 14
User onboarding 15
About the IDCS report for importing users and groups 22
User group migration from IDM to IDCS 23
Export user group information from IDM 24
Import user group information to IDCS 26
Validation, comparison reports and how to take corrective action 26
User and group import status report 31
General admin activities 32
Case studies for user migration 33
Add users to Oracle Argus Cloud Service 33
Users fields description 34
Filtering sites, groups and users 36
Applying filters to users and groups 37

3 Manage Argus Advanced Cloud Service

Create a new enterprise in Oracle Argus Mart 1
Extract, Transform and Load data (ETL) 2
Run the initial ETL 2
Schedule incremental ETLs 3
Re-initialize the ETL process 4
Replicate your data 5
Grant users with Oracle Argus Analytics access 5
Oracle Analytics Server (OAS) and Oracle Analytics Publisher user types 6
Oracle Analytics Server (OAS) and Oracle Analytics Publisher user roles 6
Oracle Analytics Server (OAS) and Oracle Analytics Publisher users examples 7
About Product Verification Pack (PVP) 8
Obtain a Product Verification Pack 8

4 Manage dictionaries

5 Use the Argus Cloud Service utilities

Data Refresh 1
Data Refresh Enterprise Specific 2

Extensibility and Integrations Framework 2
Gateway Certificate Expiry Alert Notification 4
Monitoring 6
Usage Billing 7
Enterprise Export 7

6 View the Interchange logs

7 Manage integrations

Use the federated identity Single-Sign On (SSO) 1
Enable Federated Identity SSO through SAML 2.0 2
Manage sFTP user access 2
Add an sFTP user 2
Renew the sFTP account certificate 3
Remove an sFTP user account 4
Configure SMTP 5
Configuring Argus Bridge for document management 7
Configuring Translation Service 7
Narrative Generation using OCI Gen AI 9
System Configuration 9
Analysis tab 10
Feedback 11
Identity Cloud Service (IDCS) 12
IDCS Reports 13
Federation Setup in IDCS 13
Mixed mode authentication support in IDCS 14
Password policy management in IDCS 14
Notifications in IDCS 15
Password expiry notification in IDCS 15
Muti-factor authentication in IDCS 15

8 Gateway administration

Implement gateway UI access in your Argus Cloud environment 1
Request gateway UI access 1
Grant users with Axway UI access 2
Grant users with Oracle B2B UI access 3
Request creating a trading partner or community from the Life Sciences Customer Support Portal 4
Configure Axway B2Bi to transmit reports 5
Before you begin configuring Axway B2Bi 6

Request adding a trading engine node 7
Create a community 8
Add a partner to a community 8
Create application pickups 9
Add an application pickup to a community (all agencies) 9
Add an application pickup to a community for Drugs (FDA) 11
Add an application pickup to a community for Device Reporting (FDA) 12
Add an application pickup to a community for Vaccine (FDA) 13
Specialize collaboration settings 14
Specialize collaboration settings for a partner (FDA) 15
Specialize collaboration settings for a partner (PMDA) 15
Set up application delivery 16
Update the incoming rule for Delivery Settings for each Partner 17
Add a trading pickup to a community 17
Add public URL configuration in trading pickup (Pharma Company URL) 18
Add partner encryption certificate 18
Add partner SSL certificate 19
Add public URL configuration in trading pickup 19
Post-configuration step: Transmit the generated report 20
Typical workflow for transmitting regulatory reports to agencies/partners 20

9 Get support for Oracle Argus Cloud Service

What Oracle Support services are available to Argus Cloud Service customers? 1
Work with your CSDM (Cloud Service Delivery Manager) 1
About Cloud Service Delivery Manager (CSDM) 2
CSDM is your single point of contact for Cloud Service support 2
What happens at your regular CSDM Governance call? 2
Your Oracle Argus Cloud Maintenance calendar 3
About change management 3
Use the Life Sciences Customer Support Portal to access the Oracle Support Cloud 4
Oracle Argus Cloud Service support overview 4
About support and change request features 4
Register your account 5
Log in to the Life Sciences Customer Support Portal 5
About the three types of access to the Life Sciences Support Cloud 6
Field entries common to all request types and products 6
Email notifications from the Life Sciences Support Cloud 7
You can still use Oracle and third-party consulting services 8

Preface

This preface contains the following sections:

- Intended Audience
- Related resources

Intended Audience

This document contains information intended for Oracle Argus Cloud Service customer-delegated administrators (CDA) to understand roles and responsibilities around administration tasks.

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.

1

Get started with Oracle Cloud Service Administration

This document contains information intended for Oracle Argus Cloud Service administrators to understand their role and responsibilities.

- About Oracle Argus Cloud Service
  Oracle Argus Cloud Service is a component of the Oracle Safety Cloud, a simplified package of access, environment, and services in a subscription model.
- How Oracle Argus Cloud Service differs from the on-premise version
  Oracle Argus Cloud Service differs from the on-premise version of Argus in ownership status, billing and costs, release management, and support.
- Begin with Oracle Argus Cloud Service subscriptions
  Oracle Argus Cloud Service requires a subscription license.
- Components of your Oracle Argus Cloud Service subscription
  Your organization has subscribed to either Oracle Argus Basic Cloud Service or Oracle Argus Advanced Cloud Service.
- Oracle Argus Cloud Service architecture
  This is a diagram of the Oracle Argus Cloud Service architecture, including the components of the Oracle Argus Advanced Cloud subscription.
- Get your administrator account credentials
  As primary point of contact for your company, Oracle must provision your account as Customer-Delegated Administrator (CDA) before you can start managing Oracle Argus Cloud Service.
- What you do as an administrator
  As administrator, you have specific tasks and permissions in Oracle Argus Cloud Service.
- Sign in for the first time
  Sign in to set up your account and define your own password.
- Environments you can access
  Oracle provides your company with one production environment and one non-production environment.

About Oracle Argus Cloud Service

Oracle Argus Cloud Service is a component of the Oracle Safety Cloud, a simplified package of access, environment, and services in a subscription model.

With Oracle Argus Cloud Service, there are no licenses or support contracts. You access the application via the Oracle Life Sciences Cloud. Data centers cover all global regions and you use the same cloud as Oracle clinical and healthcare applications.

Oracle Argus Cloud Service includes:

- **Infrastructure Management Services:** Infrastructure, network, firewalls, switches, data center, and physical server maintenance.

- **Platform Management Services:** Virtual machine, operating system, database, and middleware management.
- **Application Management Services (AMS):** Full lifecycle application management including deployment, upgrading, and patching.
- **Dictionary Data Services:** Loading of dictionary updates (when subscribed), execution of recoding runs.

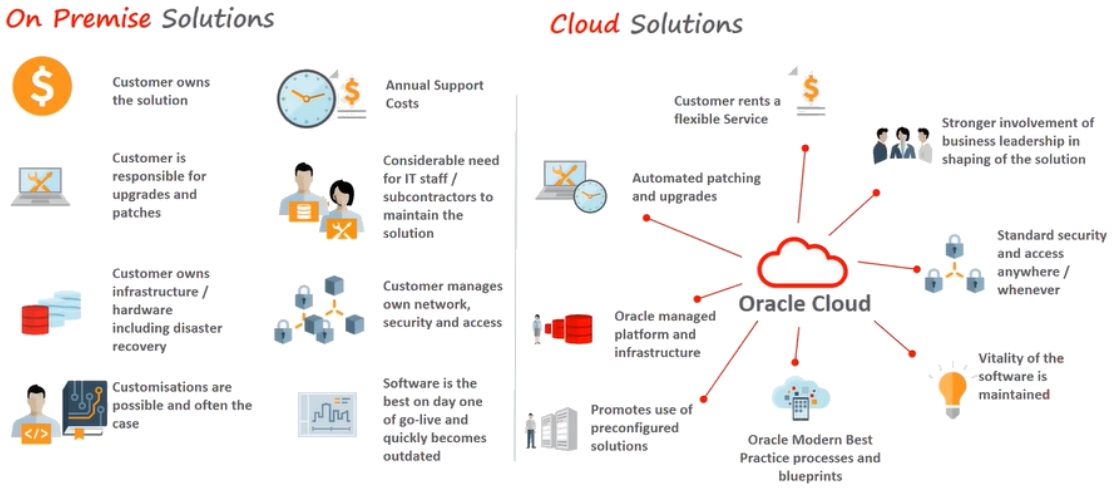
If you subscribe to Oracle Argus Advanced Cloud Service, an annually reviewed Disaster Recovery environment is also included. Oracle implements the plan in the event of a disaster. The target is a system availability of 99.5 percent and recovery within 24 hours.

> **Note**
>
> Your organization has subscribed to either Oracle Argus Basic Cloud Service or Oracle Argus Advanced Cloud Service. According to your subscription type, you can access certain Argus Cloud modules. For more information, refer to Components of your Oracle Argus Cloud Service subscription.

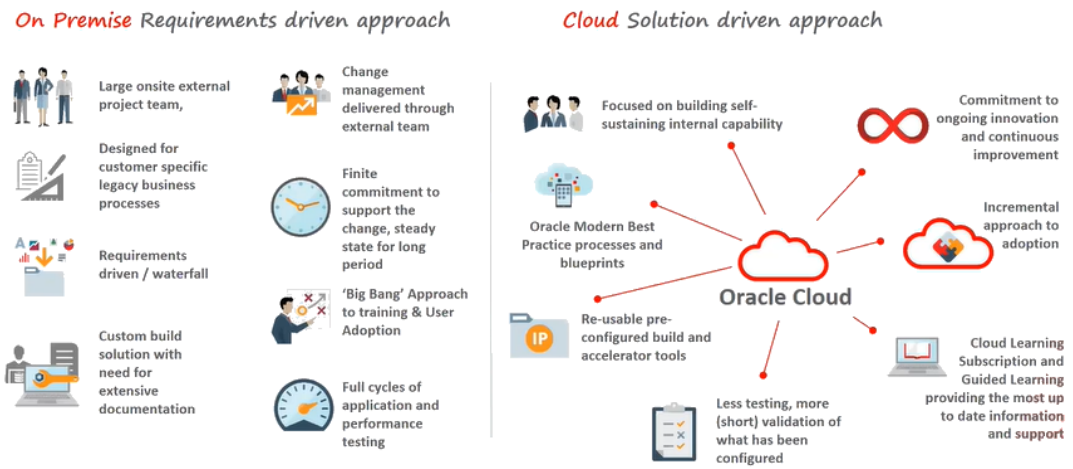
How Oracle Argus Cloud Service differs from the on-premise version

Oracle Argus Cloud Service differs from the on-premise version of Argus in ownership status, billing and costs, release management, and support.

Cloud Service solutions are different



Cloud implementations are different



Begin with Oracle Argus Cloud Service subscriptions

Oracle Argus Cloud Service requires a subscription license.

Prior to Oracle's installation of your software, you must provide evidence of licenses with the following third-party software:

- Microsoft Windows Server Standard/ Enterprise Edition
- MedDRA Dictionary
- WHO-Drug Dictionary

> **Note**
>
> For a detailed description of third-party softwares, see the Software Requirements chapter from the *Oracle Argus Safety and Oracle Argus Insight Installation Guide*.

Components of your Oracle Argus Cloud Service subscription

Your organization has subscribed to either Oracle Argus Basic Cloud Service or Oracle Argus Advanced Cloud Service.

You can access certain Argus Cloud modules, based on your subscription type:

- Oracle Argus Basic Cloud Service
- Oracle Argus Advanced Cloud Service

Oracle Argus Basic Cloud Service components

An Oracle Argus Basic Cloud Service subscription allows access to the following modules, which are the base components of Argus Cloud:

Component	Description
Oracle Argus Safety	Oracle Argus Safety enables you to: • Process case intake and attachment (adverse events received via email, phone, fax, E2B, or API) • Triage with duplicate checking **Note** For a fresh install or for a new cloud user, the **Enable smart duplicate search** option is enabled by default. For cloud users upgrading to version 25.1, this switch is disabled by default. • Leverage company-specific workflow processing • Manage comprehensive global adverse events (AE) data entry, coding, and review • Perform a quality review • Perform a Medical Assessment/Review - narrative, causality, seriousness, etc • Produce (print, fax, E2B message email) expedited and periodic regulatory reports • Perform submission tracking • Perform follow-up processing • Perform optional case report translation.
Oracle Argus Affiliate	Oracle Argus Affiliate enables life sciences companies to remain in global regulatory compliance by supporting affiliate sites and licensing partners. Companies gain greater visibility into pharmacovigilance activities by local affiliates and among partners, lowering risk from unanticipated reporting delays. It also increases overall case-processing efficiency by automating time-consuming tasks and eliminating the need for double data-entry and subsequent reconciliation. Oracle Argus Affiliate enables users from your company's affiliates to manage and track cases specific to their workflow.
Oracle Argus Interchange	Oracle Argus Interchange enables electronic exchange with partners and regulators, supporting maximum efficiency and worldwide regulatory compliance. Oracle Argus Interchange is seamlessly integrated into the Oracle Argus Cloud Service. It allows companies to efficiently process adverse events and collaborate more effectively with global license partners. E2B messaging with Oracle Argus Interchange includes the following features: • Schedule E2B export report • View and check incoming E2B import report • View E2B reports and statuses • Check E2B report DTD • Transmit E2B reports to multiple regulatory agencies or trading partners • View acknowledgments.
Oracle Argus Dossier	Oracle Argus Dossier allows pharmaceutical companies to manage the entire lifecycle of periodic safety update report (PSUR) dossiers in a timely and efficient manner, which helps to ensure compliance and lower the cost of reporting. Oracle Argus Dossier eliminates resource-intensive, manual, periodic reporting processes and shifts the paradigm from data collection to data analysis. Oracle Argus Dossier provides Period Reporting to help you: • Work with predefined report templates created by the administrator • Generate Dossier reports • Author or review Dossier reports.

Component	Description
Oracle B2B	Oracle B2B is an e-commerce gateway that enables the secure and reliable exchange of business documents between an enterprise and its trading partners. Oracle B2B supports: • Business-to-business document standards, security, transports, messaging services, and trading partner management • Health Level 7, which enables healthcare systems to communicate with each other • Numerous industry-standard e-commerce protocols, as defined for a range of industries, including healthcare, retail, IT, telecom, electronics, manufacturing, the food industry, and more.
Oracle Argus Safety Japan (Optional)	Oracle Argus Safety Japan helps to significantly reduce the total cost of ownership for global pharmaceutical companies by eliminating the need for multiple systems, avoiding costly reconciliation issues, and completely integrating Japan into the global business process. It provides essential support for Japanese Pharmaceuticals and Medical Devices Agency (PMDA) expedited reporting in the required Kanji format. A single, global database accommodates both Kanji and Western character sets, greatly increasing the efficiency of adverse event management for the Japanese life sciences industry. Oracle Argus Safety Japan helps you: • Enter Japanese case data • Code using MedDRA J and J Drug dictionaries • Review and report expedited and period reports in Japanese.

Oracle Argus Advanced Cloud Service components

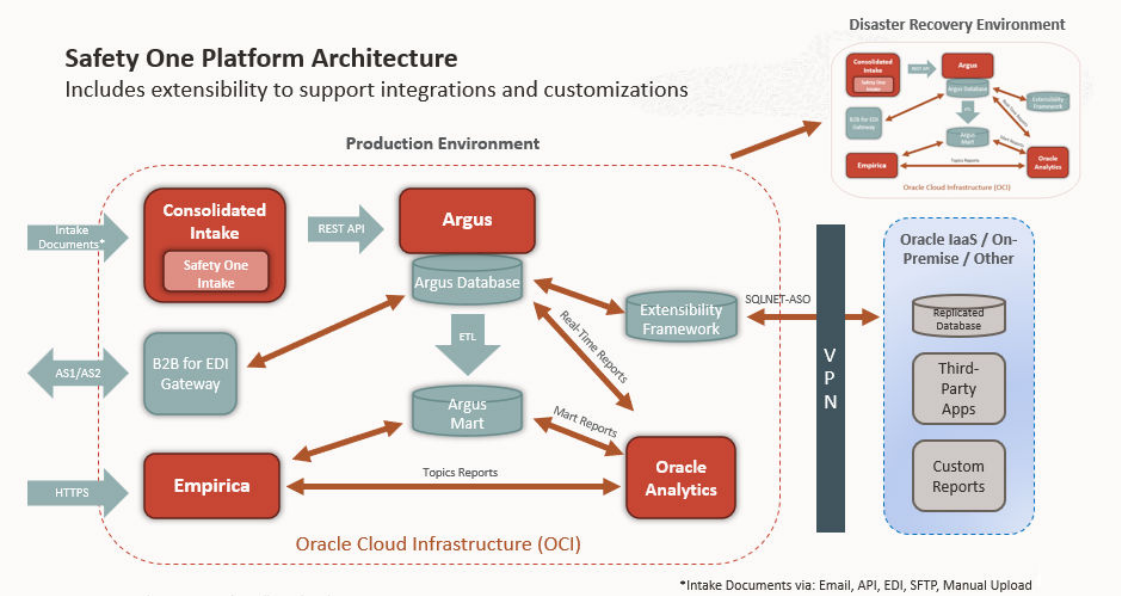
In addition to the base components, you have also access to:

Component	Description
Oracle Argus Insight	Oracle Argus Insight is an analysis tool for safety data. It provides multidimensional and comprehensive analysis of pharmaceutical safety data for making key business decisions quickly and confidently, with a comprehensive knowledge base, an extensive report library, simplified querying and reporting, and easy data access. Oracle Argus Insight includes visibility into strategic safety case and product data across the enterprise. It uncovers key statistically significant data for managing the risk/benefit profiles of products and supports key decision-making by compiling and analyzing safety case data.
Oracle Argus Analytics	Oracle Argus Analytics provides a comprehensive safety operational metrics solution, which includes drill-down dashboards and out-of-the-box integration with Oracle Argus to view key performance indicators at a glance, facilitating a higher degree of compliance and improve cost savings and operational efficiencies. Oracle Argus Analytics: • Provides access to operational data to manage workflow and support regulatory compliance • Views their key performance indicators at a glance • Provides visibility into safety data collection, case processing and submission workflow processes.
Oracle Argus Mart	Oracle Argus Mart integrates Oracle Argus Cloud Service with Oracle Life Sciences Empirica Signal and, as such, it brings the two halves of the Oracle Life Sciences Safety Suite together. It provides a data mart of the adverse event case data from Argus Safety transformed for optimal use by Oracle Empirica Signal for detection and analysis of internal safety signals.

Component	Description
Data Replication (Optional)	The Oracle Argus Data Replication Cloud Service continuously recreates a copy of Oracle Argus Cloud data into the user's target database to support integration with existing third party applications, extensions, and reporting solutions.
Safety One Intake (Optional)	Oracle Safety One Intake is an AI-powered, cloud-native service that automates the ingestion, extraction, and processing of adverse event (AE) source documents for global pharmaceutical companies. It reduces manual data entry into Argus Safety by leveraging AI tools for data extraction. The system supports various formats, including emails, PDFs, and structured data, accelerating safety case processing and compliance.

Oracle Argus Cloud Service architecture

This is a diagram of the Oracle Argus Cloud Service architecture, including the components of the Oracle Argus Advanced Cloud subscription.



Get your administrator account credentials

As primary point of contact for your company, Oracle must provision your account as Customer-Delegated Administrator (CDA) before you can start managing Oracle Argus Cloud Service.

The first administrator account (Customer-Delegated Administrator) is created by Oracle based on the information provided by your company.

After you become an Oracle customer, as primary point of contact for your company, you receive several messages via email:

- A welcome letter
- A system-generated email with the account information

- An email with all the necessary URLs
- An activation letter.

> **Note**
>
> There can be a few days delay between these emails, as required for Oracle to investigate and provision your Argus environments.

There are two scenarios for this process:

Your company is a new Oracle Argus Cloud customer

During onboarding, Oracle emails your company and requests all the information necessary to provision your CDA account. After your company has provided the necessary information, Oracle emails you the account credentials.

Your company is an existing Oracle Argus Cloud customer

Your company must raise a change request with Oracle, as follows:

1. Log in to the Life Sciences Customer Support Portal .
2. Click **Create Request** in the upper right corner, then select **Support Request**.
3. In the **Summary** field, enter a short description of your request.
4. Select appropriate value from the **Severity** drop-down list.
5. In the **Description** field, enter a detailed description of your request, including the following information about the user you want to create:
   - First name
   - Last name
   - User ID
   - User email address
   - Your company's Oracle Identity Self Service URL.
6. If you have a ticket reference number that corresponds to this request, enter it in the **Alternative reference number (if applicable)** field.
7. From the **Oracle Internal** radio buttons, select **No**.
8. From the **Customer** drop-down list, search for your company's name and select it from the list.
9. From the **Product** drop-down list, select **Argus Safety**.
10. From the **Business Service** drop-down list, select the name of the server where you want this change.
11. From the **Issue Category** drop-down list, expand **Change - Cloud Environment**, then **Application**, **User**, and select **Add**.
12. From the **Environment** drop-down list, select the environment where you want this change, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.

    If you select **Other** or **Not Sure**, enter the URL of the application in the **Application URL/ Website Address** field.

13. You can attach files relevant to the request in the **Attachments** section.
14. In the **Additional Watchers** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. Click **Submit**.

What you do as an administrator

As administrator, you have specific tasks and permissions in Oracle Argus Cloud Service.

As an administrator, you can create other administrator and user accounts for your company, and grant them permissions to Argus according to their role.

These are the tasks an administrator can perform in Oracle Argus Cloud Service:

- Create users in IDCS (requires Customer-Delegated Administrator credentials)
- Configure user sites
- Configure groups
- Create new enterprises in Oracle Argus Mart
- Manage the Extract, Transform and Load (ETL) Data
- Manage data replication
- Grant users with Oracle Argus Analytics access
- Grant users with Consolidated Intake access
- Email Intake configurations
- API Intake configurations
- Obtain a Product Verification Pack (PVP)
- Load and manage dictionaries
- Manage and use the built-in utilities
- Configure the Federated identity Single-Sign On (SSO)
- Manage sFTP user access
- Configure SMTP
- Request gateway UI access
- Grant users with Axway UI access
- Grant users with Oracle B2B UI access
- Request creating a trading partner or community from the Life Sciences Customer Support Portal
- Configure Axway B2Bi to transmit reports

Sign in for the first time

Sign in to set up your account and define your own password.

When you sign in for the first time, you can set up your own password:

1. Click the **Oracle Life Sciences Cloud account** link in the Account Password email you received.

2. Sign in using the user login from the New Account email and the password from the Account Password email.
3. Enter the old password you received in the Account Password email.
4. Enter the new password and confirm the new password.
5. Choose three of the available challenge questions from the drop-down, and enter answers for them.
6. Click **Submit**.
   Your password is changed, and the Sign In page opens.
7. Sign in using your new password.

If you don't have this information, then click **Need help logging in** and enter the email address associated with your cloud account. Oracle will send you an email with a summary of your account information.

Environments you can access

Oracle provides your company with one production environment and one non-production environment.

Your Oracle Argus Cloud Service subscription provides access to two types of environments:

- **Non-Production Environment**
  The non-production environment may be either a test (VAL) or a development (DEV) environment provided to you as part of the Cloud Services. The non-production environment is specifically sized and designed for development and training purposes and may not be used for production purposes or for performance or stress testing. Any service levels, performance targets, and disaster recovery described for the applicable Oracle Cloud Service are not applicable to non-production environments.
- **Production Environment**
  The production environment is designed for daily commercial use and production operations of live data. Unless otherwise specified, a single production environment is provided for an Oracle Cloud Service.

Only one non-production gateway will be set up for ICSR exchange with other non-production gateway. There cannot be two non-production gateways transmitting from Oracle Cloud to an agency or partner non-production gateway, even when there are multiple installations of non-production gateways in Oracle Cloud (for example, in DEV and VAL). For example, you can perform connectivity testing in DEV and then switch to VAL during formal testing phase.

2

Manage sites, groups, and users

You configure and manage sites, groups, and users from the Access Management section of the Oracle Argus Cloud Service administration console.

Each user must be assigned to at least one group in order to determine their security level. Each group is assigned a specific security level. This security level enables members of the group to view, modify, or restrict access rights to various sections of the Case Form, and so on.

The first set of steps in configuring Oracle Argus Cloud Service is to create the following exactly in the listed order:

- Sites
- Groups
- Users

For more information, see:

- Manage sites
  A user site refers to a Marketing Authorization Holder (MAH) or a Local affiliate that processes Adverse Events or local AEs.
- Manage groups
  You can add each user of Oracle Argus Cloud Service to one or more groups.
- Manage users
  You need first to provision the user in Oracle Identity Cloud Service (IDCS), then you can add the user to Oracle Argus Cloud.
- Filtering sites, groups and users
  You can use the available filtering criteria for sites, groups and users to search for specific items.

Manage sites

A user site refers to a Marketing Authorization Holder (MAH) or a Local affiliate that processes Adverse Events or local AEs.

You need to add sites before creating users, as every user must be assigned to exactly one site. The site information can also be used in the automatic numbering of case IDs.

To configure sites, use the **Sites** section.

For more information, see:

- Add user sites
- User sites fields descriptions
- Site configuration printout

Add user sites

To add a user site:

1. Navigate to **Access Management**, then **Argus**, and then **Sites**.
2. In the left pane, select **User Sites**. The user sites are listed in the right panel.
3. Click **Add New**.

> **Tip**
>
> You can alternatively click:
>
> - **Modify** to change an existing user site.
> - **Copy** to make an editable copy of an existing user site.
> - **Delete** to delete a user site.

4. In the **Add New User Site** section, enter the user site description.
5. Enter the user site abbreviation.

   A maximum four-character abbreviation is required for each user site.
6. Select a site type.

   Each Oracle Argus Cloud Service user must be assigned to exactly one user site.

   You cannot change the site type from LAM to Central if the current central site has an association with a LAM site, if the current site is associated with any user, or if the current LAM site has any events assigned to it.
7. Select the following options as required:
   - **Protect Patient Confidentiality - Default** to protect or reveal *Patient Confidentiality* for this specific user site.
   - **Protect Reporter Confidentiality - Default** to protect or reveal *Reporter Confidentiality* for this specific user site.
   - **Bulk Report by Form (Approved Reports) - Default** to enable availability of the *Bulk Reports By Form* for this specific site.
8. Add or remove any LAM Sites information.

> **Tip**
>
> To add more LAM Sites to the LAM Sites list, use the **Add/Add All** options.
>
> To delete the LAM Sites from the Lam Sites list, use the **Remove/Remove All** options.

9. In the Site Printers section, click **Add** to add a site printer.
   a. Enter the Name of the printer that will be displayed in the application when referring to the printer.

      The name can have up to 20 characters.
   b. In the **Path text** field, enter the full path of the printer on the network.

      This path name can have up to 256 characters. The specified path should be accessible from the system where Argus Safety Service is installed.

> **Tip**
>
> To delete a site printer, select the printer and click **Delete**.
>
> To print the site information, click **Print**.

10. Save the new site.

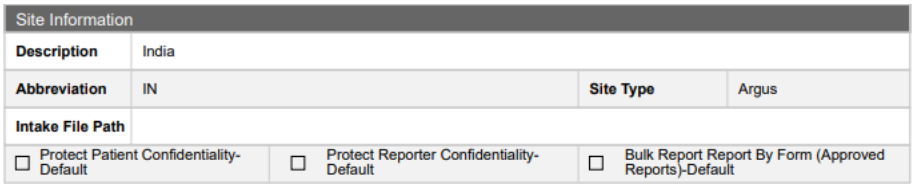
User sites fields descriptions

The following table describes the fields in the Sites section:

Field or Control Name	Description
Description	Enter a description of the site.
Abbreviation	Enter an abbreviation of the site name. A one to four character abbreviation is required for each site.
Site Type	Select the site type —Argus or LAM (Local Affiliate Module).
Intake File Path	The folder location for the XML files ingested from the given user site.
Protect Patient Confidentiality - Default	Protects or reveals the Patient Confidentiality for the specific site.
Protect Reporter Confidentiality - Default	Protects or reveals the Reporter Confidentiality for the specific site.
Bulk Report By Form (Approved Reports) - Default	Allows or protects availability of the Bulk reports by Form for the specific site.
LAM Sites	Select and add previously created LAM sites.
Site Printers	The Site Printers section is used to configure site printers.

Site configuration printout

The site configuration printout lists the user site information.



Manage groups

You can add each user of Oracle Argus Cloud Service to one or more groups.

You can configure the access rights of each user group to the menus in the user interface and the specific Case Form sections.

You configure groups using the **Groups** section.

For more information, see:

- Groups included with the Oracle Argus Cloud Service
  You can find here the description of groups included with the Oracle Argus Cloud Service by default.
- About user groups
  You can create an Argus and/or local affiliate group. An Argus group is applicable for Argus central users. A local affiliate group is available only for local affiliate users.
- Add Argus user groups
  You can add user groups and configure the security levels for each group.
- Add local affiliate user groups
  You can add affiliate user groups and configure the security levels for each group.
- User groups fields description
  The **Modify Group Information** section contains several fields described in the table below.
- Users belonging to multiple groups
  If a user belongs to multiple groups, the access rights for the user will be a combination of the highest access level permissions for each individual group.
- Print a group configuration list
  Print groups are user-defined values used to sort groups and users. Print groups control sorting on various types including case form, menus, listedness determination, advanced condition permissions, restrictions-products, restriction–studies and users. The printout displays all group permissions defined by the administrator.
- Group configuration printout
  In the **Argus Console - Print** window, select the information you want to print.

Groups included with the Oracle Argus Cloud Service

You can find here the description of groups included with the Oracle Argus Cloud Service by default.

Group	Description
Administrator	This group has access rights to the functionality and all areas of Oracle Argus Cloud Service.
Investigator	Receives an e-mail alert that can be set up during Clinical Study Configuration.

About user groups

You can create an Argus and/or local affiliate group. An Argus group is applicable for Argus central users. A local affiliate group is available only for local affiliate users.

The affiliate users are users that belong to other global sites of the company or its local affiliates. Affiliate sites may fall under different regulatory reporting requirements compared to the Central Safety site and other affiliate sites.

Add Argus user groups

You can add user groups and configure the security levels for each group.

To create an Argus user group:

1. Navigate to **Access Management**, then **Argus**, and then **Groups**.

2. Select the Argus folder and click **Add Group** to create a new group.

> **Tip**
>
> You can alternatively click:
>
> - **Copy** to make an editable copy of an existing group.
> - **Delete** to delete a group.

3. Enter the **Group Name**.

   The group name should be a unique name.

4. If applicable, enter the **Email** address.
5. If applicable, enter the **Supervisor Email** address.
6. In the **Case Form** section, select the desired access right option (**Modify**, **View**, or **No Access**) for the group's access to each of the listed items.

> **Note**
>
> To save a case, the following fields must be populated:
>
> - **Initial Receipt Date**
> - **Country of Incidence**
> - **Report Type**
> - **Suspect Product**
> - **Event Description as Reported**.
>
> Therefore, the group responsible for initial case entry must have access to these fields to save new cases.

7. In the **Menus** section, enable or disable the group's access to particular items in the Argus Cloud Service menu.

   Refer to the *Oracle Argus Safety User's Guide* for information about the functions of the Case Form sections and the menu items in the Oracle Argus Safety user interface.

8. In the **Listedness Determination** section, select a list of countries.

   This enables the end user to override the listedness determination in the **Event Assessment** section of the Case Form for product licenses that match the countries selected in this step.

9. In the **Advanced Conditions** section, select the access rights for the new group:
   - **No Access to Create Advanced Condition** - **Advanced Conditions** does not appear as an option for that user group.
   - **No Access to Share Advanced Conditions** - the user group does not have access to share advanced conditions.
   - **No Access to View and Edit SQL** - the **SQL...** button does not appear as an option for that user group.

> **Note**
>
> Only trusted users should be given access to advanced conditions, because users who have this right have complete access to the information in the Oracle Argus Safety Schema.

10. In the **Restrictions** section, check **Products** and click **Select**.
11. In the Available Products dialog box, select each product you want to add and click **OK**.
12. In the **Restrictions** section, check **Study** and click **Select**.
13. In the Available Studies dialog box, select the required studies and click **OK**.
14. Click **Save** to save the group.

> **Note**
>
> If you haven't selected any products or studies, the group will have access to all products or studies.

Add local affiliate user groups

You can add affiliate user groups and configure the security levels for each group.

Use the following procedure to create a local affiliate user group:

1. Navigate to **Access Management**, then **Argus**, and then **Groups**.
2. Select the Local Affiliate folder and click **Add Group** to create a new group.
3. Enter the **Group Name**.
4. If applicable, enter the **Email** address.
5. If applicable, enter the **Supervisor Email** address.
6. Select the **Default Report**.
7. In the **Menus** section, enable or disable the group's access to particular items in the Argus Cloud Service menu.
8. In the **Listedness Determination** section, select a list of countries.

   This enables the end user to override the listedness determination in the **Event Assessment** section of the Case Form for product licenses that match the countries selected in this step.
9. In the **Restrictions** section, check **Products** and click **Select**.
10. In the Available Products dialog box, select each product you want to add and click **OK**.
11. In the **Restrictions** section, check **Study** and click **Select**.
12. In the Available Studies dialog box, select the required studies and click **OK**.
13. Click **Save** to save the group.

> **Note**
>
> If you haven't selected any products or studies, the group will have access to all products or studies.

User groups fields description

The **Modify Group Information** section contains several fields described in the table below.

Field or Control Name	Description
Group Name	Enter a unique name for the group.
Email	Add the group email, used for case priority notifications and workflow routing notifications.
Supervisor Email	Add the group supervisor's email, as applicable. This email address is used to send notifications when the maximum time of a case for a particular workflow state is exceeded.
Menus	Lists the menus and submenus within a Case Form and allows you to enable or disable each of them.
Case Form	Lists the sections and subsections within a Case Form and enables you to assign the group the following rights: • Modify • View (Read Only) • No Access (not visible).
Advanced Condition	Allows you to configure advanced condition settings, as applicable. The options are: • No Access to Create Advanced Conditions: the Advance Condition does not appear as an option for any user belonging to the group. • No Access to Share Advanced Conditions: any user belonging to the group cannot share the Advance Conditions with others. • No Access to View and Edit SQL: the SQL option will not appear for the user belonging to the group.
Listedness Determination - Countries	Select the list of countries for which the users can change the listedness determination for the product licenses originating in the selected countries.
Restrictions - Products	Limits the number of products that can be viewed in the trade name lookup and non-study cases.
Restrictions - Studies	Limits the number of studies available for selection and the study cases that can be viewed.
Default report (LAM only)	Lists the expedited report forms in the drop-down list.

Users belonging to multiple groups

If a user belongs to multiple groups, the access rights for the user will be a combination of the highest access level permissions for each individual group.

For example, let's think about a user in Oracle Cloud Argus Service. John Smith is an Oracle Cloud Argus Service user and his profile has been added to two user groups with different access level permissions for each group. John has access rights to the Patient tab in one

group and access rights to the General tab in another group. In this case, John can access both the Patient and the General tabs of Oracle Cloud Argus Service.

Print a group configuration list

Print groups are user-defined values used to sort groups and users. Print groups control sorting on various types including case form, menus, listedness determination, advanced condition permissions, restrictions-products, restriction–studies and users. The printout displays all group permissions defined by the administrator.

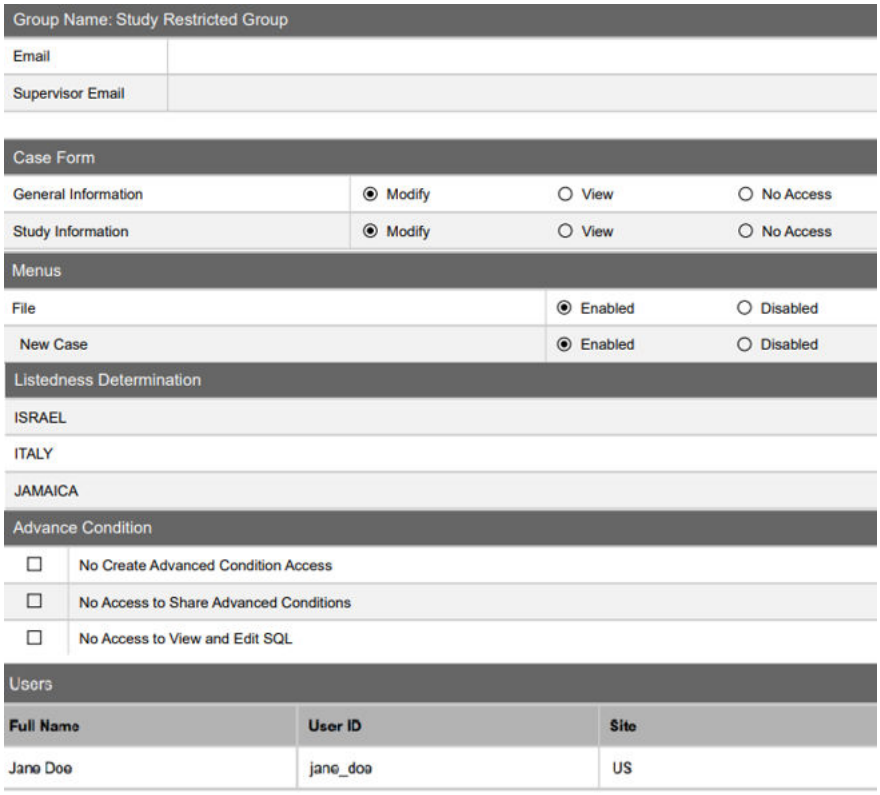
1. Click **Access Management**, then **Argus**, and then **Groups**.
2. Select a **Group** and click to view the group details in the right panel.
3. To display the **Print** dialog that enables you to print either the entire window or only the text covered by the current selection, click **Print**.
4. Select the appropriate option and click **OK**.
5. In the Print Groups window, select the sections to be printed in the Group Configuration printout.

   By default, the **Group Information** check box is selected and disabled so that this information always gets printed.
6. Select the appropriate check boxes and click **OK**.

Group configuration printout

In the **Argus Console - Print** window, select the information you want to print.

When all options are selected, the Group Configuration Report printout lists the group information, such as: name, email, the access options to the Case Form, the access options to the Menu, the listedness determination, the advanced condition permissions, the restrictions-products, the restriction–studies and the users. All options are sorted alphabetically in the report section.



Group Name: Study Restricted Group			
Email			
Supervisor Email			
Case Form			
General Information	◉ Modify	○ View	○ No Access
Study Information	◉ Modify	○ View	○ No Access
Menus			
File	◉ Enabled	○ Disabled	
New Case	◉ Enabled	○ Disabled	
Listedness Determination			
ISRAEL			
ITALY			
JAMAICA			
Advance Condition			
☐	No Create Advanced Condition Access		
☐	No Access to Share Advanced Conditions		
☐	No Access to View and Edit SQL		
Users			
Full Name	**User ID**	**Site**	
Jane Doe	jane_doe	US	

Manage users

You need first to provision the user in Oracle Identity Cloud Service (IDCS), then you can add the user to Oracle Argus Cloud.

- Manage users with Oracle Identity Cloud Service (IDCS)
- User migration in Oracle Identity Cloud Service (IDCS)
- Add users to Oracle Argus Cloud Service
  Once you have provisioned an user in Oracle Identity Cloud Service (IDCS), you can add the user to Oracle Argus Cloud Service.

Manage users with Oracle Identity Cloud Service (IDCS)

For more information, see:

- Create users in IDCS
  As a customer-delegated administrator, setting up access for your users involves two steps. First, create the user in Oracle Identity Cloud Service (IDCS). Second, add the user to the Oracle Argus Cloud Service.
- Create groups in IDCS
  Groups must be associated to the users for them to work in the application.
- Assign groups to user accounts in IDCS
  Users can't start working until they have been assigned one or more groups.
- Deactivate users in Argus Cloud Service
  Deactivating or disabling users in the Argus Cloud Service involves two steps. First,deactivate the user in IDCS. Second, disable the user in Oracle Argus Safety.

- Reset a user password
  You can reset a user password either in IDCS or by the CDA user.
- Print a user configuration list
  The user printout displays the users permissions defined by the administrator, such as user name, ID, email address, application access, user roles, user type, user group, sites and Case Form permissions.

Create users in IDCS

As a customer-delegated administrator, setting up access for your users involves two steps. First, create the user in Oracle Identity Cloud Service (IDCS). Second, add the user to the Oracle Argus Cloud Service.

You can create user accounts, only if, you have access to the identity domain administrator or user administrator role in the **Administrators** page of the Identity Cloud Service Console.

To create users in IDCS:

1. Log in to IDCS Argus Console using your Oracle Argus Cloud Service administrator credentials.
   Alternatively, if you are using OCI Identity Domain, then navigate to **Identity** > **Domains**, and go to the required domain.
2. Click **Users**, then **Create Users**.
3. Enter the user attributes listed below (the values in the table are provided only as examples) to create the user.

Item	Sample Value
First name	John
Last name	Doe
User name/Email	John Doe or john.doe@abc.xyz The value entered here can be either a valid e-mail address or a non-email string.
Use the email address as the user name	Check this check box if the user name and email address are same. Uncheck this check box, if the user name and email address are different.

4. When you are done entering the user information, click **Finish**.

For more information, refer to the Oracle Cloud Administering Oracle Identity Cloud Service Guide > Create User Accounts section.

Create groups in IDCS

Groups must be associated to the users for them to work in the application.

As part of the Argus installation, the following out-of-the-box IDCS group names are created. Each product: Oracle Argus Safety, Oracle Analytics Server, Oracle Safety One Intake gateway, and Axway gateway have their own groups.

IDCS group names

Group Display Name	Description
ls-oasafety-*env*-as-group	Argus Safety Group
ls-oasafety-*env*-bi-FAR_Admin_group	FAR Administrator Group

Group Display Name	Description
ls-oasafety-*env*-bi-FAR_SafetyAuthor_group	FAR Safety Author Group
ls-oasafety-*env*-bi-FAR_SafetyConsumer_group	FAR Safety Consumers Group
ls-oasafety-*env*-bi-AI_Admin_group	AI Administrator Group
ls-oasafety-*env*-bi-AI_Author_group	AI Author Group
ls-oasafety-*env*-bi-AI_Consumer_group	AI Consumers Group
ls-oasafety-*env*-bi-PVA_Admin_group	PVA Administrator Group
ls-oasafety-*env*-bi-PVA_Safety_group	PVA Safety Author Group
ls-oasafety-*env*-bi-PVA_SafetyConsumer_group	PVA Safety Consumers Group
ls-oasafety-*env*-bi-EXP_Admin_group	EXP Administrator Group
ls-oasafety-*env*-bi-EXP_SafetyAuthor_group	EXP Safety Author Group
ls-oasafety-*env*-bi-EXP_SafetyConsumer_group	EXP Safety Consumers Group
ls-oasafety-*env*-bi-DV_Admin_group	DV Administrator Group
ls-oasafety-*env*-bi-DV_Author_group	DV Author Group
ls-oasafety-*env*-bi-DV_Consumer_group	DV Consumers Group
ls-oasafety-*env*-b2bi-configure-group	AxwayB2BI Admin Role
ls-oasafety-*env*-b2bi-monitor-group	AxwayB2Bi View Reports Role
ls-oasafety-*env*-soa-configure-group	SOA B2B Configure Role
ls-oasafety-*env*-soa-monitor-group	SOA B2B Monitor Role

Note

- The CDA users (with IDCS admin privileges) can see all the groups in IDCS related to all the environments DEV/VAL/PROD.
- *env* in the above table represents the environment code, like dev, val, or prod. For example:
  - If the environment is development, then ls-oasafety-**dev**-bi-DV_Admin_group
  - If the environment is development1, then ls-oasafety-**dev1**-bi-DV_Admin_group
  - If the environment is validation, then ls-oasafety-**val**-bi-PVA_SafetyConsumer_group or
  - If the environment is prodution, then ls-oasafety-**prod**-bi-PVA_Safety_group

Sample groups in the development environment

Group Display Name	Description
ls-oasafety-dev-as-group	Argus Safety Group
ls-oasafety-dev-bi-FAR_Admin_group	FAR Administrator Group
ls-oasafety-dev-bi-FAR_SafetyAuthor_group	FAR Safety Author Group
ls-oasafety-dev-bi-FAR_SafetyConsumer_group	FAR Safety Consumers Group
ls-oasafety-dev-bi-AI_Admin_group	AI Administrator Group
ls-oasafety-dev-bi-AI_Author_group	AI Author Group
ls-oasafety-dev-bi-AI_Consumer_group	AI Consumers Group
ls-oasafety-dev-bi-PVA_Admin_group	PVA Administrator Group
ls-oasafety-dev-bi-PVA_Safety_group	PVA Safety Author Group

Group Display Name	Description
ls-oasafety-dev-bi-PVA_SafetyConsumer_group	PVA Safety Consumers Group
ls-oasafety-dev-bi-EXP_Admin_group	EXP Administrator Group
ls-oasafety-dev-bi-EXP_SafetyAuthor_group	EXP Safety Author Group
ls-oasafety-dev-bi-EXP_SafetyConsumer_group	EXP Safety Consumers Group
ls-oasafety-dev-bi-DV_Admin_group	DV Administrator Group
ls-oasafety-dev-bi-DV_Author_group	DV Author Group
ls-oasafety-dev-bi-DV_Consumer_group	DV Consumers Group
ls-oasafety-dev-b2bi-configure-group	AxwayB2BI Admin Role
ls-oasafety-dev-b2bi-monitor-group	AxwayB2Bi View Reports Role
ls-oasafety-dev-soa-configure-group	SOA B2B Configure Role
ls-oasafety-dev-soa-monitor-group	SOA B2B Monitor Role

Assign groups to user accounts in IDCS

Users can't start working until they have been assigned one or more groups.

1. In the Identity Cloud Service Console, under Identity Domain, click **User**.
2. Search for the user you want to assign the group, and click the user's name.
3. On the User page, scroll down to Groups, and click **Assign user to groups**.
4. Select groups you want to assign to the user, and click **Assign User**.

For more information, refer to the Oracle Cloud Administering Oracle Identity Cloud Service Guide > Assign Groups to the User Account section.
Example 1: To assign user with access to only Oracle Argus application in the development environment, select the group as `ls-oasafety-dev-as-group`.

Example 2: To assign the user with access to the Oracle Argus application and OAS Admin User in the development environment, select the following groups:

- `ls-oasafety-dev-as-group`
- `ls-oasafety-dev-bi-FAR_Admin_group`
- `ls-oasafety-dev-bi-AI_Admin_group`
- `ls-oasafety-dev-bi-PVA_Admin_group`
- `ls-oasafety-dev-bi-EXP_Admin_group`
- `ls-oasafety-dev-bi-DV_Admin_group`

Example 3: To assign the user with access to the gateway in the developmet environment:

- For Axway B2Bi, select the group as `ls-oasafety-dev-b2bi-configure-group`.
- For Oracle Safety One Argus, select the group as `ls-oasafety-dev-soa-monitor-group`.

Deactivate users in Argus Cloud Service

Deactivating or disabling users in the Argus Cloud Service involves two steps. First,deactivate the user in IDCS. Second, disable the user in Oracle Argus Safety.

Deactivate a user in IDCS

1. In the Identity Cloud Service Console, under Identity Domain, check the check box of the user you want to deactivate.
2. Click **More Actions** > **Deactivate**.
3. In the next page, click **Deactivate**.

> **Note**
>
> - Before deactivating or deleting a user, we recommend you to remove the access to any groups or applications for that user.
> - Deactivating a user account temporarily disables the access rights that the user account has to IDCS.
> - Deactivated users will not be able to log in until you reactivate the user account. Group memberships and application roles remain intact and are available once the user account is reactivated.

Disable a user in Oracle Argus Cloud Service

This is the procedure for temporary disabling the user in Oracle Argus Cloud Service.

Before you can disable a user in Oracle Argus Cloud Service, you must disable the user in Oracle Identity Self Service.

To temporarily disable a user in Oracle Argus Cloud Service:

1. Open a browser and navigate to your company's Oracle Argus Cloud Service URL. Log in with your Oracle Argus Cloud Service administrator credentials.
2. Navigate to **Access Management** , then **Argus**, and then **Users**.
3. In the left pane, select the user you want to temporarily disable.
4. In the Access section, select the **Account Disabled** option and save the changes.

Reset a user password

You can reset a user password either in IDCS or by the CDA user.

To reset a user password in IDCS

You can yourself reset the password on self-service basis.

1. In the Login page, click **Forgot password**.
2. In the **What's your user name?** field, enter the user name, and click **Next**.
   A message appears as `"Password Reset Notification Sent" to your email`.

   A notification email is sent to the user with a link by which the user can reset their password.

3. Click the **Password Reset** link in email. The link redirects to the Password Reset page.
4. In the Password Reset page, enter new password to reset the password.

To reset a user password with the help from the CDA user

1. Log in to the Identity Cloud Service Console as the CDA user.
2. Under Identity Domain, check the check box of the user for whom you want to reset the password.
3. Click **More actions** > **Reset Password**.
4. In the next page, click **Reset Password**.
   A notification email is sent to the user with a link by which the user can reset their password.
5. As the end-user, click the **Password Reset** link in email. The link redirects to the Password Reset page.
6. In the Password Reset page, the end-user enters new password to reset the password.

Print a user configuration list

The user printout displays the users permissions defined by the administrator, such as user name, ID, email address, application access, user roles, user type, user group, sites and Case Form permissions.

1. Click **Access Management**, then **Argus**, and then **Groups**.
2. Select a user and click to view the user's details in the right panel.
3. To display the Print dialog box that enables you to print either the entire window or only the text covered by the current selection, click **Print**.
4. Select the appropriate option and click **OK**.
5. In the Print Users window, select the sections to be printed in the User Configuration printout.

> **Note**
>
> By default, the **User Information** check box is selected and disabled so that this information always gets printed.

6. Select the appropriate check boxes and click **OK**.

User migration in Oracle Identity Cloud Service (IDCS)

Oracle Identity Cloud Service (IDCS) is Oracle's next generation platform for security and identity management. The platform is cloud-native and designed to be an integral part of the enterprise security fabric by providing modern identity for modern applications. Oracle Identity Cloud Service (IDCS) is an Identity-as-a-Service solution.

Oracle Life Sciences Argus Cloud Service uses IDCS for Identity and Access management.

User access management is one of the key essential activities for any identity management systems. As part of Argus Cloud Service, user management is done by using IDCS to create Users and to assign users to Groups to provide the required access to the Oracle Life Sciences Argus Cloud applications such as Argus Safety, Argus Insight, Argus Analytics OAS, SOA and Axway.

Manage users in bulk

Bulk user management is possible in one of the following scenarios:

- Initial Customer Onboarding - in the case of a fresh uptake of Argus Cloud
- Migration or upgrade from oracle IDM to IDCS - available for existing cloud users

For more information, see:

- User onboarding
- About the IDCS report for importing users and groups
- User group migration from IDM to IDCS
- Export user group information from IDM
- Import user group information to IDCS
- Validation, comparison reports and how to take corrective action
- User and group import status report
- General admin activities
- Case studies for user migration

User onboarding

The following user types are provisioned during the initial onboarding stage:

- **Oracle Application Management Users (AMS Users)**: the Oracle AMS team can access the Argus application for URL validation purpose. An AMS User does not have access to make any changes in the Argus applications.
- **Customer Users**: This user type is for the application end users that need to access applications.
- **Oracle Consulting and Support Users**: These users are created by customers on a need-only basis and only if consulting is required for migration or any other activity. Customers can provide a list of the required Oracle Consulting users to AMS. AMS then creates these users with the help of the User Commissioning utility.

This chapter covers the first two user types.

For more information, see:

- AMS user on-boarding
- User onboarding with help from AMS
- Onboarding self-service

AMS user on-boarding

After the initial Argus Safety Suite setup is completed in any customer environment, the AMS team logs in to each application and performs a sanity check. Once the validation and sanity check are completed, an environment is released.

The following activities are performed as part of the AMS on-boarding process:

- **Setup SSO Federation between Customer IDCS and Oracle IAMS**: AMS users are authenticated via Oracle IAMS (Corporate OIM). To accomplish this, the federation is setup

between customer IDCS and Oracle IAMS, as part of the Argus Cloud Service provisioning.

- **Create a user in IDCS**: Oracle Users in IDCS are created as federated users. Thus, the users can not authenticate via IDCS.
- **Create a user in Argus Safety**: AMS Users have restricted access in the Argus application. AMS users only have login access and do not have access to case data.

User onboarding with help from AMS

Initial Argus Cloud Service onboarding requires you to create and/or to migrate users to IDCS. To do so, you can use the out-of-the-box option to import users to IDCS.

You can also perform bulk import with help from Oracle AMS team. The AMS team uses proprietary automation when bulk importing users.

> **Note**
>
> If you have a requirement to authenticate by using a Custom Identity Solution (OKTA or Azure for example), it is recommended that you set up Federation before migrating users to IDCS.

For bulk user migration:

1. You prepare the CSV files for Users and Groups.
2. Create an Life Sciences CX ticket for the AMS team in which you request the users and group import. Make sure you attached the CSV files to the ticket.
3. The Oracle AMS team generates a pre-validation report by using the CSV files and then shares the report with you.
4. You review the report and either:
   a. Confirm that the information is correct.
   b. Correct any discrepancies in the CSV file and then send the updated file to the Oracle AMS team.
5. After your confirmation, the AMS team imports the users and groups information to IDCS.
6. The AMS team generates a post-import validation report and then shares it with you.
7. In case of any changes, see step 4.

For more information on the bulk import process, see the Use Best Practices for Bulk Loading Data section of the *IDCS Administering Oracle Identity Cloud Service* guide.

For more information on the CSV file preparation, see:

- How to prepare for CSV import
- Guidelines for preparing users CSV
- User CSV examples
- Guidelines for preparing CSV files for IDCS groups
- Pre-validation and comparison report

How to prepare for CSV import

In this chapter, you can find guidelines for your users to prepare the users.csv and groups.csv files. These files are sent to AMS for bulk import.

The user is advised to follow the below guidelines while preparing the CSV files to avoid error messages during the import process.

Users, CSV and CSV groups are provided to AMS for bulk import.

General Guidelines

- The users need to prepare two CSV files:
  - Users.csv: This file contains user information, formatted in the standard of IDC sample user CSV file.
  - Groups.csv: This file contains groups and user-group associations, formatted in the standard of IDCS sample group CSV file.
- CSV files need to be in the UTF-8 format.
- the CSV file name should not include special characters such as commas or spaces.
- To create a CSV file, you can use a standard spreadsheet application such as Microsoft Excel or Google Sheets, or you can use a text editor, such as Notepad or TextPad.

For more information, see:

Guidelines for preparing users CSV

The user CSV file needs to be set up as per the IDCS standards. For more information, see the Import User Accounts section of the *Administering Oracle Identity Cloud Service* guide and the IDCS: Bulk Loading Users and Groups using CSV files page.

The user CSV file is a simple text file in a tabular format (containing rows and columns). The first row in the file defines the fields in the table.

For each account, you can create a new row and enter data into each column. Each row represents one record.

The table below details the minimum attributes that you need to provide for users in the CSV file:

Column heading in the CSV file	Value
User ID	The value entered in the User Name field can be either a valid e-mail address or a non-email string. In case of a non-email string, the following characters are supported: • a-z • A-Z • 0-9 • Special characters, such as !@#$%^&*()_+=-{}[]|\:'";<>?/
Last Name	The user's last name
First Name	The user's first name
Work Email	User's valid email address, such as john.smith@custom.com

Column heading in the CSV file	Value
Primary Email Type	Lists your user's email type. It can be set to either **Work**, **Home** or **Other**.
User Type	Your user's type. The valid values are: • Contractor • Employee • External • Generic • Intern • Service • Temporary
Active	This field determines if the user is Active of Disabled. The valid values are **True** or **False**. **Note** For Inactive users, set the Bypass Notification field to True so that the user does not receive any notification when the it is imported to IDCS.
Bypass Notification	This field determines if the user receives notifications via email when a user is created or modified. The valid values are **True** and **False**. If you do not want your users to be notified when Oracle IDCS creates an account for them, then you must set the Bypass Notification field to **True**.

Column heading in the CSV file	Value
Federated	The valid values are True or False. If you want your users to use their federated accounts to sign in to IDCS, then the Federated field must be set to True. When this field is set, Oracle IDCS no longer manages the federated user's password. This prevents Oracle IDCS from enforcing a password change for those imported user accounts. This field must be set to True is the intended user authenticates via a federated SSO and not via IDCS. This field must be set to False if the indented user authenticates via IDCS. If this field is left blank, the user is created as a non-federated user who can authenticate via IDCS. **Note** Set the Bypass Notification field to True for federated users, so that they do not receive email notifications from IDCS.

You must ensure that the value from the above fields are not null.

In addition, ensure that the User ID is unique. If the ID is not unique, the following scenarios may occur:

- If there are two entries with the same User ID and with the same attributes in the CSV file, then the first User ID will be created and the second User ID creation fails.
- If there are two entries with the same User ID, but there are different attributes in the CSV file, then the first User ID is created and the second record will update with the details of the first user.

The users can extend the CSV file columns based on the IDCS supported attributes listed in the Use Best Practices for Bulk Loading Data section of the *Administering Oracle Identity Cloud Service* guide.

For more information, see:

User CSV examples

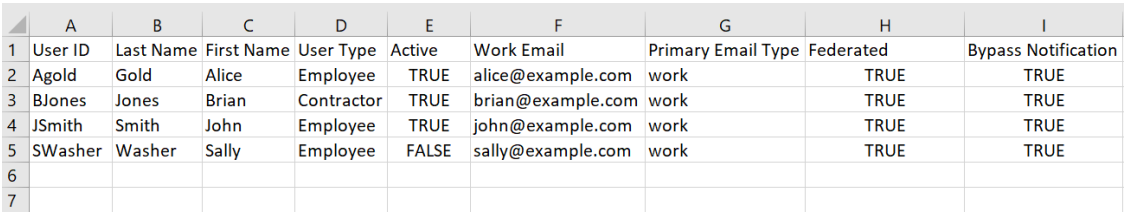
Figure 2-1 User CSV example 1

	A	B	C	D	E	F	G	H	I
1	User ID	Last Name	First Name	User Type	Active	Work Email	Primary Email Type	Federated	Bypass Notification
2	Agold	Gold	Alice	Employee	TRUE	alice@example.com	work	FALSE	FALSE
3	BJones	Jones	Brian	Contractor	FALSE	brian@example.com	work	FALSE	TRUE
4	JSmith	Smith	John	Employee	TRUE	john@example.com	work	FALSE	FALSE
5	SWasher	Washer	Sally	Employee	TRUE	sally@example.com	work	FALSE	FALSE
6									
7									

In the above CSV file example, the second user has the Active field set to **False** and the Bypass Notification is set to **True**. Thus, when the user is imported, the user does not receive an email notification.

In addition, the Federated field is set to **False**, which means that no federation is applied in this situation.

Figure 2-2 User CSV example 2



	A	B	C	D	E	F	G	H	I
1	User ID	Last Name	First Name	User Type	Active	Work Email	Primary Email Type	Federated	Bypass Notification
2	Agold	Gold	Alice	Employee	TRUE	alice@example.com	work	TRUE	TRUE
3	BJones	Jones	Brian	Contractor	TRUE	brian@example.com	work	TRUE	TRUE
4	JSmith	Smith	John	Employee	TRUE	john@example.com	work	TRUE	TRUE
5	SWasher	Washer	Sally	Employee	FALSE	sally@example.com	work	TRUE	TRUE
6									
7									

In the above CSV file example, the Federation field is set to **True** for all users and so the Bypass Notification field is set to **True** as well, irrespective if the users are active or not.

Guidelines for preparing CSV files for IDCS groups

The CSV files for groups need to be set up as per the IDCS standards. For more information, see the Import User Accounts section of the *Administering Oracle Identity Cloud Service* guide and the IDCS: Bulk Loading Users and Groups using CSV files page.

The group CSV file is a simple text file in a tabular format (containing rows and columns). The first row in the file defines the fields in the table.

The table below details the minimum attributes that you need to provide for users in the CSV file.

CSV file column headings	Value
Display Name	The group name
Description	The description of your group name
User Members	The list of users associated with the group, separated by a semi-colon. Example: BJones;JSmith

Ensure that the fields in the above columns are unique. Also, verify that the user names from the User Members column already exist in Oracle Identity Cloud Service or in the Users CSV file that is going to be imported before the Groups CSV.

For each account, you create a new row and enter data into each column. Each row equals one record.

When updating the Groups CSV file, you can get the Group Display Names and Description by logging in to IDCS with any Admin user credentials.

In the below table, you can see the OOB IDCS Group Names and Descriptions created as part of the initial installation in IDCS. A user with IDCS Admin privileges can see the groups in IDCS based on the DEV, VAL or PROD environments:

Group Display Name	Description
ls-oasafety-<env>-bi-FAR_Admin_group	FAR Administrator Group
ls-oasafety-<env>-bi-FAR_SafetyAuthor_group	FAR Safety Author Group
ls-oasafety-<env>-bi-FAR_SafetyConsumer_group	FAR Safety Consumers Group
ls-oasafety-<env>-bi-AI_Admin_group	AI Administrator Group
ls-oasafety-<env>-bi-AI_Author_group	AI Author Group
ls-oasafety-<env>-bi-AI_Consumer_group	AI Consumer Group
ls-oasafety-<env>-bi-PVA_Admin_group	PVA Administrator Group
ls-oasafety-<env>-bi-PVA_Safety_group	PVA Safety Author Group
ls-oasafety-<env>-bi-PVA_SafetyConsumer_group	PVA Safety Consumers Group
ls-oasafety-<env>-bi-EXP_Admin_group	EXP Administrator Group
ls-oasafety-<env>-bi-EXP_SafetyAuthor_group	EXP Safety Author Group
ls-oasafety-<env>-bi-EXP_SafetyConsumer_group	EXP Safety Consumers Group
ls-oasafety-<env>-bi-DV_Admin_group	DV Administrator Group
ls-oasafety-<env>-bi-DV_Author_group	DV Author Group
ls-oasafety-<env>-bi-DV_Consumer_group	DV Consumers Group
ls-oasafety-<env>-as-group	Argus Safety Group
ls-oasafety-<env>-b2bi-configure-group	AxwayB2BI Admin Role
ls-oasafety-<env>-b2bi-monitor-group	AxwayB2Bi View Reports Role
ls-oasafety-<env>-soa-configure-group	SOA B2B Configure Role
ls-oasafety-<env>-soa-monitor-group	SOA B2B Monitor Role

> **Note**
>
> The <env> value from the above table can be set as **dev**, **val** or **prod**. For example: `ls-oasafety-dev-bi-DV_Admin_group`, `ls-oasafety-val-bi-PVA_SafetyConsumer_group` or `ls-oasafety-prod-bi-PVA_Safety_group`.

The user needs to prepare all the OOB groups for each environment: dev, val and prod. In addition, the user needs to have either SOA or Axway groups based on the gateway configured in the environment.

Apart from OOB Groups, the user can also add custom groups in the CSV file, along with proper description and user members.

Figure 2-3 Group CSV example

	A	B	C
1	Display Name	Description	User Memebers
2	ls-oasafety-cust1-bi-PVA_Admin_group	PVA Administrator Group	jsmith; jane.doe@abc.com;tushar
3	ls-oasafety-cust1-bi-EXP_SafetyAuthor_group	EXP Administrator Group	jsmith;tushar
4	ls-oasafety-cust1-as-group	Argus Safety Group	jsmith;suman.dodda@abc.com
5	ls-oasafety-cust1-bi-AI_Consumer_group	AI Consumers Group	john
6			
7			

The example from above illustrates how you are required to update your `groups.csv` file.

Pre-validation and comparison report

After you completed the CSV file preparation and shared the respective files with the AMS team, a pre-validation and comparison report is executed.

For the comparison report, the CSV files are considered as the Source and the users and groups are the Target in IDCS.

This pre-validation step helps with identifying any issues with the CSV files, such as missing mandatory fields or a change in the Employee Type, for example. For more information, see the Validation, comparison reports and how to take corrective action section.

Onboarding self-service

Before you proceed with the onboarding self-service process, it is required that you prepare the .CSV files for both users and groups as per the required standards. You can find these detailed guidelines in the below chapter: How to prepare for CSV import.

Once the .CSV files are defined, you can import them into IDCS by using the options present in the application.

For more information, see:

- Import users and groups with the Identity Cloud Service (IDCS) console

Import users and groups with the Identity Cloud Service (IDCS) console

How to import users

To import users to IDCS, follow the steps from the Import Users section of the IDCS *Administering Oracle Identity Cloud Service* guide.

How to import groups

To import groups to IDCS, follow the steps from the Import Groups section of the IDCS *Administering Oracle Identity Cloud Service* guide.

About the IDCS report for importing users and groups

The AMS team uses the IDCS Bulk User Migration utility to import users, groups and user-group associations.

Once the utility execution is completed, a log file is generated and it contains the status of the import. The AMS team then shares the report with the user.

The User Status report and the IDCS Group Import Status report contains the following information:

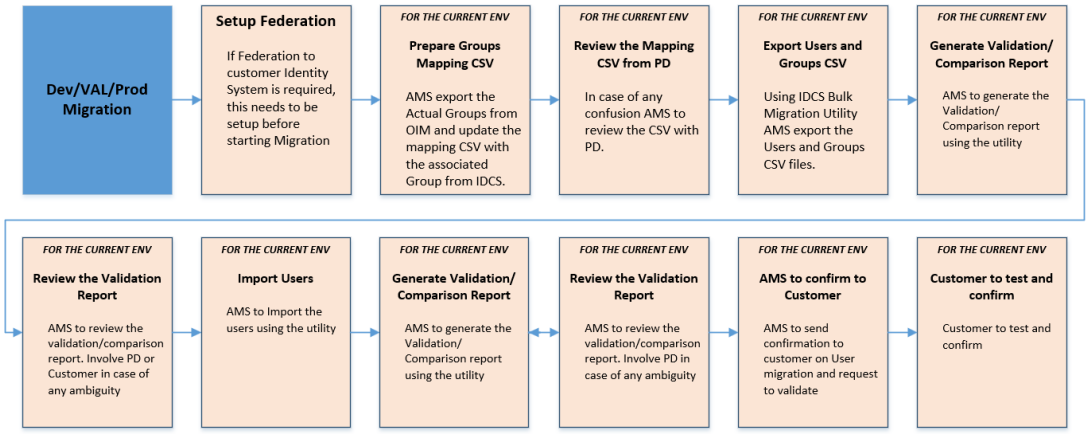
- Report generation date
- Executed by (email ID)
- Customer name
- Customer environment
- Import Job type
- Job ID
- Success count

- Failure count

User group migration from IDM to IDCS

This chapter presents the workflow for Argus Safety users that upgrade from IDM to IDCS. Oracle Application Management (AMS) executes the IDM export utility to capture users, groups and user-group associations. Moreover, IDM user and group export is done for one environment at a time (DEV, VAL and PROD).

Check out the below workflow for user and groups migration:



For the detailed steps, follow the workflow below:

Step No.	Step	Owner	Description
1.	Set up federation	User	This setup is optional. It is only required if the federation is set up between the Oracle IDM and the user's Identity Systems. In case of user migration, federation setup is required. This step is done by the user and it is a one-time setup. For more information on how to set up federation, see the General admin activities chapter.
2.	Prepare group mapping .CSV	AMS	AMS exports Actual Groups from Oracle IDM and then updates the mapping of the .CSV file with the associated IDCS group. This step is done internally for importing groups and user-group associations.
3.	Review the .CSV mapping	AMS	AMS reviews the .CSV mapping
4.	Export users and groups .CSV files	AMS	AMS exports the users and groups .CSV files by using the IDCS bulk migration utility.
5.	Generate the validation and comparison report	AMS	AMS generates the validation and comparison report by using the IDCS bulk migration utility.

Step No.	Step	Owner	Description
6.	Review the validation report	AMS	AMS is required to review the validation and comparison reports and involve the user when required. AMS updates or modifies the required information as per the reports. **Note:** Refer to the *Validation and Comparison reports* section for more information.
7.	Import users and groups	AMS	AMS imports the users and groups .CSV files by using the IDCS User Migration utility. Once the import is completed, a status report is generated.
8.	Generate the validation and comparison report	AMS	After the import is completed, AMS generates the validation and comparison reports again.
9.	Review the validation report	AMS	AMS is required to review the validation and comparison reports and involve the user when required. AMS updates or modifies the required information as per the reports. **Note:** Refer to the *Validation and Comparison reports* section for more information.
10.	AMS sends confirmation	AMS	AMS sends the user a confirmation stating that the import is successfully completed and then requests to validate the user group migration.
11.	User tests and confirms the migration.	User	The user is required to test the user group migration and then to confirm that the migration was successful.

For more information on migration from IDM to IDCS, navigate to My Oracle Support, and search for Doc ID 2979853.1. To access this article, you must be logged in to My Oracle Support.

Export user group information from IDM

AMS executes the automated Export utility to add the users, groups and user-group association to the .CSV file.

The following columns are exported from Oracle IDM:

Column name in the OIM table (IDM)	Mapped to the following column in IDCS
USR_LOGIN	User Name
USR_STATUS	Active
USR_POSTAL_ADDRESS	Work Address Street
USR_LOCALITY_NAME	Work Address Locality
USR_POSTAL_CODE	Work Address Postal Code
USR_COUNTRY	Work Address Country
USR_HOME_POSTAL_ADDRESS	Home Address Street
USR_DISPLAY_NAME	Display Name

Column name in the OIM table (IDM)	Mapped to the following column in IDCS
USR_EMAIL	Work Email
USR_LOCALE	Locale
USR_INITIALS	Honorific Prefix
USR_FIRST_NAME	First Name
USR_MIDDLE_NAME	Middle Name
USR_LAST_NAME	Last Name
USR_TELEPHONE_NUMBER	Work Phone
USR_MOBILE	Mobile No
USR_HOME_PHONE	Home Phone
USR_FAX	Fax
USR_PAGER	Pager
USR_LANGUAGE	Preferred Language
USR_TIMEZONE	Time Zone
USR_TITLE	Title
USR_EMP_TYPE	User Type
USR_DEPT_NO	Department
USR_EMP_NO	Employee Number
USR_MANAGER	Manager
ACT_KEY (ORGANIZATION)	Organization Name
USR_POSTAL_ADDRESS	Instant Messaging Address

Groups and user-group association are exported from IDM for the current environment where IDCS migration is being done.

Environment-specific migration

Migration is specific to each environment, which means that only the users and their group association with the current environment where migration is done are migrated.

After the environment is migrated, the user is advised to use IDCS to manage the environment.

Any user who has access only to the environment that is currently migrated:

- Any changes done to the user attributes in IDM post-migration will not be migrated to IDCS.
- If a user is assigned to an IDM Groups/Roles for an environment that is not yet migrated, then these changes are migrated to IDCS during the migration of that specific environment.

> **Note**
>
> Deleted users in IDM are not exported from IDM.

> **Note**
>
> Locked users in IDM are marked as unlocked in IDCS as part of the import.

> **Note**
>
> User passwords are not migrated from IDM to IDCS.

> **Note**
>
> All CDA users are exported, irrespective of environment export/import.

Import user group information to IDCS

Once the .CSV files are generated, AMS executes the pre-validation report on those files. In addition, the user can take corrective actions, in case there are any discrepancies, and then send the .CSV files to AMS. For more information on the validation and comparison reports, see Validation, comparison reports and how to take corrective action.

AMS imports users and groups by using the IDCS Bulk Migration utility.

After the import is completed, AMS runs the validation and comparison report again to check if there are any issues and then shares the results with the user.

> **Note**
>
> After import, non-federated active users receive an e-mail from IDCS requesting them to activate their account. For federated users, no e-mail is sent.

All CDA users are imported, irrespective of environment and the user assigns the necessary groups to them, as per their respective requirements.

Validation, comparison reports and how to take corrective action

The validation report is run before and after import. This is done to help understand and mitigate if there are any issues with the CSV files, for example if any mandatory fields are missing.

In the case of a new migration, the Source represents the .CSV files that are prepared by the user and the Target is represented by the IDCS users and groups. In case of upgrade, the Source is the IDM users and groups and the Target is the IDCS users and groups.

The validation and comparison of users .CSV and groups .CSV files provides the following information:

User Summary

In the User Summary section of the report, you can find the following information:

The total number of:

- Users
- Active users
- In-active users
- Federated users

- Non-federated users
- Admin users
- Deleted users

User Mandatory Check

If there are any mandatory fields missing, the User Mandatory check section provides the following information:

```
Mandatory Checks
========================================
Missing Work Email for User ID <username1>, at row 3
Missing User Last name for User ID <username2>, at row 4
```

> **Note**
>
> If the above errors are not resolved, then the import fails for the specified users.

If all user entries from the CSV files have all the mandatory fields populated, then the below message is displayed in the Mandatory Checks section:

```
Mandatory Checks
========================================
All mandatory columns are present in Groups.csv. NO ACTION REQUIRED
```

Validating User Type

IDCS supports specified user types only. If any of the user employee type is not set as per the IDCS standards, then the Validating User Type section displays the following warning message:

```
Validating User Type
====================
User Type "Consultant" is not supported by IDCS. User ID xxx, Row 1
User Type "CWK" is not supported by IDCS. User ID xxxxxx , Row 3
User Type "NONW" is not supported by IDCS. User ID xxxxxxxxx , Row 4
User Type "OTHER" is not supported by IDCS. User ID xxxxxxxx , Row 5
```

> **Note**
>
> If the above errors are not resolved, then the import fails for the specified users.

If all user entries from the CSV files match the IDCS standards, then the following message is displayed:

```
All User Type are supported by IDCS. NO ACTION REQUIRED.
```

Validate Bypass Notification

This section features details for the following scenarios:

- When an inactive user's bypass notification is set to False.
- When a federated user's bypass notification is set to False.

The following message is displayed:

```
Validate Bypass Notification
============================
At row 4, for User ID xxxxxxxxx, ACTIVE is FALSE but BYPASS NOTIFICATION is
TRUE
```

If there are no issues with the bypass notification, then the following message is displayed:

```
Bypass notification is correctly marked. NO ACTION REQUIRED.
```

Validate User ID

The user ID is required to adhere to the IDCS standards. If all users are compliant, then the following message is displayed:

```
Validate User ID
================
User ID conforms with IDCS User ID standards. NO ACTION REQUIRED.
```

Validate Active/Federated/Bypass Notification

If the active, federated and bypass notifications have any other value other than True or False set, then the following message is displayed in this section:

```
Validate Active/Federated/Bypass Notification
=============================================
Column Active/Federated/Bypass only has 'true/false' value. NO ACTION
REQUIRED.
```

Admin users

This section displays the CDA Admin users from IDM in case of upgrade.

> **Note**
>
> In case of upgrade, the user assigns the relevant groups to the Admin users listed in this section.

```
Admin users
============
User_test3@gmail.com
custuser3@abc.com
custuser4@abc.com
```

> **Note**
>
> Post-import, you are required to assign appropriate admin groups to the above users.

Deleted users

In case of upgrade, this section displays the deleted users from the IDM Source as follows:

```
Deleted users
==============
deleteduser2@gmail.com
Note: Deleted users will not be imported in IDCS.
```

IDM Source/IDCS Target User Difference Report

This section displays the difference between the Source and Target Users, together with the difference in their attributes:

```
+-----------+-------------+--------------------+-------------------+
| User Name | Field       | Source Value       | Target Value
|
+-----------+-------------+--------------------+-------------------+
|user_dev1  | User Type   | OTHER              | Employee          |
|user_val20 | Display Name| custuser4@abc.com  | cust user4        |
|user_prod4 | Mobile No   |                    | xxxxxxxxx         |
+-----------+-------------+--------------------+-------------------+
```

User available in Source but missing in Target

This section displays the users that are available in Source but not in Target:

```
+--------------------------------------+
| User Name                            |
+--------------------------------------+
| a6888@abc.com                        |
| buser_perf_test100                   |
| john.smith@abc.com                   |
+--------------------------------------+
```

User available in Target but missing in Source

This section displays the users that are available in Target but not in Source:

```
+--------------------------------------+
| User Name                            |
+--------------------------------------+
| dikffj@abc.com                       |
| perf_user1                           |
| tech_user@edrg.com                   |
+--------------------------------------+
```

Actions users can perfom

The user is required to update the mandatory fields wuth the required information. Similarly, various other fields require validation and the report marks the fields that don't comply.

The reports also provides prompts so that the user knows what corrective action is needed. The same corrective method is followed for group associations.

In the validation report, the following columns are mandatory:

- User ID
- Last Name
- First Name
- Work Email
- Primary email Type
- User Type
- Active
- Bypass Notification
- Federated

The user updated the .CSV as per the corrective action displayed in the report and then send the files back to AMS for import.

Once the user confirms the report, then the user approves the import of .CSV files and AMS imports the .CSV files into IDCS.

Comparison report

In this report, you can see a comparison between the information from the already imported users and groups in IDCS. This comparison reports contains the following sections:

- Source / Target User Difference Report
- Users available in Source, but missing in Target
- Users available in Target, but missing in Source
- User Role Association Difference Report
- Admin User Role Association Difference Report
- Deleted Users in the Target

> **Note**
>
> Source refers to IDCS and Target refers to the CSV files.

User and group import status report

User status report

When you import users and groups, a status report is generated and it contains the following information:

```
==================================================
IDCS User Import Status Report
==================================================
Report generation date    : 2023-06-16 10:26:31 UTC
Executed by (email id)    : abc@xyz.com
Customer name             : 12345
Customer environment      : ABCD
Import Job type           : User Import

Job ID                    : 6bc784037b8b4f078d681668c7fd4
Success Count             : 100
Failure Count             : 1
Total Count               : 101


+-------------------------------------------------------------------+
|                 User Import Failure Report                        |
+---------+------------+-----------+--------+-------+---------------+
| User Id | First Name | Last Name | Status | Email | Message       |
+---------+------------+-----------+--------+---------+-------------+
| smith_k | John       | niki      | Active |       | Missing required
attribute(s): emails.value
+-------------------------------------------------------------------+
```

Group status report

```
==================================================
IDCS Group Import Status Report
==================================================
Report generation date    : 2023-06-16 10:26:31 UTC
Executed by (email id)    : abc@xyz.com
Customer name             : 12345
Customer environment      : ABCD
Import Job type           : Groups Import

Job ID                    : 6bc784037b8b4f078d681668c7fd4e1a
Success Count             : 25
Failure Count             : 2
Total Count               : 27

------------------------------------------------------------
Group Import Failure Details
------------------------------------------------------------
Display Name  ls-oasafety-val-bi-EXP_Admin_group, EXP Administrator Group for
val Environment
Error Message Unable to determine the ID for : User : buser_perf_test100
```

```
Display Name  ls-oasafety-val-bi-AI_Admin_group, AI Administrator Group for
val Environment
Error Message Unable to determine the ID for : User : john.smith@abc.com
```

If any discrepancies occur in the report, the user can modify the details of any user or group by logging in to IDCS or the user can perform the import again, by following the same import process.

After the users are created, an e-mail is set by IDCS to the primary e-mail ID of the user, prompting to activate the account. The e-mail contains an *Activate Your Account* link. After the user clicks the link, they are redirected to IDCS and prompted to reset their password.

General admin activities

How to create users in IDCS

See the Create User Accounts section from the IDCS *Administering Oracle Identity Cloud Service guide*.

How to create groups in IDCS

See the Create Groups chapter from the IDCS *Administering Oracle Identity Cloud Service guide*.

How to change the logo in IDCS

See the Customizing the service section from the Oracle IDCS tutorials.

How to set up federation in IDCS

See the Before you begin section of the *Setting Up Federation Between Okta and Oracle Identity Cloud Service* page in Oracle Help Center.

How to enable MFA in IDCS

To set up multi-factor authentication security (MFA) in IDCS, see the Enable Multi-Factor Authentication Security for Oracle Cloud section from the IDCS *Administering Oracle Identity Cloud Service guide*.

How to set password policy

Once migrated to IDCS, customer delegated administrator users (CDA) are requited to manage the password policy. For more information, see the Set the Password Policies for Your Identity Domain section from the IDCS *Administering Oracle Identity Cloud Service guide*.

How to reset the Passwords for User accounts

See the Reset Passwords for User Accounts section from the IDCS *Administering Oracle Identity Cloud Service guide*.

How to activate/deactivate/unlock user accounts

To activate user accounts in IDCS, see the Activate User Accounts section from the IDCS *Administering Oracle Identity Cloud Service* guide.

To deactivate user accounts in IDCS, see the Deactivate User Accounts section from the IDCS *Administering Oracle Identity Cloud Service* guide.

To unlock the user accounts in IDCS, see the Unlock User Accounts section from the IDCS *Administering Oracle Identity Cloud Service* guide.

How to disable notification during user creation

In case you do not want the user to receive notifications during user creation, please follow the steps from the Customize Oracle Identity Cloud Service Notifications section to disable user notification.

How to assign admin roles to CDA users

If you want to assign admin roles to CDA users or read more information about administrator roles and privileges, see the Understand Administrator Roles section from the *Administering Oracle Identity Cloud Service* guide

Case studies for user migration

Federated users

- Both Active and Inactive federated users are migrated from IDM to IDCS and are set as either Active or Inactive.
- These users are marked as Federated in IDCS.
- The federated users do not receive e-mail notifications from IDCS.
- Active federated users are expected to use user identity systems to authenticate to Argus Cloud Service.

Non-federated users

- Both Active and Inactive non-federated users are migrated from IDM to IDCS and are set as either Active or Inactive.
- Active users receive e-mail notifications on the primary e-mail ID mentioned in the user details.
- Inactive users do not receive e-mail notifications from IDCS.
- Active users can log in to IDCS.

Oracle user disabled in IDCS and Active in IAMS

For any Oracle user who is disabled in IDCS and active in IAMS, the IDCS login page displays a message that User is deactivated in IDCS.

Add users to Oracle Argus Cloud Service

Once you have provisioned an user in Oracle Identity Cloud Service (IDCS), you can add the user to Oracle Argus Cloud Service.

To add a user:

1. Open a browser and navigate to your company's Oracle Argus Cloud Service URL. Log in with your Oracle Argus Cloud Service administrator credentials.
2. Click **Argus Console**, then **Access Management**, **Argus**, and **Users**.
3. In the right pane, select **Add Users**.
4. Enter the user name, the user ID and, if applicable, the email address.
5. In the Application Access section, configure the application access.

6. In the Access section, select the applicable options:
   - Account Disabled
   - Security Disabled Account
   - Force Password Change at Login
   - Force Password To Expire Every x Days
   - Reset Password
7. Assign the user to a site.
8. Assign the user to a pre-configured user groups.
9. Select the type of user from the UserType drop-down list.
10. Assign a role to the user.
11. In the Worklist To Display At Login section, configure the users to see their worklist immediately after login.
12. In the Case Form section, select the applicable options.
13. If applicable, select **Enable Site Security** to enable the site-based data security for the user and decide what type of access you grant for each site.
14. Click **Save** to save the new user.

> **Note**
>
> - When you create a user in Oracle Argus Cloud Service, you must use the same user name and email address that you used when you created the user in Oracle Identity Cloud Service (IDCS).
> - When you use Oracle Identity Self Service authentication, you must select **Enable LDAP Login** in the Oracle Argus Cloud Service user creation pane.

For more information about the fields in the Add User window, see:

- Users fields description
  Find here a table that describes the fields in the Users section.

Users fields description

Find here a table that describes the fields in the Users section.

Field or Control Name	Description
User Name	Enter the full name.
User ID	Enter a unique user identification (ID).
Reset Password	Reset the password of a user to a default value specified in the common profile section.
Email Address	Enter the user's e-mail address.
Site	Assign the user to a site. The values in this field are populated from the codelist item **User Sites**.
User Group - Select	Attach the user to pre-configured user groups.

Field or Control Name	Description
User Type	Select the type of user, such as an Oracle Argus Safety Japan user, from the drop-down list.
User Roles - Select	Attach the user to pre-configured user roles. The following user roles are available: • **Enterprise User** - allows you to configure a workflow manager user as an enterprise user. If the enterprise role is assigned, the user can view cases of any site outside their own site. • **ESM Admin** - allows the user to access the Interchange Mapping utility in the Argus Console. • **Copy Configuration** - lets a user copy all the configuration data from the enterprise where they have this role to any new enterprise that they create through Global Enterprise Management. The factory data administrator user has this role enabled by default. • **Global Admin** - gives you the right to designate users as Global Users for selected enterprises, and not necessarily all enterprises. By default, a Global Admin role is granted to only one administrator, who can grant/ revoke this role to other Argus users. • **AC Library Admin** - gives you the right to allow users to perform specific operations on ACs, such as re-assigning the ownership, and granting access to various user groups using Permission, Modification, and Deletion. • **Intake Designer** - creates document processing recipes for Condolidated Intake. • **Intake Processor** - verifies the data in the various records that are ingested to the consolidated Intake Worklist and controls whether the records are accepted as cases for further processing. This role is required to access the Intake Worklist located in the Consolidated Intake interface. • **Workflow Manager** - allows users to perform specific workflow operations such as routing cases to any workflow state, routing cases to users, viewing all open cases and all action items present in the system, changing the priority of a case and changing the assignee of an action item or a case.
Application Access	Configure the user access settings for Argus Console and Oracle Argus Safety. You can select the default application access for the user from the list.
Worklist to display at login	Configure users to see their worklists immediately upon login. The options are: • **None** (default) - Does not open any worklist when the user logs into Oracle Argus Cloud Service. Displays personal Oracle Argus status on login. • **Action Items** - Opens Worklist - Action Items screen for the user on login. • **New** - Opens Worklist - New screen for the user on login. • **Open** - Opens Worklist - Open screen for the user on login. • **Reports** - Opens Worklist - Reports screen for the user on login.
Enable Site Security	If **Enable Site Security** is checked, the site-based data security will be enabled for the user. If the box is not checked, the user will have full access to data from all sites.
Service User	This check box is enabled for the Argus Service users (system users).
LDAP Server Alias	This is the alias for the LDAP server used for user authentication if the LDAP login is enabled for a user.
Enable LDAP Login	Authenticates users against the active directory server. When **Enable LDAP Login** is selected, all fields inside the **Access** section are disabled, excluding the **Account Disabled** option.

Field or Control Name	Description
Account Disabled	When this option is selected, the user account is temporarily disabled to prevent users from logging in. This option is different from deleting a user, as it enables you to re-activate the account at a later date. Before you disable a user account in Oracle Argus Cloud Service, you must disable the account in Oracle Identity Self Service. For more information, see *Disable a User Account* below.
Security Disabled Account	When unchecked, the login procedure keeps track of the number of consecutive unsuccessful attempts at logging into the system. If the count reaches three, the user is locked out. Administrators with rights to user maintenance can reset the login attempts for the user to unlock the account. When checked, the login procedure that tracks the consecutive unsuccessful attempts at logging in to the system does not apply.
Force Password Change at Login	If this check box is selected, the user must change the password the first time they log in to the system.
Force Password To Expire Every	Enables you to force the user's password to expire in the specified number of days.
Days	Enables you to enter the number of days after which the password should expire.
Allow Unblinding Of Cases	Enables the user to unblind a study case. For example, a user without unblinding rights does not see the Study Drug field. A user with unblinding rights sees a yellow Unblind tag next to concentration of product field and the **Broken by Sponsor** option in the **Blinding Status** drop-down if enabled. The user will have to enter their password when they select the **Broken by Sponsor** option.
Protect From Unblinded Information	When checked, the user cannot view any unblinded information.
Protect From Printing Unblinded Information	When checked, the user cannot print any unblinded information.
Allow Locking Of Cases	Enables the user to lock/unlock cases.
Allow Local Locking	Enables the user to locally lock/unlock a case for which local Japan data entry/assessment is complete, triggering the scheduling and/or generation of the applicable local reports.
Allow Forced Unlock On Pending Reports	Allow users to force unlock the pending reports.
Allow Global Unlock On Pending Local Lock	Allows users to be set up with the privilege to forcibly unlock a case that is still pending a local lock. This option is enabled only if the **Allow locking of cases** check box (above) is checked.
Allow Closing Of Cases	Allows the user to close cases.
Route On Close Case	Opens a routing dialog when the user closes the case.
Enable Checklist On Route	By default, this check box is selected. If this check box is not selected, the checklist for the workflow is not displayed to the user while routing cases, even if the rule that is being used has a checklist.

Filtering sites, groups and users

You can use the available filtering criteria for sites, groups and users to search for specific items.

The Oracle Argus Cloud Service administration console provides filtering options for the **Access Management** section.

The system displays the filtering criteria in the top-left corner of the left pane. You can filter information based on:

- Code list if you select **Sites** from the Access Management drop-down list
- Groups or users if you select **Groups** or **Users** from the Access Management drop-down list.

For more information, see:

- Applying filters to users and groups

Applying filters to users and groups

You can filter based on either of the two options in the drop-down list, **Groups** and **Users**:

- If you enable **Organized by Groups**, the generated output is displayed in a tree format in the left pane. The structure is based on the entire categorization of groups and users.
- If you enable the **Organized by Users**, only the user list is available in the tree view in the left pane.

Use **Contains** or **Starts with** to specify whether your search should contain or start with specific characters. For example, if you select **Contains** and type **administrator** in the text box, the system searches for all the groups that contain the word "administrator".

3

Manage Argus Advanced Cloud Service

There are several actions you can take for the Oracle Argus Advanced Cloud Service management.

- Create a new enterprise in Oracle Argus Mart
  To create a new enterprise in Oracle Argus Mart, you need to create a change request ticket in Life Sciences Customer Support Portal.
- Extract, Transform and Load data (ETL)
  The change request examples included below for Extract, Transform and Load (ETL) tasks can be used for Oracle Argus Mart, Oracle Argus Analytics, and Oracle Argus Insight.
- Replicate your data
  The Oracle Argus Data Replication Cloud Service continuously recreates a copy of Oracle Argus Cloud data into the user's target database to support integration with existing third party applications, extensions, and reporting solutions.
- Grant users with Oracle Argus Analytics access
  To grant Oracle Argus Cloud Service users with Oracle Argus Analytics access, you need to associate their user accounts with specific roles in Oracle Identity Cloud Service (IDCS).
- About Product Verification Pack (PVP)
  The Product Verification Pack (PVP) is a collection of product release artifacts that are aimed at helping with your validation efforts.

Create a new enterprise in Oracle Argus Mart

To create a new enterprise in Oracle Argus Mart, you need to create a change request ticket in Life Sciences Customer Support Portal.

1. Log in to the Life Sciences Customer Support Portal .
2. Click **Create Request** in the upper right corner, then select **Support Request**.
3. In the **Summary** field, enter a short description of your request.

   Example: `Create enterprise <enterprise name> in the <environment name> environment.`
4. Select appropriate values from the **Severity** drop-down lists.
5. In the **Description** field, enter a detailed description of your request, including the enterprise to use as a source for the configuration of the new enterprise.

   Example: `Please create a new enterprise named <enterprise name> in the <environment name> environment, using <source enterprise name> as a source to copy the configuration.`
6. If you have a ticket reference number that corresponds to this request, enter it in the **Alternative reference number (if applicable)** field.
7. From the **Oracle Internal** radio buttons, select **No**.
8. From the **Customer** drop-down list, search for your company's name and select it from the list.

9. From the **Product** drop-down list, select **Argus Safety**.
10. From the **Business Service** drop-down list, select the name of the server where you want to create the enterprise.
11. From the **Issue Category** drop-down list, select **Other**.
12. From the **Environment** drop-down list, select the environment where you want to create the new enterprise, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.

    If you select **Other** or **Not Sure**, enter the URL of the application in the **Application URL/ Website Address** field.
13. You can attach files relevant to the request in the **Attachments** section.
14. In the **Additional Watchers** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. Click **Submit**.

Extract, Transform and Load data (ETL)

The change request examples included below for Extract, Transform and Load (ETL) tasks can be used for Oracle Argus Mart, Oracle Argus Analytics, and Oracle Argus Insight.

Make sure you include the applicable product name in your change request, instead of the *<product name>* placeholder.

For more information, see:

- Run the initial ETL
  To run the initial ETL, you need to create a change request ticket in Life Sciences Customer Support Portal.
- Schedule incremental ETLs
  To schedule incremental ETLs, you need to create a change request ticket in Life Sciences Customer Support Portal.
- Re-initialize the ETL process
  Once an initial ETL process has been successfully executed on a database, it cannot be executed again until the Mart environment is reset. To request this:

Run the initial ETL

To run the initial ETL, you need to create a change request ticket in Life Sciences Customer Support Portal.

1. Log in to the Life Sciences Customer Support Portal .
2. Click **Create Request** in the upper right corner, then select **Support Request**.
3. In the **Summary** field, enter a short description of your request.

   Example: `Run <product name> initial ETL in the <environment name> environment.`
4. Select appropriate values from the **Severity** drop-down lists.
5. In the **Description** field, enter a detailed description of your request.
6. If you have a ticket reference number that corresponds to this request, enter it in the **Alternative reference number (if applicable)** field.

7. From the **Oracle Internal** radio buttons, select **No**.
8. From the **Customer** drop-down list, search for your company's name and select it from the list.
9. From the **Product** drop-down list, select **Argus Safety**.
10. From the **Business Service** drop-down list, select the name of the server where you want to run the initial ETL.
11. From the **Issue Category** drop-down list, expand **Service Request**, then **Application**, **General**, and select **Action**.
12. From the **Environment** drop-down list, select the environment where you want to run the initial ETL, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.

    If you select **Other** or **Not Sure**, enter the URL of the application in the **Application URL/ Website Address** field.
13. You can attach files relevant to the request in the **Attachments** section.
14. In the **Additional Watchers** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. Click **Submit**.

Schedule incremental ETLs

To schedule incremental ETLs, you need to create a change request ticket in Life Sciences Customer Support Portal.

1. Log in to the Life Sciences Customer Support Portal .
2. Click **Create Request** in the upper right corner, then select **Support Request**.
3. In the **Summary** field, enter a short description of your request.

   Example: `Schedule <product name> incremental ETLs in the <environment name> environment.`
4. Select appropriate values from the **Severity** drop-down lists.
5. In the **Description** field, enter a detailed description of your request.

   Example: `Please schedule <product name> incremental ETLs to run every <number> hours in the <environment name> environment.`
6. If you have a ticket reference number that corresponds to this request, enter it in the **Alternative reference number (if applicable)** field.
7. From the **Oracle Internal** radio buttons, select **No**.
8. From the **Customer** drop-down list, search for your company's name and select it from the list.
9. From the **Product** drop-down list, select **Argus Safety**.
10. From the **Business Service** drop-down list, select the name of the server where you want to schedule the incremental ETLs.
11. From the **Issue Category** drop-down list, expand **Service Request**, then **Application**, **General**, and select **Action**.
12. From the **Environment** drop-down list, select the environment where you want to create the new enterprise schedule the incremental ETLs, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down list above.

If you select **Other** or **Not Sure**, enter the URL of the application in the **Application URL/ Website Address** field.

13. You can attach files relevant to the request in the **Attachments** section.
14. In the **Additional Watchers** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. Click **Submit**.

Re-initialize the ETL process

Once an initial ETL process has been successfully executed on a database, it cannot be executed again until the Mart environment is reset. To request this:

1. Log in to the Life Sciences Customer Support Portal .
2. Click **Create Request** in the upper right corner, then select **Support Request**.
3. In the **Summary** field, enter a short description of your request.

   Example: `Run re-initial <product name> ETL in the <environment name> environment.`
4. From the **Severity** drop-down list, select the appropriate value.
5. In the **Description** field, enter a detailed description of your request.

   Example: `Please run a re-initial <product name> ETL in the <environment name> environment.`
6. If you have a ticket reference number that corresponds to this request, enter it in the **Alternative reference number (if applicable)** field.
7. From the **Oracle Internal** radio buttons, select **No**.
8. From the **Customer** drop-down list, search for your company's name and select it from the list.
9. From the **Product** drop-down list, select **Argus Safety**.
10. From the **Business Service** drop-down list, select the name of the server where you want to re-initialize the ETL process.
11. From the **Issue Category** drop-down list, expand **Service Request**, then **Application**, **General**, and select **Action**.
12. From the **Environment** drop-down list, select the environment where you want to e-initialize the ETL process, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down list above.

    If you select **Other** or **Not Sure**, enter the URL of the application in the **Application URL/ Website Address** field.
13. You can attach files relevant to the request in the **Attachments** section.
14. In the **Additional Watchers** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. Click **Submit**.

Replicate your data

The Oracle Argus Data Replication Cloud Service continuously recreates a copy of Oracle Argus Cloud data into the user's target database to support integration with existing third party applications, extensions, and reporting solutions.

What does it do?

The Oracle Argus Data Replication Cloud Service enables users to replicate cloud data in the Oracle GBU tenancy to a separate database instance in their own target environment (OCI tenancy, User's Premise, AWS, or Azure) using GoldenGate.

This utility includes:

- **Initial data load**. An initial load synchronizes the source and target databases. It extracts an entire copy of the source dataset, transforms it (if necessary), and applies it to the target tables.
- **On-going replication**. After the initial data load, an on-going data replication process from the Oracle Argus Cloud source database to user managed target database begins.
- **Monitoring**. Users can monitor the overall health and performance of the source side replication process.

How do I get it?

This utility requires an additional subscription, so you need first to purchase the Oracle Argus Data Replication Cloud Service utility license. Contact your sales representative for more information.

Where can I find more information?

For information about Oracle Argus Data Replication Cloud Service and the deployment process, log in to My Oracle Support and see article *2702658.1*.

Grant users with Oracle Argus Analytics access

To grant Oracle Argus Cloud Service users with Oracle Argus Analytics access, you need to associate their user accounts with specific roles in Oracle Identity Cloud Service (IDCS).

Oracle Argus Cloud Service users can access Oracle Analytics Server (OAS) and Oracle Analytics Publisher based on their user type and role.

Once you have identified the specific role for each user account that needs to access OAS and Publisher, you must Create groups in IDCS and Assign groups to user accounts in IDCS.

Note

- Make sure that the respective user accounts are available in Argus and have access to Oracle Argus Analytics.
- The roles will be provisioned as part of Argus Cloud Setup and are available to the CDA.
- Any user should only be associated with one Oracle Argus Analytics role. Any association with more than one role will result in having zero privileges.

After completing the role association, when the users log in to OAS, they will be able to access the Oracle Argus Analytics application (Privilege will be based on the associated Role).

- Oracle Analytics Server (OAS) and Oracle Analytics Publisher user types
  There are three types of OAS and Publisher users.
- Oracle Analytics Server (OAS) and Oracle Analytics Publisher user roles
  There are multiple out-of-the-box OAS and Publisher roles available for Oracle Argus Cloud Service users.
- Oracle Analytics Server (OAS) and Oracle Analytics Publisher users examples
  Some OAS and Publisher users examples, for a better understanding of the user type and role association.

Oracle Analytics Server (OAS) and Oracle Analytics Publisher user types

There are three types of OAS and Publisher users.

- **Admin**: can create, update, delete, and view reports and dashboards. Moreover, the admin user has OAS and Publisher Administrator privileges. This user is similar to the Customer Delegated Administrator user in IDCS and only few users in an organization should have this privilege.
- **Author**: can create, update, delete, and view reports and dashboards. Only few users from technical team that design and develop custom reports should have this privilege.
- **Customer**: can view and generate reports and dashboards. These are typical end users who generate reports continuously.

Oracle Analytics Server (OAS) and Oracle Analytics Publisher user roles

There are multiple out-of-the-box OAS and Publisher roles available for Oracle Argus Cloud Service users.

Associate Oracle Argus Cloud Service user accounts with specific roles in IDCS, according to their user type.

#	Role	Type	Subject Area	Description
1	FARAdminGroup	Admin	Argus Safety Aggregate Reporting	Admin for FAR (Argus Safety Aggregate Reporting) Publisher Reports
2	FARSafetyAuthorGroup	Author	Argus Safety Aggregate Reporting	Author for FAR (Argus Safety Aggregate Reporting) Publisher Reports
3	FARSafetyConsumerGroup	Consumer	Argus Safety Aggregate Reporting	Consumer for FAR (Argus Safety Aggregate Reporting) Publisher Reports
4	AIAdminGroup	Admin	Argus Insight	Admin for AI (Oracle Argus Insight) Publisher Reports
5	AIAuthorGroup	Author	Argus Insight	Author for AI (Oracle Argus Insight) Publisher Reports
6	AISafetyConsumerGroup	Consumer	Argus Insight	Consumer for AI (Oracle Argus Insight) Publisher Reports
7	PVAAdmin	Admin	Argus Analytics	Admin for Oracle Argus Analytics OAS Reports

#	Role	Type	Subject Area	Description
8	PVASafetyGroup	Author	Argus Analytics	Author for Oracle Argus Analytics OAS Reports
9	PVASafetyConsumersGroup	Consumer	Argus Analytics	Consumer for Oracle Argus Analytics OAS Reports
10	EXPAdminGroup	Admin	Argus Safety Expedited Reports	Admin for Argus Safety Expedited Publisher Reports
11	EXPSafetyAuthorGroup	Author	Argus Safety Expedited Reports	Author for Argus Safety Expedited Publisher Reports
12	EXPSafetyConsumerGroup	Consumer	Argus Safety Expedited Reports	Consumer for Argus Safety Expedited Publisher Reports

Note

- The Admin role includes the privileges associated with the Author and Consumer role.
- The Author role includes the privileges associated with the Consumer role.
- Any user has all the privileges associated with the Subject Area.

Oracle Analytics Server (OAS) and Oracle Analytics Publisher users examples

Some OAS and Publisher users examples, for a better understanding of the user type and role association.

In the following table, each type of user has only the roles associated in IDCS.

#	Type of User	Type of User	Roles/Groups associated with the users
1	**Organization Admin User**: can view, update, delete and create reports and dashboards.	Admin	• FARAdminGroup • AIAdminGroup • PVAAdmin • EXPAdminGroup
2	**Organization Author Users**: can view, update, delete and create reports and dashboards across all Subject Areas.	Author	• FARSafetyAuthorGroup • AIAuthorGroup • PVASafetyGroup • EXPSafetyAuthorGroup
3	**Author for Argus Analytics Reports and Dashboards**: can view, update, delete and create reports and dashboards only for Argus Analytics.	Author	• PVASafetyGroup
4	**Organizational Consumers**: can view and generate reports and dashboards across all the Subject Areas.	Consumer	• FARSafetyConsumerGroup • AISafetyConsumerGroup • PVASafetyConsumerGroup • ExpSafetyConsumerGroup

About Product Verification Pack (PVP)

The Product Verification Pack (PVP) is a collection of product release artifacts that are aimed at helping with your validation efforts.

The documents in the PVP are used by Oracle for product certification purposes, and Oracle makes the documents available to you at no charge with each major and minor product release. You can use the PVP as a blueprint for acceptance testing.

> **Note**
>
> PVP is available for both Basic and Advanced Oracle Argus Cloud Service subscriptions.

You'll find the following documents in the Oracle Argus Safety PVPs:

- Summary report
- Test requirements
- Test cases
- Traceability matrix
- Test results
- Objective evidence.

A new PVP is made available for every release except patch releases.

We request you to use this PVP on as-is basis and modify as suitable to your intended use of the application, configuration and environment prior to using application in production.

For more information, see:

- Obtain a Product Verification Pack
  To obtain a PVP, you need to create a change request ticket in Oracle Life Sciences Customer Support Portal.

Obtain a Product Verification Pack

To obtain a PVP, you need to create a change request ticket in Oracle Life Sciences Customer Support Portal.

1. Log in to the Life Sciences Customer Support Portal .
2. Click **Create Request** in the upper right corner, then select **Support Request**.
3. In the **Summary** field, enter your request as a short text.
4. From the **Severity** drop-down list, select **4 - Low**.
5. In the **Description** field, provide the SFTP access details to a remote folder where the Oracle support team can copy the requested PVP files.
6. If you have a ticket reference number that corresponds to this request, enter it in the **Alternative reference number (if applicable)** field.
7. From the **Oracle Internal** radio buttons, select **No**.

8. From the **Customer** drop-down list, search for your company's name and select it from the list.
9. From the **Product** drop-down list, select **Argus Safety**.
10. From the **Business Service** drop-down list, select a business service or **No Value**.
11. From the **Issue Category** drop-down list, select **General Inquiry**.
12. From the **Environment** drop-down list, select the environment type.

    If you select **Other** or **Not Sure**, enter the URL of the application in the **Application URL/ Website Address** field.
13. You can attach files relevant to the request in the **Attachments** section.
14. In the **Additional Watchers** field you can enter one or more email addresses to be notified about this request, separated by a semicolon.
15. Click **Submit**.

    You will receive an email confirmation of your submission.

4

Manage dictionaries

Dictionaries are loaded and managed using the Dictionary Management menu in Argus Console to ensure adverse event terms, drug coding, and device problems are coded correctly.

You can load new dictionaries, overwrite existing dictionaries, recode a MedDRA dictionary, or load a dataset for smart event encoding.

For details refer to the *Oracle Argus Safety Administration Guide > Dictionaries Management*.

5

Use the Argus Cloud Service utilities

Oracle Argus Cloud Service provides various utilities that the Oracle team executes after receiving a Change Request through the Life Sciences Customer Support Portal.

- Data Refresh
  This utility adds the data refresh and restoration capability to Oracle Argus Cloud.
- Data Refresh Enterprise Specific
  This utility adds the data refresh and restoration capability for specific enterprises to Oracle Argus Cloud. This utility is for CRO customers.
- Extensibility and Integrations Framework
  Use this utility to develop and deploy business extensions and cloud integrations into Oracle Argus Cloud Service.
- Gateway Certificate Expiry Alert Notification
  Use this utility to notify users about the Gateway Certificates expiration.
- Monitoring
  The Monitoring utility is an internal custom plug-in that leverages Oracle Enterprise Manager (OEM) to monitor the Argus application.
- Usage Billing
  Use this utility to track your case volume by generating various license usage reports.
- Enterprise Export
  Use this utility to export data for a specific tenant or Enterprise.

Data Refresh

This utility adds the data refresh and restoration capability to Oracle Argus Cloud.

What does it do?

Users periodically refresh the data in the Development and Validation environments. Using current Production data is necessary to facilitate validation efforts with release upgrades.

The Data Refresh utility provides automated data refresh and restoration capabilities, allowing users to copy data from their Production to Development and/or Validation environments with minimum manual intervention.

How do I get it?

You need to create a change request (CR) in the Life Sciences Customer Support Portal, asking to execute the Oracle Argus Data Refresh utility. After logging the CR, the Oracle team will run the utility in the environment you specify.

Where can I find more information?

Log in to My Oracle Support and search for the following article: *KB317773*. Locate the Release Notes for Data Refresh.

Data Refresh Enterprise Specific

This utility adds the data refresh and restoration capability for specific enterprises to Oracle Argus Cloud. This utility is for CRO customers.

What does it do?

Users periodically refresh the data in the Development and Validation environments. Using current Production data is necessary to facilitate validation efforts with release upgrades.

For CRO customers, the Data Refresh Enterprise Specific utility provides automated data refresh and restoration capabilities at enterprise level, allowing users to copy data from their Production to Development and/or Validation environments with minimum manual intervention for the specific enterprises.

How do I get it?

You need to create a change request (CR) in the Life Sciences Customer Support Portal, asking to execute the Oracle Argus Data Refresh Enterprise Specific utility. After logging the CR, the Oracle team will run the utility in the environment you specify.

Where can I find more information?

Log in to My Oracle Support and search for the following article: *KB317773*. Locate the Release Notes for Data Refresh.

Extensibility and Integrations Framework

Use this utility to develop and deploy business extensions and cloud integrations into Oracle Argus Cloud Service.

What does it do?

The Extensibility and Integrations Framework allows you to develop business extensions and cloud integrations in the Oracle Argus Cloud using PL/SQL code.

With this utility, you can deploy and utilize custom database objects through a special customized schema, by leveraging the reporting and ETL extensibility without impacting the out-of-the-box database objects supplied by Oracle Argus Safety.

Extensibility and Integrations Use Cases

The following use case examples provide a high level overview of what you can do with this framework:

- **Cloud Integration**. You can directly access your database to push periodic updates to the central repository to downstream applications such as Oracle Argus Safety to maintain compliance.

Master Data Load	When you maintain a central repository (custom and/or 3rd party such as SAP or Oracle Agile PLM etc.) to store master data, you can push periodic updates for the following field types to maintain compliance: – Company products and licenses

	– Study information – Datasheets – Product lot numbers – Product distribution data.
Reference Data Load	When you maintain a central repository to reference data, you can push updates for: – MEDDRA - Synonym list, Event list, etc. – Reporter data and institution data load.
Argus Configuration Data Load	Reduces the effort required to manually configure data load through the Oracle Argus Safety application. – Argus accelerators built by customers and partners automate the Argus Configuration data loading process. For example, Codelist, Reporting rules, Product-Study data load, Case Processing rules, Workflow rules etc.

- **Business Extensions**. You can now directly extend business rules by writing your own packages using the following extensions:

Pre/Post Case Save Business Extension	You can configure extensions in the Case Save extension hooks to: – Add Validation Logic. – Update Case Data – user defined fields, generate Action Items, Event Assessment. – Populate custom tables for Reporting/ Analysis. – Use PL/SQL functions, Procedures, or Packages. – Audit Case Data.
Case Processing Automation	**Medical Narrative Placeholders** – Summarize all relevant clinical and related information, including patient demographics, therapy details, medical history, clinical course of the event(s), relevant laboratory evidence, and any other information that contributes to an adverse event (AE) assessment. – Contain adequate information to serve as a comprehensive stand-alone “medical story”.

- Have a corresponding SQL statement to be executed by the respective narrative.

Letter Templates Placeholders:

- Letter templates are defined by the Safety department to perform Case Queries or/and follow-up Case Processing via email.
- Specialized letter templates are created for specific Products and/or Events such as Cancer therapies, Pregnancy cases etc.
- Placeholders have a corresponding SQL statement to be executed by the respective letter template.
- They are important to Argus Case processing, save manual effort, and enable good PV practices.

Case Data Update as per changes in the Master Data:

- Datasheet changes trigger Event Assessment.

How do I get it?

You need to create a change request (CR) in the Life Sciences Customer Support Portal, asking to execute the Argus Cloud Extensibility and Integrations Framework utility. After logging the CR, the Oracle team will run the utility in the environment you specify.

Where can I find more information?

Log in to My Oracle Support and search for the following article: *KB317773*. Locate the Release Notes for Extensibility and Integrations Framework.

Gateway Certificate Expiry Alert Notification

Use this utility to notify users about the Gateway Certificates expiration.

What does it do?

The Gateway Certificate Expiry Alert Notification utility sends an automated email when a configured Gateway Certificate has been expired or about to expire.

How do I get it?

You need to create a change request (CR) in the Life Sciences Customer Support Portal, asking to execute this utility, and provide the following information, based on the gateway you are using (Axway or Oracle B2B):

Axway/B2Bi

1. Certificate Expiry Alert Days - Number of days to receive alert notification in advance before the certificate expiry date.

> **Note**
>
> This field is set to 30 days, by default. You can request to modify this field as per your requirement.

2. Email Addresses:
   - FROM - Sender's email address to send out the certificate expiry alert notification email.

     > **Note**
     >
     > You can provide a different sender email address for each environment (Development/Validation/Production). To identify the email alert received from each environment, you must provide distinct email address for each environment. For the example:
     >
     > *PROD_<customer>_noreply@<customerdomain>*
     >
     > *VAL_<customer>_noreply@<customerdomain>*
     >
     > The sender's email address is not required to be a valid one.
     >
     > If this field is being configured at the community level to support any AS1 transmission, then the FROM email address at alert.xml will be overridden. Hence, when this field is configured it must be distinct to identify the environment.

   - TO - Receiver's email address who would receive the certificate expiry alert notification email: Receiver Email Address.
3. Community - Community for which the certificate expiry alert notifications are triggered.

Oracle B2B

1. TO - Receiver's email address who would receive the certificate expiry alert notification email: Receiver Email Address.
2. Certificate Expiry Alert Days - Number of days to receive alert notification in advance before the certificate expiry date.

> **Note**
>
> This field is set to 30 days, by default. You can request to modify this field as per your requirement.

Where can I find more information?

Log in to My Oracle Support and search for the following article: *KB317773*. Locate the Release Notes for Gateway Certificate Expiry Alert Notification.

Monitoring

The Monitoring utility is an internal custom plug-in that leverages Oracle Enterprise Manager (OEM) to monitor the Argus application.

What does it do?

Oracle uses a wide variety of tools to monitor the Cloud Service environment at every layer of the Oracle technical stack. Monitoring collects, compiles, and provides information about the operational state, performance, and configuration of the Oracle applications running in the environment.

The Monitoring utility scans the Argus Web and Argus Transaction servers, using a large number of metrics:

Metric	Description
Argus Windows Services	Checks if the Argus Windows Services are running without errors.
ETL Argus Insight	Monitors the ETL status during Insight Initial and Incremental ETL run.
Argus Interchange DTD URL	Monitors if the FDA, EMA and Korean DTD URLs are accessible from the Argus Safety transaction server.
DB Links Argus Safety PDB	Checks if Argus Safety DBLinks are valid at runtime.
DB Links Safety Data Mart PDB	Checks if Argus Mart DBLinks are valid at runtime.
DB Jobs Argus Safety PDB	Checks if Argus DB Jobs are able to connect to the database.
DB Jobs Safety Data Mart PDB	Checks if Argus Mart DB Jobs are able to connect to the database.
Argus LDAP Health Check	Verifies the Argus Bind User connectivity with LDAP.
Argus NFS File Age Check	Monitors the file age in network file shares which Argus Safety is using for Case Intake, Literature Intake and E2B Intake.
Argus NFS or SMB Folder Access Check	Checks if Argus M-Tier and Argus Web Server are able to connect to respective file share in ZFS.
DB Schema Connectivity Argus Safety	Checks if the DB connection details for Argus Web, AG Service application are valid at runtime.
DB Schema Connectivity Argus Insight	Checks if the DB connection details for Argus Web, AG Service application are valid at runtime.
Argus Report Services	Checks if the child processes launched by AG Service are working without errors.
ETL Argus Mart	Checks if ODI ETL for Argus Mart is in ERROR state.
ETL Argus Analytics	Checks if ODI ETL for Argus Analytics is in ERROR state.

How do I get it?

Oracle implements the Monitoring utility by default, as part of initial setup of your Argus Cloud environment. Oracle also manages the Monitoring utility upgrades, each time a new version is released. If the implementation requires a downtime, Oracle will contact you.

Where can I find more information?

Log in to My Oracle Support and search for the following article: *KB317773*. Locate the Release Notes for Monitoring Framework.

Usage Billing

Use this utility to track your case volume by generating various license usage reports.

What does it do?

The Usage Billing utility adds the case usage counting capability to Oracle Argus Cloud Service, allowing you to track the case volume to support subscription and license compliance.

This utility can generate the following reports:

- **Case Perpetual Report (Whole Month Report)** - counts the total number of new cases created over a specified period rolled down by each calendar month / year.
- **Case Subscription Report** - counts the total number of new cases created over a specified period from the Subscription Start Date rolled down by quarter and pseudo month.
- **User Perpetual Report (Whole Month Report)** - counts the total number of new human users (that is, excluding system users) created in user tables over a specified period rolled down by each calendar month / year for the specified period.
- **User Subscription Report** - counts the total number of new human users (that is, excluding system users) created in user tables over a specified period from the Subscription Start Date rolled down by quarter and pseudo month.

The Usage Billing utility provides support for both Oracle Argus Cloud Service Subscriptions and Argus Perpetual license customers.

How do I get it?

The Usage Billing utility is available for you by default. To obtain usage reports based on your subscription for a specified time interval, you need to create a change request (CR) in Life Sciences Customer Support Portal. After logging the CR, the Oracle team will send you the requested reports.

Where can I find more information?

Log in to My Oracle Support and search for the following article: *KB317773*. Locate the Release Notes for Usage Billing.

Enterprise Export

Use this utility to export data for a specific tenant or Enterprise.

What does it do?

This utility is used by multi-tenant customers to export data for a specific tenant / Enterprise.

How do I get it?

You need to create a change request (CR) in the Life Sciences Customer Support Portal, asking to execute the Enterprise Export utility. After logging the CR, the Oracle team will run the utility in the environment you specify.

You can use the following example when filling out the **Summary** section:

You need to provide the following information in the ticket description:

- The enterprises you need to be exported from Safety. The enterprise short names need to be separated by a comma. Example: ENT1,ENT2,ENT3.

  > **Note**
  >
  > In case no enterprise is provided, the data is extracted for DEFAULT enterprise.

- Do you need to export DLP data?

  > **Note**
  >
  > The default value is set to yes.

After you have provided the above information, Oracle will extract the data based on the given inputs and the following files will be exported:

- non-enterprise dumps:
  - argus_non_enterprise_table_export.dmp
  - interchange_non_enterprise_table.dmp
  - interchange_udt.dmp
  - dlp_non_enterprise_table_export.dmp

    > **Note**
    >
    > The `dlp_non_enterprise_table_export.dmp` dump is provided only if DLP data export is selected.

  - bridge_non_enterprise_table_export.dmp
- Enterprise dumps for each enterprise:
  - ENT1_argus_enterprise_table_export.dmp
  - ENT1_interchange_enterprise_table_export.dmp
  - ENT1_dlp_enterprise_table_export.dmp

    > **Note**
    >
    > A log file is also shared for each dump file: For example if there are six dumps, then six log files are shared.

  - bridge_enterprise_table_export.dmp

These dump files are password protected. Oracle provides the details regarding from where the files need to be downloaded along with the password in the ticket itself.

Where can I find more information?

Log in to My Oracle Support and search for the following article: *KB317773*. Locate the Release Notes for Enterprise Export.

6

View the Interchange logs

For versions prior to 8.4.1, log files were created for different Interchange activities on multiple machines where Interchange services were installed.

Starting with version 8.4.1 and above, Interchange logs are not available in physical files form, instead they are part of the `INTERCHANGE_ACTIVITY_LOGS` table from the `ESM_OWNER` schema. You can access this table by using a Read Only user to get the Interchange logging details.

Data in the `INTERCHANGE_ACTIVITY_LOGS` table are retained for 30 days from the date of creation. After that, data are purged.

7

Manage integrations

As Argus Cloud administrator, you can set up the connection with external severs and applications that you need.

- Use the federated identity Single-Sign On (SSO)
  With Oracle Argus Cloud Service, you can enable the Federated Identity Single Sign-On (SSO) through Security Assertion Markup Language (SAML).
- Manage sFTP user access
  Find out how you can add, remove sFTP user access and reset sFTP user passwords.
- Configure SMTP
  The Oracle Argus Cloud Service uses the SMTP configuration utility for e-mail transmission if it has been enabled and configured in the application.
- Configuring Argus Bridge for document management
- Configuring Translation Service
- Narrative Generation using OCI Gen AI
- Identity Cloud Service (IDCS)
  Oracle Identity Cloud Service (IDCS) is Oracle's next generation platform for security and identity management.

Use the federated identity Single-Sign On (SSO)

With Oracle Argus Cloud Service, you can enable the Federated Identity Single Sign-On (SSO) through Security Assertion Markup Language (SAML).

Oracle Argus Cloud Service does not support SAML integration directly. The Oracle Life Sciences Identity and Access Management Service, which acts as Service Provider, supports the SAML integration. Once the federated identity SSO is implemented, the user created by the Customer-Delegated Administrator in Oracle Identity Manager will not store the password, since Oracle SSO will not authenticate the user.

The following Argus applications support federated login:

- Oracle Argus Safety
- Oracle Argus Insight
- Oracle Analytics Server (OAS) and Oracle Analytics Publisher Reporting
- Axway B2Bi
- Oracle Identity Manager.

For more information, see:

- Enable Federated Identity SSO through SAML 2.0
  Oracle Cloud supports any SAML 2.0–compliant identity provider.

Enable Federated Identity SSO through SAML 2.0

Oracle Cloud supports any SAML 2.0–compliant identity provider.

To enable Federated Identity SSO:

1. Read thoroughly the *2691858.1* article from My Oracle Support.

   This article includes complete information about the requirements and the various steps involved.
2. Make sure that the user names are identical across Oracle Argus Safety, Oracle Identity Manager Console and your local environment (IdP).
3. Log a change request (CR) ticket in the LSGBU Customer Support Portal, asking to instantiate the process of enabling identity federation.
4. The Oracle team updates the Service Provider Configuration to make the SP Metadata XML available for download.
5. Create an Identity Provider Configuration using the SP Metadata XML provided by Oracle with your IdP Solution.
6. Update the Change Request ticket with IdP Metadata XML URL (or the XML itself) and confirm that the IdP configuration is complete.
7. The Oracle team enables the Identity Federation for an environment.
8. Check that the federated URLs are working correctly.
9. The Oracle team disables the IDCS user notifications in SP.
10. The Oracle team closes the Change Request ticket.

The identity federation has been implemented successfully.

Manage sFTP user access

Find out how you can add, remove sFTP user access and reset sFTP user passwords.

- Add an sFTP user
  To upload an SFTP user, you need to create a change request ticket in Life Sciences Customer Support Portal.
- Renew the sFTP account certificate
  To renew the sFTP account certificate, you need to create a change request ticket in Life Sciences Customer Support Portal.
- Remove an sFTP user account
  To remove an SFTP user account, you need to create a change request ticket in Life Sciences Customer Support Portal.

Add an sFTP user

To upload an SFTP user, you need to create a change request ticket in Life Sciences Customer Support Portal.

1. Log in to the LSGBU Customer Support Portal.
2. On the upper-side menu, click **Change Requests**.
3. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.

4. On the **SFTP User Access** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.

5. From the **Category** drop-down list, expand **Change - Cloud Infrastructure**, then **Infrastructure Services**, **SFTP**, **User** and select **Add**.
6. From the **Customer** drop-down list, search for your company's name and select it from the list.
7. From the **Product** drop-down list, select **Argus Safety**.
8. From the **Business Service** drop-down list, select the name of the server where you want this change.
9. From the **Action** drop-down list, select **Other**.
10. From the **Oracle Internal** radio buttons, select **No**.
11. From the **Environment** drop-down list, select the environment where you want to create the sFTP user, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.
12. In the **Summary** field, enter a short description of your request.

    Example: `Create sFTP user <user name> in <environment>`.
13. In the **Description** field, enter a detailed description of your request.
14. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. In the **sFTP path** field, enter the relevant sFTP path.
16. Select appropriate values from the **Severity** and **Implementation Window** drop-down lists.
17. In the **Date Required By** field, select a value from the calendar.
18. To load the public key for the user you want to create, under **Attach Documents**, click **Choose Files**, and then navigate to the key file.

> **Note**
>
> For information on how to generate a public key for certificate-based sFTP user authentication, navigate to My Oracle Support, at https://support.oracle.com/, and search for Doc ID 2467980.1. To access this article, you must be logged in to My Oracle Support.

19. Click **Submit**.

> **Note**
>
> It is mandatory for Argus Safety Cloud users to use the certificate-based authentication process.

Renew the sFTP account certificate

To renew the sFTP account certificate, you need to create a change request ticket in Life Sciences Customer Support Portal.

1. Log in to the LSGBU Customer Support Portal.
2. On the upper-side menu, click **Change Requests**.
3. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
4. On the **SFTP User Access** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.
5. From the **Category** drop-down list, expand **Change - Cloud Infrastructure**, then **Infrastructure Services**, **SFTP**, **User** and select **Change**.
6. From the **Customer** drop-down list, search for your company's name and select it from the list.
7. From the **Product** drop-down list, select **Argus Safety**.
8. From the **Business Service** drop-down list, select the name of the server where you want this change.
9. From the **Action** drop-down list, select **Other**.
10. From the **Oracle Internal** radio buttons, select **No**.
11. From the **Environment** drop-down list, select the environment where you want to reset the sFTP user password, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.
12. In the **Summary** field, enter a short description of your request.

    Example: `Renew the sFTP account certificate for <user name> in <environment>.`
13. In the **Description** field, enter a detailed description of your request.
14. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. In the **sFTP path** field, enter the relevant sFTP path.
16. Select appropriate values from the **Severity** and **Implementation Window** drop-down lists.
17. In the **Date Required By** field, select a value from the calendar.
18. Click **Submit**.

Remove an sFTP user account

To remove an SFTP user account, you need to create a change request ticket in Life Sciences Customer Support Portal.

1. Log in to the LSGBU Customer Support Portal.
2. On the upper-side menu, click **Change Requests**.
3. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
4. On the **SFTP User Access** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.
5. In the **SFTP User Access** tile, click **Create a Request**.
6. From the **Category** drop-down list, expand **Change - Cloud Infrastructure**, then **Infrastructure Services**, **SFTP**, **User** and select **Remove**.

7. From the **Customer** drop-down list, search for your company's name and select it from the list.
8. From the **Product** drop-down list, select **Argus Safety**.
9. From the **Business Service** drop-down list, select the name of the server where you want this change.
10. From the **Action** drop-down list, select **Other**.
11. From the **Oracle Internal** radio buttons, select **No**.
12. From the **Environment** drop-down list, select the environment where you want to remove the sFTP user, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.
13. In the **Summary** field, enter a short description of your request.

    Example: `Remove sFTP user <user name> from <environment>.`
14. In the **Description** field, enter a detailed description of your request.
15. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
16. In the **sFTP path** field, enter the relevant sFTP path.
17. Select appropriate values from the **Severity** and **Implementation Window** drop-down lists.
18. In the **Date Required By** field, select a value from the calendar.
19. Click **Submit**.

Configure SMTP

The Oracle Argus Cloud Service uses the SMTP configuration utility for e-mail transmission if it has been enabled and configured in the application.

Oracle Argus Safety supports modern authentication and basic authentication. Modern authentication is a method of identity management that offers more secure user authentication and authorization. To use this option, you must register Oracle Argus Safety in Azure AD and obtain required credentials to send emails.

The basic authentication method can be used with Oracle Cloud Infrastructure (OCI) Email Delivery service, which is not part of the Standard Cloud offering and needs to be purchased separately by customers.

When using the basic authentication method with OCI Email Delivery service, you can authenticate by providing your SMTP user name and password. These credentials are used to authenticate your request to send emails through the OCI Email Delivery SMTP endpoint.

To configure SMTP:

1. Navigate to `Argus Console > System Configuration > SMTP` configuration.
2. Check the **Enable SMTP** checkbox.
3. In the Server Configuration section, enter the following parameters:
   - SMTP Server IP address or name
   - Port number (Default value is 25)
   - FQDN (Fully Qualified Domain Name)

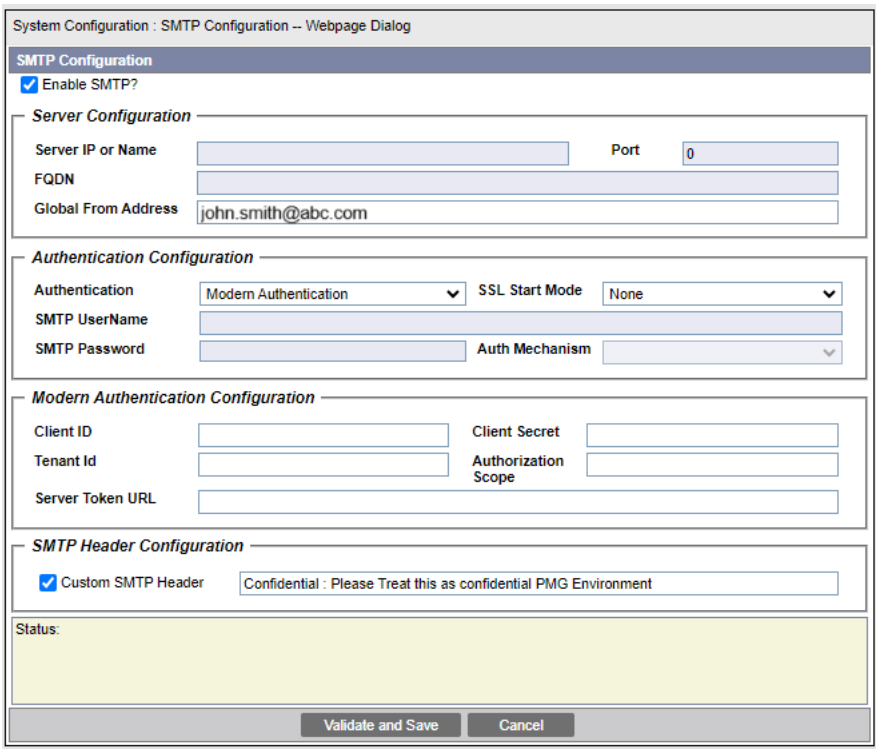
- Valid e-mail address in the Global From Address field.
  When e-mails are sent from Oracle Argus Safety, the From address for all e-mails is set to the e-mail specified in Global From Address.

4. To configure SMTP for modern authentication, skip step 3, and perform the following steps:

> **Note**
>
> Argus application supports modern authentication for only Microsoft Office 365. As a pre-requisite, Argus application needs to be registered in Azure AD to obtain required credentials like Client ID, Client Secret to send emails.

   a. From the **Authentication** drop-down, select **Modern Authentication**.

      The Modern Authentication Configuration section is enabled.



   b. Enter the following parameters:

      - Client ID: Registered Argus application client ID.
      - Client Secret: This field is masked similar to the password field.
      - Tenant ID: Token ID provided while registering.
      - Server Token URL: Server end point which defaulted by the system.
      - Authorization Scope: Scope of authorization defaulted by the system.

5. To configure SMTP for basic authentication, perform the following steps:

   a. From the **Authentication** drop-down, select **Basic Authentication**. Modern Authentication Configuration section fields are now disabled.

   b. Enter the following parameters:

- SSL Start Mode: Select Automatic.
- SMTP UserName : Enter OCI email service userid
- SMTP Password: Enter OCI email service password
- Auth Mechanism: Select SASL Plain.

6. To mark sent emails as confidential, select the **Custom SMTP Header** checkbox.

   All e-mail messages sent using the following processes are sent as Confidential:

   - AG Service: Bulk Transmit Email
   - AG Service: General Email
   - ESM Service: Business / User / IT Email

   The Audit Log tracks updates to this field.

7. Click **Validate and Save**, to connect to the e-mail server as per the configuration data, in modern authentication mode or in basic authentication mode, if set as mentioned in step 3. If the connection is successful, then the configuration data is saved and a test e-mail is sent. If the connection is not successful, the error is displayed in the Status field and the configuration is not saved.

All e-mail messages sent using the following processes are sent as Confidential:

- AG Service: Bulk Transmit Email
- AG Service: General Email
- ESM Service: Business / User / IT Email.

The Audit Log tracks updates to this field.

> **Note**
>
> If Oracle Argus Safety needs to use the proxy set up for SMTP configuration, ensure that the Proxy setting is configured under `System Configuration > System Management > Network Settings > Proxy`.

Configuring Argus Bridge for document management

The Document Management configuration option is hidden for cloud users, as it is managed by Oracle and you are not supposed to make any changes to this configuration. Any changes made may impact document storage.

Configuring Translation Service

Argus case processing user or medical reviewer can translate the narratives, company/sender comments, and other multilingual fields by calling the translation service through the translation adapter. This translation adapter can be integrated with Argus using configuration in Console. The configured translation adapter, auto-translates the text entered in the system to the target language instead of the manual process of translation outside Argus and then manually copying the translated text in to Argus.

> **Note**
>
> This menu is visible only if you belong to groups with access set to Enabled on the Webservice screen in `Console > Access Management > Argus > Groups > Menus > Webservice`.

About the Oracle Translate Service

Oracle Argus Safety provides out-of-the-box support for integration with the Oracle Translate Service via OCI Translation Adapter. This tool allows users to translate text seamlessly within the application's multilingual dialog boxes. It transforms input parameters from Argus into a format compatible with the translation service and reformats the output for usability within Argus. For more details, Log in to My Oracle Support and search for the following article: *3041636.1*.

To enable the translation service:

1. **Raise Change Request (CR) for Adapter configuration:** If you want to use Oracle Translate which is available out-of-the-box then raise a Change Request with the Oracle AMS team from Oracle Life Sciences Support Cloud.
2. **Enable the translation service:** Go to Console > System Configuration > Webservice > Bridge Configuration. In the Service Assembly section, select Translation in the Service drop down. In the Service Settings section, check the Enable Translation Service checkbox.

   > **Note**
   >
   > By default, this checkbox is unchecked.

3. **Update the Language code list** (Optional)
   Click **Save**.

   The translation codes being used by the translation service configured in the translation adapter can be viewed or updated from the `Console > Code Lists > Flexible Data Re-categorization > Code List Name > Languages`. These translation codes appear under Trans_Lang_Code field.

   > **Note**
   >
   > Translation codes used by Oracle Translate are already part of factory data. If a new language is supported by Oracle Translate then the Trans_Lang_code field must be updated with the corresponding language code.
   > For details on supported languages, refer to the Oracle Cloud Infrastructure Documentation > Oracle Translate.

To disable the translation service:

1. Go to `Console > System Configuration > Webservice > Bridge Configuration`.
2. In the **Service** drop down, select **Translation**.
3. In the Service Settings section, deselect the **Enable Translation Service** checkbox.

> **Note**
>
> This procedure disables the translation service only for the specific enterprise. To disable the translation service for multiple enterprises, you must repeat the procedure for each enterprise respectively.

Narrative Generation using OCI Gen AI

Oracle Safety One Argus enhances the case narrative generation process by integrating with Oracle Cloud Infrastructure (OCI) Generative AI service. This update makes the narrative creation process more efficient by generating more accurate and complete information with minimal manual intervention.

The previous template-based approach required managing multiple complex templates and often needed significant rework. Now, you can generate narratives using Gen AI, compare the output with the existing narrative, and choose to use it as-is or edit it as needed.

To use this feature, you need to enable it in the Argus Console under System Settings. The generated narrative can be easily reviewed, and you have full control over the final content, ensuring faster and more efficient narrative generation.

> **Note**
>
> The narrative generated by Gen AI is intended for evaluation purposes only. Review the output thoroughly before use.

For more information, see:

- System Configuration
- Analysis tab
- Feedback

System Configuration

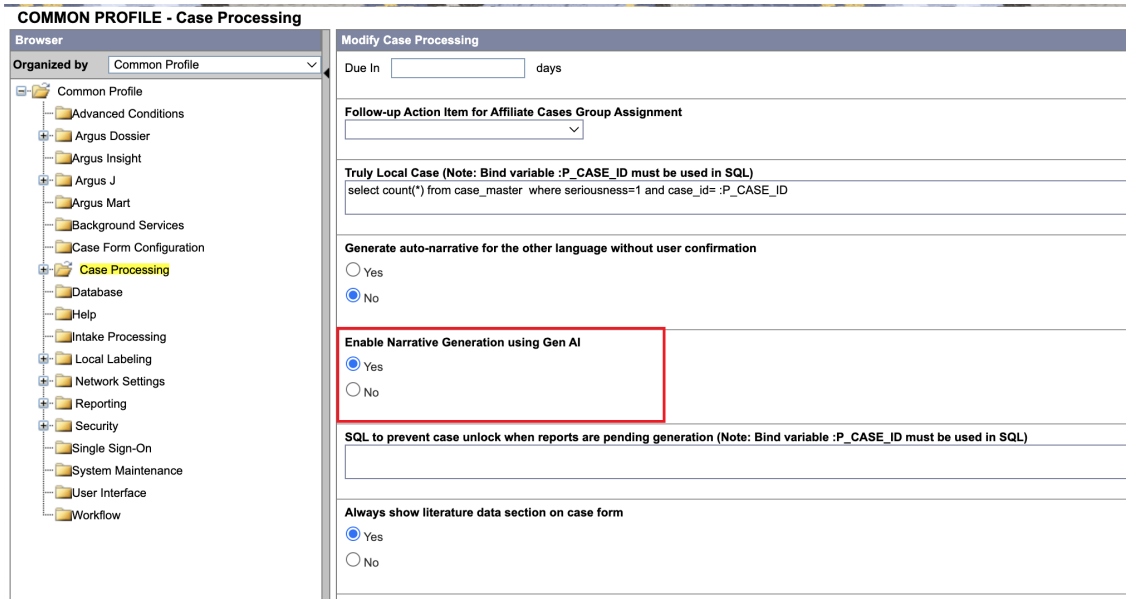
Configuration

Create a change request (CR) in the Life Sciences Customer Support Portal to request configuration for the OCI Gen AI service for narrative generation.

Enable Feature

Once the configuration is done by Oracle AMS, to enable the Narrative Generation feature in the Argus Console:

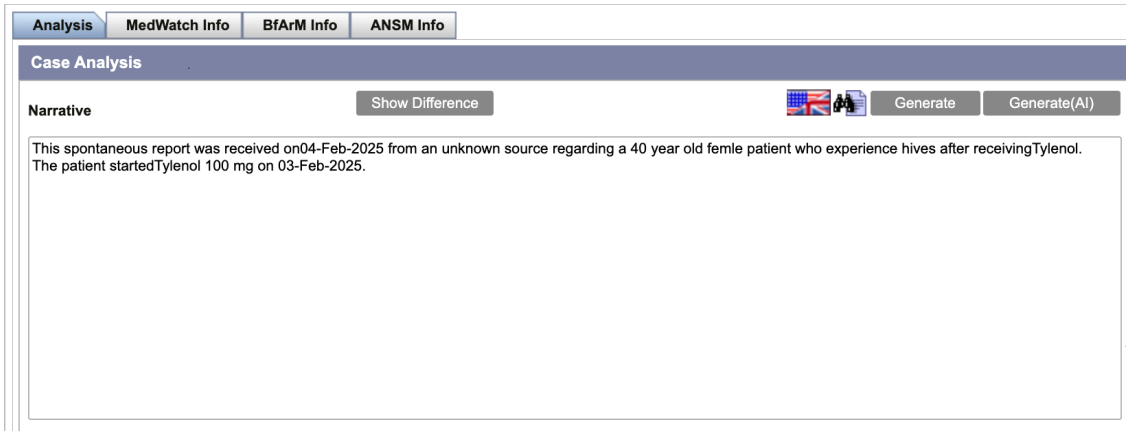
1. Navigate to **System Configuration** > **System Management** > **Case Processing**.
2. Use the Enable Narrative Generation using Gen AI global switch to turn the feature on or off. The default setting is set to No.



> **Note**
>
> When disabled, the option to generate narratives using Gen AI will not appear in the case form.

Analysis tab

The Analysis tab includes the option to generate narrative text using Generative AI. This feature is available if the **Enable Narrative Generation using Gen AI** switch is set to **Yes** in Argus Console (**System Configuration** > **System Management** > **Case Processing**).



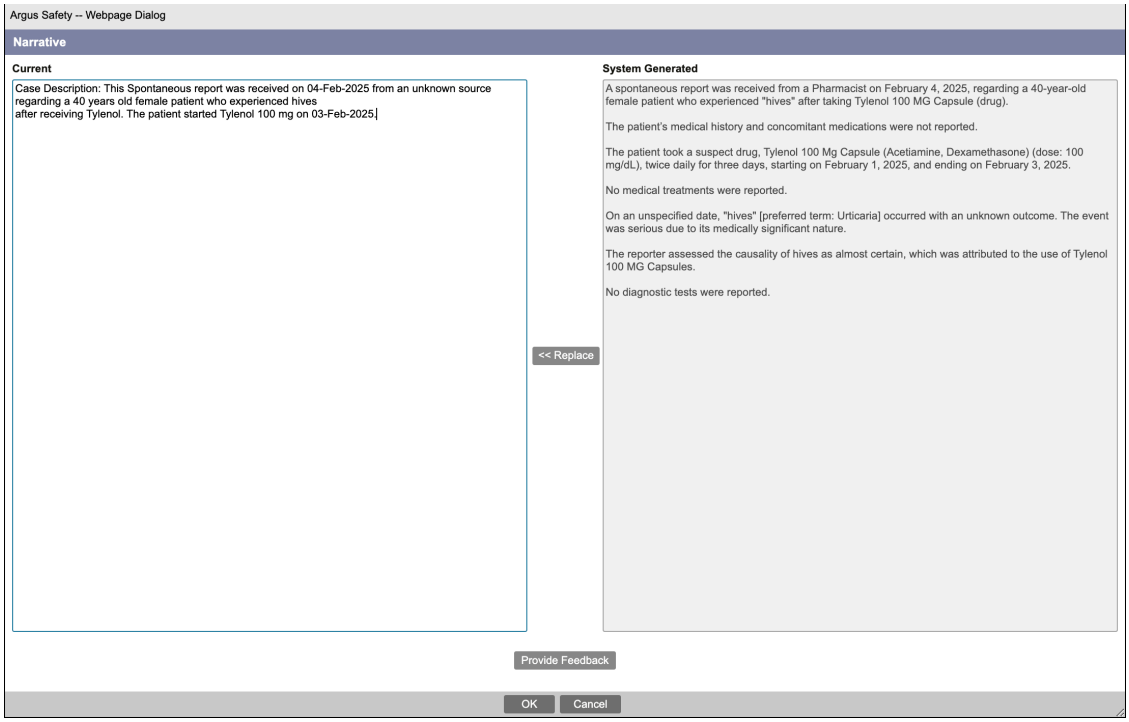
When you click **Generate (AI)**, a new dialog opens, displaying:

- Existing Narrative - This is an editable field, shown on the left.
- System-Generated Narrative - This is a read-only field, shown on the right.

You can perform the following actions within the dialog box:

- Click **Replace** to substitute the entire existing narrative with the system-generated text.

- Manually copy specific sections of the system-generated text and paste them into the existing narrative.
- Edit the existing narrative directly in the left text box.
- Generate system-generated text, even if the existing narrative is empty.
- Click **OK** to save the updated narrative. The dialog box closes, and the updated text appears in the Narrative field on the Analysis tab.
- Click **Cancel** to discard any modifications.



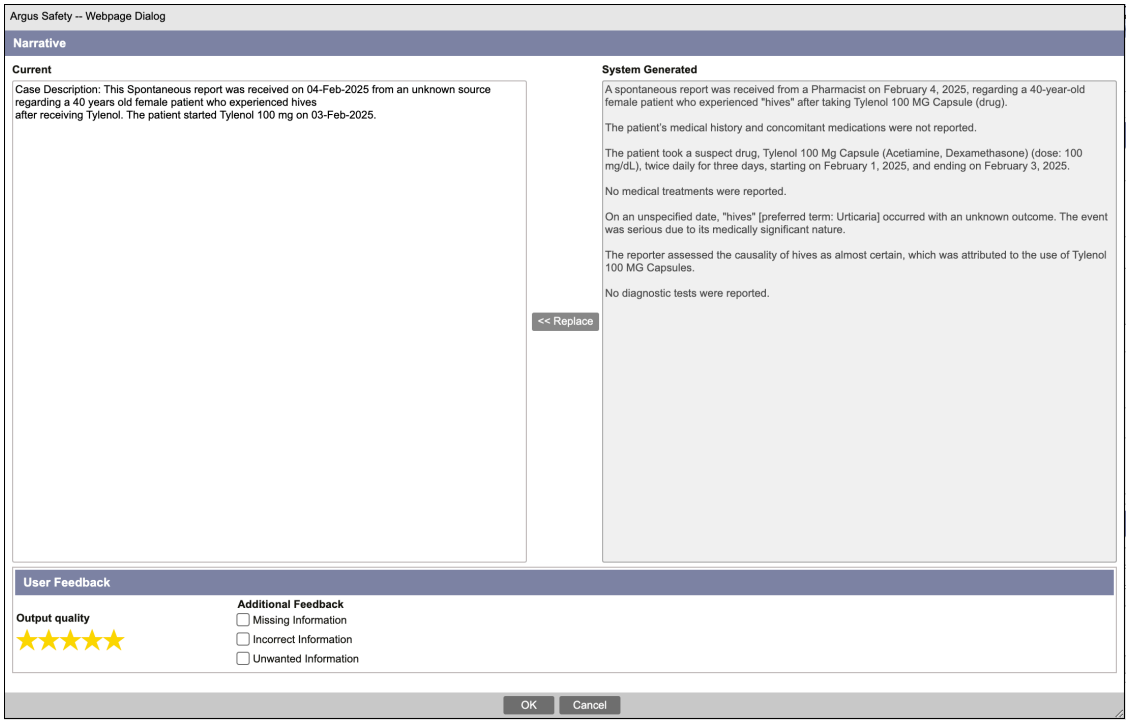
Feedback

You can provide feedback for the AI-generated narrative by clicking the **Provide Feedback** button in the dialog box. You can rate the output quality on a scale of 1 to 5 stars, where 1 is the lowest and 5 is the highest.

You can also provide additional feedback by selecting the appropriate check boxes:

- Missing Information - The output lacks required details.
- Incorrect Information - The output contains errors, such as incorrect dates or details.
- Unwanted Information - The output includes irrelevant details.

To save your feedback, click **OK**; click **Cancel** to discard it. Feedback can be submitted each time new output is generated using the **Generate (AI)** button.



Identity Cloud Service (IDCS)

Oracle Identity Cloud Service (IDCS) is Oracle's next generation platform for security and identity management.

In this chapter:

- IDCS Reports
  Use this utility to generate out-of-the-box (OOB) reports provided by the Oracle Identity Cloud Service (IDCS).
- Federation Setup in IDCS
  Use this utility to track your case volume by generating various license usage reports.
- Mixed mode authentication support in IDCS
  User authentication can be done through IDCS or Federated log in.
- Password policy management in IDCS
  Learn how to manage password policies for Oracle Identity Cloud Service.
- Notifications in IDCS
  Learn about the various user and administrator notifications available in Oracle Identity Cloud Service.
- Password expiry notification in IDCS
- Muti-factor authentication in IDCS
  You can add multiple layers of security to the Oracle Cloud sign in process by configuring Multi-Factor Authentication (MFA).

IDCS Reports

Use this utility to generate out-of-the-box (OOB) reports provided by the Oracle Identity Cloud Service (IDCS).

What does it do?

The Identity Domain in IDCS provides different flavors of the out-of-the-box reports.

- **Audit Log**: Capture system activity such as successful and failed logins, user creation, update and deletion, and much more.
- **Notification Delivery Status:** View the email notification delivery status for events such as new users, self-initiated password changes, and much more.
- **Successful Login Attempts:** View users who have logged in to the Oracle Identity Cloud Service successfully.
- **Unsuccessful Login Attempts:** View users who were unable to log in to the Oracle Identity Cloud Service.
- **Dormant Users:** View users who have not logged into Oracle Identity Cloud Service since a specified date.
- **Application Access Report:** View how many times users logged in to both the Oracle Identity Cloud Service, and Oracle applications or custom applications in your identity domain.
- **Application Role Privileges Reports:** View application role grants and revocations for users and groups for applications that are configured in the Oracle Identity Cloud Service.
- **Diagnostic Data:** View logging data captured in the Oracle Identity Cloud Service.

How do I get it?

To run the Identity Domain reports, you must have either of the following roles:

- Identity domain administrator
- Audit administrator
- Application administrator

Where can I find more information?

For more information, refer to the Oracle Cloud Administering Oracle Identity Cloud Service Guide > Run Oracle Identity Cloud Service Reports chapter.

Federation Setup in IDCS

Use this utility to track your case volume by generating various license usage reports.

What does it do?

An identity provider, also known as an Authentication Authority provides external authentication to the users who want to sign into the Identity Cloud Service using their external provider's credentials.

By setting up a Federation between the customer Identity Systems and Oracle Identity Cloud Service, Oracle enables user access to the applications in Oracle Identity Cloud Service using their credentials, authenticated by the customer Identity Systems.

IDCS supports SAML 2.0 based federation with most of the Identity Systems like Azure, OKTA, and others.

How do I get it?

With IDCS, CDA must configure the Federation between IDCS and customer Identity System.

Federation setup consists of the following activities:

Set up or enable the Federation

Log in to My Oracle Support.

- To set up the Federation between IDCS as the service provider and Azure AD as the identity provider, search for the article 2795951.1.
- To set up the Federation between IDCS as the service provider and OKTA as the identity provider, search for the article 2463197.1.

Set up the user and group sync

Log in to My Oracle Support.

- To provision the users and groups from Azure AD to IDCS, search for the article 2796340.1.
- To provision the users and groups from OKTA to IDCS, refer to the Oracle Cloud Infrastructure Documentation > User Provisioning for Federated Users.

Mixed mode authentication support in IDCS

User authentication can be done through IDCS or Federated log in.

What does it do?

With IDCS integrated Oracle Argus Cloud Service, end-users can authenticate through IDCS or from the Federated log in.

How do I get it?

Federated users must be marked as Federated in IDCS, so that, the user cannot log in though IDCS.

Password policy management in IDCS

Learn how to manage password policies for Oracle Identity Cloud Service.

What does it do?

You can set up policies in the Oracle Identity Cloud Service for an identity domain. You then attach a policy to a group that is applicable to all the users in that group.

Where can I find more information?

For more information, refer to the Administering Oracle Identity Cloud Service guide > Manage Oracle Identity Cloud Service Password Policies chapter.

> **Note**
>
> - You can create at max ten password policies in the Oracle Identity Cloud Service. Each policy is assigned a priority. The password policy is assigned to a group, and all users in that group can use that policy. When a user is a member of more than one group, the password policy with the highest priority applies.
> - With IDCS integrated Argus, customer must manage the password policy.

Notifications in IDCS

Learn about the various user and administrator notifications available in Oracle Identity Cloud Service.

What does it do?

You can customize the email notifications in the Oracle Identity Cloud Service for users and administrators.

Where can I find more information?

For more information on the user notifications, refer to the Administering Oracle Identity Cloud Service guide > About User Notifications section.

For more information on the administrator notifications, refer to the Administering Oracle Identity Cloud Service guide > About Administrator Notifications section.

To customize the notifications, refer to the Administering Oracle Identity Cloud Service guide > Understand How to Customize Notifications section.

Password expiry notification in IDCS

In IDCS, there is no configuration available to notify an end user when their password is about to expire. The user is prompted to change their password as per the password policies. This is done via the user interface.

Muti-factor authentication in IDCS

You can add multiple layers of security to the Oracle Cloud sign in process by configuring Multi-Factor Authentication (MFA).

What does it do?

IDCS offers you one more layer of security to the Oracle Cloud sign in process by configuring Multi-Factor Authentication (MFA) to the customers who have recently signed up for the Oracle Cloud Service or those who have migrated to a new Oracle Cloud account.

The MFA feature in Oracle Identity Cloud Service enables you to add an extra security step to the authentication process.

Where can I find more information?

For more information, refer to the Administering Oracle Identity Cloud Service guide > Enable Multi-Factor Authentication Security for Oracle Cloud chapter.

8

Gateway administration

Oracle Argus Cloud Service customers use either Axway B2Bi or Oracle B2B for secure and reliable exchange of E2B files with trading partners/regulatory authorities. You can find here more information about the Argus Cloud gateway administration tasks.

- Implement gateway UI access in your Argus Cloud environment
  As Oracle Argus Cloud Service administrator, you can configure users access to Axway B2BI / Oracle B2B.
- Request creating a trading partner or community from the Life Sciences Customer Support Portal
  If you don't have write access to Axway B2Bi interface and you want to create a trading partner or community, you must log a change request ticket to the Life Sciences Customer Support Portal.
- Configure Axway B2Bi to transmit reports
  You can choose whether you want to access the Axway gateway self-service and configure trading partners and communities by yourself, or ask the Oracle team to make these settings for you.

Implement gateway UI access in your Argus Cloud environment

As Oracle Argus Cloud Service administrator, you can configure users access to Axway B2BI / Oracle B2B.

- Request gateway UI access
  If you don't have privileges to assign Axway UI / Oracle B2B access to users, you need to create a change request ticket in Life Sciences Customer Support Portal.
- Grant users with Axway UI access
  To grant Oracle Argus Cloud Service users with Axway UI access, you need to associate their user accounts with Axway B2Bi specific roles in IDCS.
- Grant users with Oracle B2B UI access
  To grant Oracle Argus Cloud Service users with Oracle B2B access, you need to associate their user accounts with specific roles in IDCS.

Request gateway UI access

If you don't have privileges to assign Axway UI / Oracle B2B access to users, you need to create a change request ticket in Life Sciences Customer Support Portal.

1. Log in to the LSGBU Customer Support Portal.
2. On the upper-side menu, click **Change Requests**.
3. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
4. On the **Application Install/Change/Re-setup/Uninstall** tile, click **Create a Request**.
5. From the **Category** drop-down, expand **Change - Cloud Environment, Application, Integration** then select **Setup**.

6. From the **Customer** drop-down, search for your company's name and select it from the list.
7. From the **Product** drop-down, select **Argus Safety**.
8. From the **Business Service** drop-down, select the name of the server where you want this change.
9. From the **Action** drop-down, select **Other**.
10. From the **Oracle Internal** radio buttons, select **No**.
11. From the **Environment** drop-down, select the environment where you want this change to be performed, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.
12. In the **Summary** field, enter a short description of your request.

    Example: `Implement Axway UI / Oracle B2B access in <environment>.`

    > **Note**
    >
    > Once the request is implemented, a CDA user can grant appropriate roles to other users.

13. In the **Description** field, enter more details for your request.
14. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. If you use an sFTP location to exchange files with the Oracle team, enter its address in the **sFTP path** field.

    If you don't use sFTP and prefer to attach the documents directly to this change request, select **Tick if sFTP path is not applicable for this request**.
16. Select the appropriate values from the **Severity** and **Implementation Window** drop-downs.
17. Click the **Date Required By** field and select a value from the calendar.
18. Click **Submit**.

Grant users with Axway UI access

To grant Oracle Argus Cloud Service users with Axway UI access, you need to associate their user accounts with Axway B2Bi specific roles in IDCS.

Oracle Argus Cloud Service users can access the Axway gateway self-service interface based on their user role.

Once you have identified the specific Axway B2Bi access type for each Argus user, you need to Assign groups to user accounts in IDCS.

> **Note**
>
> If you don't have privileges to assign Axway UI access to users, you need to create a change request ticket in LSGBU Customer Support Portal.

There are two types of Axway UI users, based on their access rights: monitor users and configuration users.

User role	Access type	OIM role	Description
Monitor	Read-only	ls-oasafety-*dev/val/prod*-b2bi-configure-group	Monitor the communication between a customer and their partner: • Search for messages processed by the trading engine • Add notes to messages • Manage document types • Manage global message search settings • Monitor any Axway failed message transmission • Resubmit messages • Save, change, and delete searches • View payloads and backups • View Trading Partners configuration
Configuration	Configuration	ls-oasafety-*dev/val/prod*-b2bi-monitor-group	In addition to the monitor role access, this role allows to: • Manage Trading Partners configuration, including the option to deploy the partner certificate • Manage agreements • View the pick-up groups

Grant users with Oracle B2B UI access

To grant Oracle Argus Cloud Service users with Oracle B2B access, you need to associate their user accounts with specific roles in IDCS.

Argus Cloud Service users can access the Oracle B2B gateway self-service interface based on their user role.

Once you have identified the specific Oracle B2B access type for each Argus user, you need to Assign groups to user accounts in IDCS.

> **Note**
>
> If you don't have privileges to assign Oracle B2B access to users, you need to create a change request ticket in LSGBU Customer Support Portal.

There are two types of Oracle B2B users, based on their access rights: monitor users and configuration users.

User role	Access type	IDCS Role	Description
Monitor	Read-only	ls-oasafety-*dev/val/prod*-soa-configure-group	Monitor the communication between a customer and their partner: • Search for messages • View messages • Monitor messages, also B2B failed message transmissions • Download messages

User role	Access type	IDCS Role	Description
Configuration	Configuration	ls-oasafety-*dev/val/prod*-soa-monitor-group	In addition to the monitor role access, this role allows to: • Manage Trading Partner (create, update and delete), including the option to deploy the trading partner certificates • Monitor and download messages • Resubmit messages

Request creating a trading partner or community from the Life Sciences Customer Support Portal

If you don't have write access to Axway B2Bi interface and you want to create a trading partner or community, you must log a change request ticket to the Life Sciences Customer Support Portal.

> **Note**
>
> You need to create one change request ticket for adding a trading partner, and another one for adding a community.

1. Log in to the LSGBU Customer Support Portal.
2. On the upper-side menu, click **Change Requests**.
3. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
4. On the **Application Install/Change/Re-setup/Uninstall** tile, click **Create a Request**.
5. From the **Category** drop-down, expand **Change - Cloud Environment, Application, Integration** then select **Setup**.
6. From the **Customer** drop-down, search for your company's name and select it from the list.
7. From the **Product** drop-down, select **Argus Safety**.
8. From the **Business Service** drop-down, select the name of the server where you want this change.
9. From the **Action** drop-down, select **Other**.
10. From the **Oracle Internal** radio buttons, select **No**.
11. From the **Environment** drop-down, select the environment where you want this change to be performed, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.
12. In the **Summary** field, enter a short description of your request.

    Example: `Create an Axway trading partner.`
13. In the **Description** field, enter more details for your request.
14. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. If you use an sFTP location to exchange files with the Oracle team, enter its address in the **sFTP path** field.

If you don't use sFTP and prefer to attach the documents directly to this change request, select **Tick if sFTP path is not applicable for this request**.

16. Select the appropriate values from the **Severity** and **Implementation Window** drop-downs.
17. Click the **Date Required By** field and select a value from the calendar.
18. Download the form template suited for your request (community form template or partner form template).
    a. Click the **Download Documents and Request Forms** link.

       The **Document & Request Forms** page appears.
    b. On the left-side menu, click **Request Forms**.

       A table with a list of form documents appears.
    c. Click the request template that you need (for AxwayB2Bi partner or community setup) to download it.
    d. Fill in the downloaded XLS file with the community/partner information. The file includes instructions on how to provide the required details.
19. Click **Choose file** to attach the XLS file that you have downloaded and filled-in.
20. Click **Submit**.

Configure Axway B2Bi to transmit reports

You can choose whether you want to access the Axway gateway self-service and configure trading partners and communities by yourself, or ask the Oracle team to make these settings for you.

> **Note**
>
> If you do not have access to the Axway B2Bi interface, skip this procedure, and go to Request creating a trading partner or community from the LSGBU Customer Support Portal.

- Before you begin configuring Axway B2Bi
  Regulatory reports are submitted to the Reporting Destination. Before you begin configuring the Axway B2Bi settings, make sure you have set up your reporting destination in Argus.
- Create a community
  Follow these steps to create a community in Axway B2Bi.
- Add a partner to a community
  Follow these steps to add a partner to a community in Axway B2Bi.
- Create application pickups
  An application pickup is an Axway B2Bi object that specifies the way the product consumes messages and files from back-end applications. You can configure multiple application pickups within a community.
- Specialize collaboration settings
  Collaboration settings specify how Axway B2Bi packages the messages that a community sends to its partners.

- Set up application delivery
  An application delivery is a B2Bi object that specifies the way B2Bi sends files to applications. You set up application deliveries within a community. You can have multiple application deliveries.
- Update the incoming rule for Delivery Settings for each Partner
  Define conditions that will cause payloads to be delivered to the appropriate exchange. If a payload does not satisfy the delivery criteria for any exchange, then the first available exchange will be used. An exchange with no criteria will be used only if it is the first available exchange.
- Add a trading pickup to a community
  Trading pickups are located in community objects. A trading pickup specifies how you want the community to pick up or receive documents over the Internet from a remote partner.
- Add public URL configuration in trading pickup (Pharma Company URL)
  Use this procedure to configure the URL that your partners use to connect to the HTTPS server to exchange messages.
- Add partner encryption certificate
  Use this procedure to import a trading partner's certificate and associate it with a partner object in your configuration.
- Add partner SSL certificate
  Axway B2Bi provides options for allowing certificates to be used for authenticating the identity of trading partners. Secure Sockets Layer (SSL) protocol authentication provides an added layer of security to trading relationships.
- Add public URL configuration in trading pickup
  Use this procedure to add public URL configuration for all the agencies, once for each community or partner.
- Post-configuration step: Transmit the generated report
  After you have configured the required settings in both Argus and Axway B2Bi environments, you can transmit your report to the reporting destination via the Axway gateway.
- Typical workflow for transmitting regulatory reports to agencies/partners
  Transmitting a report to an agency or a partner requires a series of configurations in both Argus and Axway B2Bi environments.

Before you begin configuring Axway B2Bi

Regulatory reports are submitted to the Reporting Destination. Before you begin configuring the Axway B2Bi settings, make sure you have set up your reporting destination in Argus.

Use the following procedure to configure reporting destination in your Argus environment:

1. In Argus, select **Code Lists**, then **Argus** to view the Code List Maintenance screen.
2. Click **Reporting Destination** on the left pane of the Code List screen.

   The reporting destination settings appear in the main window.
3. Configure the settings available in the **Agency Information**, **Local Company Contact** and **SMTP** tabs.

   For more details, refer to the Oracle Argus Safety Administration Guide chapter 6 Code List Configuration, Configuring Reporting Destination.
   For more information, see:

- Request adding a trading engine node
  Before starting to create communities and trading partners, you need to have a trading engine (TE) node implemented in your Axway B2Bi environment.

Request adding a trading engine node

Before starting to create communities and trading partners, you need to have a trading engine (TE) node implemented in your Axway B2Bi environment.

A TE node is an instance of a Java virtual machine that performs the work of the application. The Oracle team implements the TE node in your Axway B2Bi environment by your request.

> **Note**
>
> You need to request a TE node only once, before creating the first community.

Follow the next steps to create a change request ticket for adding a TE node.

1. Log in to the LSGBU Customer Support Portal.
2. On the upper-side menu, click **Change Requests**.
3. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
4. On the **Application Install/Change/Re-setup/Uninstall** tile, click **Create a Request**.
5. From the **Category** drop-down, expand **Change - Cloud Environment, Application, Integration** then select **Setup**.
6. From the **Customer** drop-down, search for your company's name and select it from the list.
7. From the **Product** drop-down, select **Argus Safety**.
8. From the **Business Service** drop-down, select the name of the server where you want this change.
9. From the **Action** drop-down, select **Other**.
10. From the **Oracle Internal** radio buttons, select **No**.
11. From the **Environment** drop-down, select the environment where you want this change to be performed, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.
12. In the **Summary** field, enter a short description of your request.

    Example: `Create a trading engine node.`
13. In the **Description** field, enter more details for your request.
14. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
15. If you use an sFTP location to exchange files with the Oracle team, enter its address in the **sFTP path** field.

    If you don't use sFTP and prefer to attach the documents directly to this change request, select **Tick if sFTP path is not applicable for this request**.
16. Select the appropriate values from the **Severity** and **Implementation Window** drop-downs.
17. Click the **Date Required By** field and select a value from the calendar.

18. Click **Submit**.

Create a community

Follow these steps to create a community in Axway B2Bi.

1. From the menu bar, hover over the **Trading configuration** icon, then click **Manage Trading Configuration**.

   The Communities screen opens.

2. Click **Add a community**.

   The Add Community Wizard opens.

3. Select **Manually create a new community**, then click **Next**.

   The Create a community screen is displayed.

4. Fill in the following required fields:
   - Community name: enter a short name that identifies the community.
   - Full name: enter an administrative contact name.
   - E-mail address: enter the e-mail address of the specified contact name.
   - Routing ID: Enter an ID that serves as routing reference.
5. Click **Finish**.

The community is created.

Add a partner to a community

Follow these steps to add a partner to a community in Axway B2Bi.

1. From the Getting Started screen, click the **Home** menu, then click the community name.

   The Summary screen opens.

2. From the menu bar, hover over the **Partners** icon, then select **Add a partner**.

   The Partner Wizard opens.

3. Select **Manually create a new partner**, then click **Next**.

   The Enter partner information screen is displayed.

4. Fill in the following required fields for the partner setup:
   - Partner name: enter a name that identifies the partner.
   - Contact name: enter an administrative contact name for this partner.
   - Email address: enter the e-mail address of the specified contact name.
   - Routing ID: Enter an ID that serves as routing reference.

> **Note**
>
> A partner can have one or more routing IDs. If there are multiple Routing IDs, click the **Trading partner** icon under the menu bar, then click the partner name. After that, perform the next steps for each additional routing ID:
>
> a. Click the **Routing IDs** link.
>
> b. Enter an ID that serves as routing reference in the **Add a routing ID** field, then click **Add**.
>
> c. If you want to define this routing ID as default, select the **Default routing ID** radio button .

5. Select the **Choose the community for this partner** option.
6. Click **Finish**.

The partner is created.

Create application pickups

An application pickup is an Axway B2Bi object that specifies the way the product consumes messages and files from back-end applications. You can configure multiple application pickups within a community.

Add an application pickup when you want to enable Axway B2Bi to consume messages from an application that is located in your back-end system.

- Add an application pickup to a community (all agencies)
  Follow this procedure to add an application pickup for EMEA, FDA (Drugs only), and other agencies.
- Add an application pickup to a community for Drugs (FDA)
  Follow this procedure to add an application pickup to a community for FDA (Drugs) only.
- Add an application pickup to a community for Device Reporting (FDA)
  Follow this procedure to add an application pickup to a community for FDA (Device Reporting) only.
- Add an application pickup to a community for Vaccine (FDA)
  Follow this procedure to add an application pickup for EMEA, FDA (Drugs only), and other agencies.

Add an application pickup to a community (all agencies)

Follow this procedure to add an application pickup for EMEA, FDA (Drugs only), and other agencies.

1. From the Getting Started screen, click the **Home** menu, then click the community name.

   The **Summary** screen opens.
2. From the menu bar, click **Trading configuration**.
3. From the navigation graphic below the menu bar, click **Application pickup**.

   The Application pickup page opens.
4. From the Related tasks list at the bottom of the page, click **Add an application pickup**.

   The Exchange Wizard screen opens.

5. From the **Choose transport protocol** tab, select **Application File System**, then click **Next**.
6. From the **From address** tab, select **Always Parse for the address**, then configure the following settings:
   a. Select the option **If the document is EDI, parse for the address** (only for PMDA).
   b. Select the option **If the document is XML, use XPaths to locate the address**.
   c. Configure the settings for **If the document is XML, use XPaths to locate the address**, by adding the following values in the **From XPath** field:

      For FDA, EMEA and PMDA (R2 only):

      - */ichicsrack/ichicsrmessageheader/messagesenderidentifier*

      For EMEA and PMDA (R3 only):

      - */MCCI_IN200100UV01/PORR_IN049016UV/sender/device/id/@extension*
      - */MCCI_IN200101UV01/MCCI_IN000002UV01/sender/device/id/@extension*

      > **Note**
      >
      > You can add the paths for both R2 and R3, if required.

   d. Click **Next**.
7. From the **To address** tab, select **Always Parse for the address**, then configure the following settings:
   a. Select the option **If the document is EDI, parse for the address** (only for PMDA).
   b. Select the option **If the document is XML, use XPaths to locate the address**.
   c. Configure the settings for **If the document is XML, use XPaths to locate the address**, by adding the following values in the **To XPath** field:

      For FDA, EMEA and PMDA (R2 only):

      - *//ichicsrack/ichicsrmessageheader/messagereceiveridentifier*

      For EMEA and PMDA (R3 only):

      - */MCCI_IN200100UV01/PORR_IN049016UV/receiver/device/id/@extension*
      - */MCCI_IN200101UV01/MCCI_IN000002UV01/receiver/device/id/@extension*

      > **Note**
      >
      > You can add the paths for both R2 and R3, if required.

   d. Click **Next**.
8. From the **Enter file system settings** tab, in the **Directory** field, click **Browse** and select the path to the agency directory on the trading engine server file system, then click **Next**.
9. In the **Exchange name** tab, enter a name for the delivery exchange.
10. Click **Finish**.

    The application pickup is created, and the Change this application pickup screen is displayed.

11. Click the **Inline processing** tab and enter the following information under the Inline processor customization section:
    - **Description**: *GetMessagesInformation*
    - **Class name**: *com.cyclonecommerce.relsys.router.GetMessageInfo*
    - **Parameter**: *Relsys Argus*
12. Click the **Advanced** tab, and, under Message processing section, select **Limited - only use message handler and collaboration settings**.

    > **Note**
    >
    > This option is available in Axway B2Bi 2.3.x version only.

13. Click **Save changes**.

Add an application pickup to a community for Drugs (FDA)

Follow this procedure to add an application pickup to a community for FDA (Drugs) only.

1. From the Getting Started screen, click the **Home** menu, then click the community name.

   The Summary screen opens.
2. From the menu bar, click **Trading configuration**.
3. From the navigation graphic below the menu bar, click **Application pickup**.

   The Application pickup page opens.
4. From the Related tasks list at the bottom of the page, click **Add an application pickup**.

   The Exchange Wizard screen opens.
5. From the **Choose transport protocol** tab, select **Application File System**, then click **Next**.
6. From the **From address** tab, select **Specify the address. Always use a fixed address**, then click the **Choose party** button.

   Select the community name, then click **Next**.
7. From the **To address** tab, select **Specify the address. Always use a fixed address**, then click the **Choose party** button.

   Select the partner name, then click **Next**.
8. From the **Enter file system settings** tab, in the **Directory** field, click **Browse** and select the path to the FDA directory on the trading engine server file system, then click **Next**.
9. In the **Exchange name** tab, enter a name for the FDA delivery exchange.
10. Click **Finish**.

    The application pickup is created, and the Change this application pickup screen is displayed.
11. Click the **Inline processing** tab and enter the following information under the Inline processor customization section:
    - **Description**: *GetMessagesInformation*
    - **Class name**: *com.cyclonecommerce.relsys.router.GetMessageInfo*
    - **Parameter**: *Relsys Argus*

12. Click the **Message attribute** tab, and configure the following:
    a. Under Fixed message attribute section, enter the following values in the **Value** field, then click **Add** after each entry:
        - *FdaCenter*
        - *FdaSubmissionType*
    b. From the **Attribute name** drop-down, select **FDACenter**, enter *CBER* in the **Value** field, then click **Add**.
    c. From the **Attribute name** drop-down, select **FdaSubmissionType**, enter *AERS* in the **Value** field, then click **Add**.
13. Click the **Advanced** tab, and, under Message processing section, select **Limited - only use message handler and collaboration settings**.

> **Note**
>
> This option is available in Axway B2Bi 2.3.x version only.

14. Click **Save changes**.

Add an application pickup to a community for Device Reporting (FDA)

Follow this procedure to add an application pickup to a community for FDA (Device Reporting) only.

1. From the Getting Started screen, click the **Home** menu, then click the community name.

   The Summary screen opens.
2. From the menu bar, click **Trading configuration**.
3. From the navigation graphic below the menu bar, click **Application pickup**.

   The Application pickup page opens.
4. From the Related tasks list at the bottom of the page, click **Add an application pickup**.

   The Exchange Wizard screen opens.
5. From the **Choose transport protocol** tab, select **Application File System**, then click **Next**.
6. From the **From address** tab, select **Specify the address. Always use a fixed address**, then click the **Choose party** button.

   Select the community name, then click **Next**.
7. From the **To address** tab, select **Specify the address. Always use a fixed address**, then click the **Choose party** button.

   Select the partner name, then click **Next**.
8. From the **Enter file system settings** tab, in the **Directory** field, click **Browse** and select the path to the FDA directory on the trading engine server file system, then click **Next**.
9. In the **Exchange name** tab, enter a name for the FDA delivery exchange.
10. Click **Finish**.

    The application pickup is created, and the screen Change this application pickup is displayed.

11. Click the **Inline processing** tab and enter the following information under the Inline processor customization section:
    - **Description**: *GetMessagesInformation*
    - **Class name**: *com.cyclonecommerce.relsys.router.GetMessageInfo*
    - **Parameter**: *Relsys Argus*
12. Click the **Message attribute** tab, and configure the following:
    a. Under Fixed message attribute section, enter the following values in the **Value** field, then click **Add** after each entry:
       - *FdaCenter*
       - *FdaSubmissionType*
    b. From the **Attribute name** drop-down, select **FDACenter**, enter *CDRH* in the **Value** field, then click **Add**.
    c. From the **Attribute name** drop-down, select **FdaSubmissionType**, enter *Adverse_Events* in the **Value** field, then click **Add**.
13. Click the **Advanced** tab, and, under Message processing section, select **Limited - only use message handler and collaboration settings**.

> **Note**
>
> This option is available in Axway B2Bi 2.3.x version only.

14. Click **Save changes**.

Add an application pickup to a community for Vaccine (FDA)

Follow this procedure to add an application pickup for EMEA, FDA (Drugs only), and other agencies.

1. From the Getting Started screen, click the **Home** menu, then click the community name.

   The Summary screen opens.
2. From the menu bar, click **Trading configuration**.
3. From the navigation graphic below the menu bar, click **Application pickup**.

   The Application pickup page opens.
4. From the Related tasks list at the bottom of the page, click **Add an application pickup**.

   The Exchange Wizard screen opens.
5. From the **Choose transport protocol** tab, select **Application File System**, then click **Next**.
6. From the **From address** tab, select **Always Parse for the address**, then configure the following settings:
   a. Select the option **If the document is EDI, parse for the address** (only for PMDA).
   b. Select the option **If the document is XML, use XPaths to locate the address**.
   c. Configure the settings for **If the document is XML, use XPaths to locate the address**, by adding the following values in the **From XPath** field for FDA EVAERS:
      - */MCCI_IN200100UV01/PORR_IN049016UV/sender/device/id/@extension*

- *//MCCI_IN200101UV01/MCCI_IN000002UV01/sender/device/id/@extension*

d. Click **Next**.

7. From the **To address** tab, select **Always Parse for the address**, then configure the following settings:
   a. Select the option **If the document is EDI, parse for the address** (only for PMDA).
   b. Select the option **If the document is XML, use XPaths to locate the address**.
   c. Configure the settings for **If the document is XML, use XPaths to locate the address**, by adding the following values in the **To XPath** field for FDA EVAERS:
      - */MCCI_IN200100UV01/PORR_IN049016UV/receiver/device/id/@extensio n*
      - *//MCCI_IN200101UV01/MCCI_IN000002UV01/receiver/device/id/@extension*
   d. Click **Next**.
8. From the **Enter file system settings** tab, in the **Directory** field, click **Browse** and select the path to the agency directory on the trading engine server file system, then click **Next**.
9. In the **Exchange name** tab, enter a name for the delivery exchange.
10. Click **Finish**.

    The application pickup is created, and the screen Change this application pickup is displayed.
11. Click the **Inline processing** tab and enter the following information under the Inline processor customization section:
    - **Description**: *GetMessagesInformation*
    - **Class name**: *com.cyclonecommerce.relsys.router.GetMessageInfo*
    - **Parameter**: *Relsys Argus*
12. Click the **Message attribute** tab, and configure the following:
    a. Under Fixed message attribute section, enter the following values in the **Value** field, then click **Add** after each entry:
       - *FdaCenter*
       - *FdaSubmissionType*
    b. From the **Attribute name** drop-down, select **FDACenter**, enter *CBER* in the **Value** field, then click **Add**.
    c. From the **Attribute name** drop-down, select **FdaSubmissionType**, enter *VAERS* in the **Value** field, then click **Add**.
13. Click the **Advanced** tab, and, under Message processing section, select **Limited - only use message handler and collaboration settings**.

> **Note**
>
> This option is available in Axway B2Bi 2.3.x version only.

14. Click **Save changes**.

Specialize collaboration settings

Collaboration settings specify how Axway B2Bi packages the messages that a community sends to its partners.

- Specialize collaboration settings for a partner (FDA)
  You can specify collaboration settings that apply between one specific community and one specific partner. This procedure applies to FDA only.
- Specialize collaboration settings for a partner (PMDA)
  You can specify collaboration settings that apply between one specific community and one specific partner. This procedure applies to PMDA only.

Specialize collaboration settings for a partner (FDA)

You can specify collaboration settings that apply between one specific community and one specific partner. This procedure applies to FDA only.

1. From the menu bar, hover over the **Trading configuration** icon, then click **Manage trading configuration**.

   The Communities screen opens.
2. From the list of communities, click the name of the community that you want.

   The Summary screen opens.
3. From the navigation graphic below the menu bar, click **Collaboration settings**.

   The Configure community-specific collaboration settings screen opens.
4. From the left pane, click **Specialize collaboration settings for a partner**.

   The Add special collaboration settings for a partner screen opens.
5. Click **Choose party**, then select a partner from the list of available partners, then click **Add**.
6. Select the option **Pick the sender routing ID** then, from Define the settings the community will use to send messages to this partner, select the appropriate routing ID.
7. Select the option **Pick the receiver routing ID** then, from Define the settings the community will use to send messages to this partner, select the appropriate routing ID.
8. Select the option **Set sending rules for the AS2 message protocol**.
9. Select the option **Specify message attributes to be packaged with message**.
10. Click **Save changes**.
11. Select *FdaCenter* and *FdaSubmissionType* from the list, then click **Add**.
12. Click **Save changes**.

Specialize collaboration settings for a partner (PMDA)

You can specify collaboration settings that apply between one specific community and one specific partner. This procedure applies to PMDA only.

1. b. From the Getting Started screen, click the **Home** menu, then click the community name.

   The Summary screen opens.
2. From the menu bar, hover over the **Trading configuration** icon, then click **Manage trading configuration**.

   The Communities screen opens.
3. From the list of communities, click the name of the community that you want.

   The Summary screen opens.

4. From the navigation graphic below the menu bar, click **Collaboration settings**.

   The Configure community-specific collaboration settings screen opens.

5. From the left pane, click **Specialize collaboration settings for a partner**.

   The Add special collaboration settings for a partner screen opens.

6. Click **Choose party**, then select a partner from the list of available partners, then click **Add**.

7. Configure the options under Choose the settings to specialize as follows:

   - Select **Pick the sender routing ID** then, from Define the settings the community will use to send messages to this partner, select the appropriate routing ID.
   - Select **Pick the receiver routing ID** then, from Define the settings the community will use to send messages to this partner, select the appropriate routing ID for PMDA.
   - Select the option **Set sending rules for the AS2 message protocol**.
   - Select the option **Specify the signing certificate to use**.

8. Configure the options under AS2 as follows:

   - Select **Request receipts from partners**.
   - For **Receipt signing algorithm**, select **SHA256**.
   - Select the option **Encrypt messages**.
   - For **Message encryption algorithm**, select **AES(256-bit)**.
   - Select **Sign messages. Partners use your certificate to verify you as the sender**.
   - For **Message signing algorithm**, select **SHA256**.

9. For **Specify the signing certificate to use**, enter your certificate key.

10. Click **Save changes**.

Set up application delivery

An application delivery is a B2Bi object that specifies the way B2Bi sends files to applications. You set up application deliveries within a community. You can have multiple application deliveries.

1. From the menu bar, hover over the **Trading configuration** icon, then click **Manage trading configuration**.

   The Communities screen opens.

2. From the list of communities, click the name of the community that you want.

   The Summary screen opens.

3. From the navigation graphic below the menu bar, click **Application Delivery**.

4. From the Related tasks list at the bottom of the page, click **Add an application delivery**.

   The Exchange Wizard opens.

5. In the Choose transport protocol screen, select **File system**, and click **Next**.

6. In the Configure the file system settings screen, to enter the directory path, click **Browse**, select the IN folder, and click **Next**.

7. In the Exchange name screen, enter the Name for Exchange, and click **Finish**.

Update the incoming rule for Delivery Settings for each Partner

Define conditions that will cause payloads to be delivered to the appropriate exchange. If a payload does not satisfy the delivery criteria for any exchange, then the first available exchange will be used. An exchange with no criteria will be used only if it is the first available exchange.

> **Note**
>
> Use this procedure only when the application delivery directory path is unique for every Partner. These steps may vary according to the Customer Partner Configurations.

1. From the menu bar, hover over the **Trading configuration** icon, then click **Manage trading configuration**.

   The Communities screen opens.
2. From the list of communities, click the name of the community that you want.

   The Summary screen opens.
3. From the navigation graphic below the menu bar, click **Delivery Settings**.

   The Application delivery settings screen opens.
4. From the Related tasks list at the bottom of the page, click **Add an application delivery setting**.
5. In the Delivery Settings Wizard, select the application delivery for the partner, and click **Finish**.
6. To add a rule, from the list of application delivery, for the specified application delivery, click the link under **Criteria and Settings**.

   The Change application delivery settings page appears.
7. In the Delivery criteria tab, click **OR**, then click **Compare**.
8. From the drop-down list, select **From Routing ID**, and enter the routing ID.
9. Click **Save Changes**.

Repeat this procedure to create **OR** rule for all the Routing IDs available for a partner.

Add a trading pickup to a community

Trading pickups are located in community objects. A trading pickup specifies how you want the community to pick up or receive documents over the Internet from a remote partner.

Execute this procedure once for each community.

1. From the menu bar, hover over the **Trading configuration** icon, then click **Manage trading configuration**.

   The Communities screen opens.
2. From the list of communities, click the name of the community that you want.

   The Summary screen opens.

3. From the navigation graphic below the menu bar, click **Trading pickup** (Pickup Delivery exchange).
4. From the Related tasks list at the bottom of the page, click **Add a pickup**.
5. From the Choose Message Protocol, select **EDIINT AS2 (HTTP)**, and click **Next**.
6. From the Choose HTTP transport type, select **Use the system's global embedded HTTP server**, and click **Next**.
7. The Configure URL screen appears with default Routing ID, click **Next**.
8. Enter the name of the pickup exchange to receive messages from partners, and click **Finish**.

Add public URL configuration in trading pickup (Pharma Company URL)

Use this procedure to configure the URL that your partners use to connect to the HTTPS server to exchange messages.

1. From the menu bar, hover over the **Trading configuration** icon, then click **Manage trading configuration**.

   The Communities screen opens.
2. From the list of communities, click the name of the community that you want.

   The Summary screen opens.
3. From the navigation graphic below the menu bar, click **Trading pickup** (Pickup Delivery exchange).
4. From the list of trading pickups, click the link under Name.

   The Change this pickup page appears.
5. In the HTTP (embedded) settings tab, enter the URL used by partners, and click **Save changes**.
6. If you are using Axway B2Bi version 2.3.x, perform the following steps:
   a. Click the **Advanced** tab.
   b. For the Message processing, select **Limited**, and click **Save changes**.

> **Note**
>
> Ignore this step, if the **Limited** option is not visible.

Add partner encryption certificate

Use this procedure to import a trading partner's certificate and associate it with a partner object in your configuration.

Add a certificate for each community or partner for all agencies.

1. From the menu bar, hover over the **Partners** icon, then click **Manage Partners**.

   The Partners screen opens.
2. From the list of partners, click the name of the partner that you want.

   The Summary screen opens.

3. From the navigation graphic below the menu bar, click **Certificates**.
4. From the Certificates tab, click **Add a certificate**.
5. From the Certificate Wizard, select **Import a certificate from a file**, and click **Next**.
6. Click **Browse**, locate the Self-Sign certificate file as received from the agency: FDA or EMA or PMDA, and click **Next**.

> **Note**
>
> The certificate file is available on the server from where Axway UI is accessible.

7. From the View Certificate screen, check the **Make this the default encryption certificate** check box, and click **Finish**.

Repeat this procedure to add partner encryption certificate for all the agencies.

Add partner SSL certificate

Axway B2Bi provides options for allowing certificates to be used for authenticating the identity of trading partners. Secure Sockets Layer (SSL) protocol authentication provides an added layer of security to trading relationships.

Use this procedure to import a trading partner's SSL certificate is provided by FDA or PMDA.

1. From the menu bar, hover over the **Partners** icon, then click **Manage Partners**.

   The Partners screen opens.
2. From the list of partners, click the name of the partner that you want.

   The Summary screen opens.
3. From the navigation graphic below the menu bar, click **Certificates**.
4. In the Certificates tab, click **Add a certificate**.
5. In the Certificate Wizard, select **Import a certificate from a file**, and click **Next**.
6. Click **Browse**, and locate the Self-Sign certificate file as received from the agency: FDA or PMDA, and click **Next**.
7. In the View Certificate screen, check the **Trust this for SSL server and/or client authentication** check box, and click **Finish**.
8. Click **Save changes**.

Repeat this procedure to add all SSL certificate provided by FDA or PMDA.

Add public URL configuration in trading pickup

Use this procedure to add public URL configuration for all the agencies, once for each community or partner.

Add a certificate for each community or partner for all agencies.

1. From the menu bar, hover over the **Partners** icon, then click **Manage Partners**.

   The Partners screen opens.
2. From the list of partners, click the name of the partner that you want.

   The Summary screen opens.

3. From the navigation graphic below the menu bar, click **Partner delivery**.
4. From the Related tasks list at the bottom of the page, click **Add a delivery**.
5. In the Choose Message Protocol, select **EDIINT AS2 (HTTP)**, and click **Next**.
6. In the Configure the HTTP settings screen, enter the partner URL for an agency.
7. Check the **Clients must use SSL to connect to this server** check box, and click **Next**.

> **Note**
>
> Select this check box only for agencies whose URL starts with HTTPS.

8. In the Delivery exchange point screen, enter the name, and click **Finish**.
9. Log out of the application.
10. Log in to the Axway Server, and validate the connection with the partner URL by using the Telnet:`telnet <Partner URL domain> or <IP of Partner URL> <port>`

Repeat this procedure to add partner URLs for all the agencies.

Post-configuration step: Transmit the generated report

After you have configured the required settings in both Argus and Axway B2Bi environments, you can transmit your report to the reporting destination via the Axway gateway.

1. Click the icon associated with a report and select the **Transmission** tab from Report Details. The Report Details dialog box opens.
2. Click **OK** or **Cancel** to approve the transmission or discard any changes.
3. Click the **Transmit** button. The Transmit to Recipients dialog box is displayed.
4. Select the recipients of the report from the **Available Recipients** list.
5. Select the method of transmission from **Method**.
6. Enter any remarks in **Comments**.
7. Click **Transmit**. The selected report is transmitted to the specified recipients.

Typical workflow for transmitting regulatory reports to agencies/partners

Transmitting a report to an agency or a partner requires a series of configurations in both Argus and Axway B2Bi environments.

Follow the next steps to configure your Argus and Axway environments for transmitting a report to a regulatory agency or partner.

1. In Argus, create reporting destinations for the report to be transmitted using the Axway gateway.
2. In the Axway B2Bi interface, configure the following settings:
   a. Create a change request ticket to create the trading node engine.
   b. Create a community.
   c. Add a partner to a community.
   d. Create application pickups
   e. Specialize collaboration settings.

f. Set up application delivery.
g. Update the incoming rule for Delivery Settings for each partner.
h. Add a trading pickup to a community.
i. Add public URL configuration in trading pickup (Pharma Company URL).
j. Add partner certificate:
   - Add an encryption certificate.
   - Add a SSL certificate.
k. Add public URL configuration in trading pickup.

3. Create some cases compatible with the report.
4. Generate the report.
5. Post-configuration step: Transmit the generated report

9

Get support for Oracle Argus Cloud Service

Support is provided by your Cloud Service Delivery Manager, the Oracle Life Sciences Support Cloud, and Oracle's consulting organization or an Oracle partner.

- What Oracle Support services are available to Argus Cloud Service customers?
  Oracle Argus Cloud Service customers have access to two sources of support.
- Work with your CSDM (Cloud Service Delivery Manager)
  The CSDM team is a customer-facing service team that provides a single point of contact to Argus Cloud Service customers after provisioning is complete and the environment is turned over to customers.
- Use the Life Sciences Customer Support Portal to access the Oracle Support Cloud
  Cloud customers can access Life Sciences Support Cloud through the Life Sciences Customer Support Portal.
- You can still use Oracle and third-party consulting services
  Implementation, post-go-live, and upgrade services are available through Oracle Life Sciences Consulting (LSC) and Oracle Partner Network (OPN) consultants.

What Oracle Support services are available to Argus Cloud Service customers?

Oracle Argus Cloud Service customers have access to two sources of support.

- Regular meetings and referral through your Cloud Service Delivery Manager (CSDM)
- Submitting a support request ticket to Oracle Support.

Work with your CSDM (Cloud Service Delivery Manager)

The CSDM team is a customer-facing service team that provides a single point of contact to Argus Cloud Service customers after provisioning is complete and the environment is turned over to customers.

- About Cloud Service Delivery Manager (CSDM)
  A Cloud Service Delivery Manager (CSDM) is assigned to your account to serve as your single point of contact for support.
- CSDM is your single point of contact for Cloud Service support
  CSDM is a dedicated customer-facing service team that will be your single point of contact.
- What happens at your regular CSDM Governance call?
  You and your CSDM meet regularly for a governance call.
- Your Oracle Argus Cloud Maintenance calendar
  Based on the different types of maintenance required for each Cloud Service product, there is a schedule for each product and each customer.

- About change management
  Oracle Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software to maintain operational stability, availability, security, and performance.

About Cloud Service Delivery Manager (CSDM)

A Cloud Service Delivery Manager (CSDM) is assigned to your account to serve as your single point of contact for support.

The CSDM team works with you during implementation and after you go live.

CSDM doesn't replace Oracle Support and My Help; instead, your CSDM will route your questions to the proper groups in Oracle, saving you time and effort and getting you the information you need as quickly as possible. Your CSDM will:

- Conduct regular governance meetings with you to review open issues and escalated support requests, answer questions, provide metrics on support and change requests, and escalate solutions to problems
- Assist with coordinating upgrade and migration plans, when necessary
- Provide information on planned maintenance activities
- Update you on future product planning and enhancements
- Guide you on using the Oracle Support Cloud portal
- Route your feedback to the appropriate team to affect change to LSGBU products and processes
- Provide assistance with user setup and management.

CSDM is your single point of contact for Cloud Service support

CSDM is a dedicated customer-facing service team that will be your single point of contact.

The Oracle Life Sciences Support Cloud is self-service in the sense that you enter support and change requests yourself, update your requests, and mark them closed. For escalated tickets, your CSDM follows up with the cross-organization teams on:

- Root-cause investigations, incident reports, etc.
- Issue resolutions or planned activities with the Oracle AMS team, product teams, infrastructure team, Oracle Legal, Regulatory and Compliance, Sales, etc.
- Planning and coordinating the timing for application migrations and updates in the Cloud environment
- Training opportunities; for example, support cloud user management training
- Reviewing product documentation and standard procedures with you, such as user setup, MedDRA upgrades, Secure File Transfer Protocol (SFTP) folder creation and SFTP user creation and password reset, notifications, Oracle Identity Cloud Service (IDCS) functions, and Cloud infrastructure information.

What happens at your regular CSDM Governance call?

You and your CSDM meet regularly for a governance call.

The governance call covers escalated issues and questions. The CSDM includes the people who can solve the issues in the meeting, eliminating the need for you to coordinate issues with the involved specialized Oracle support services. A typical agenda looks like this:

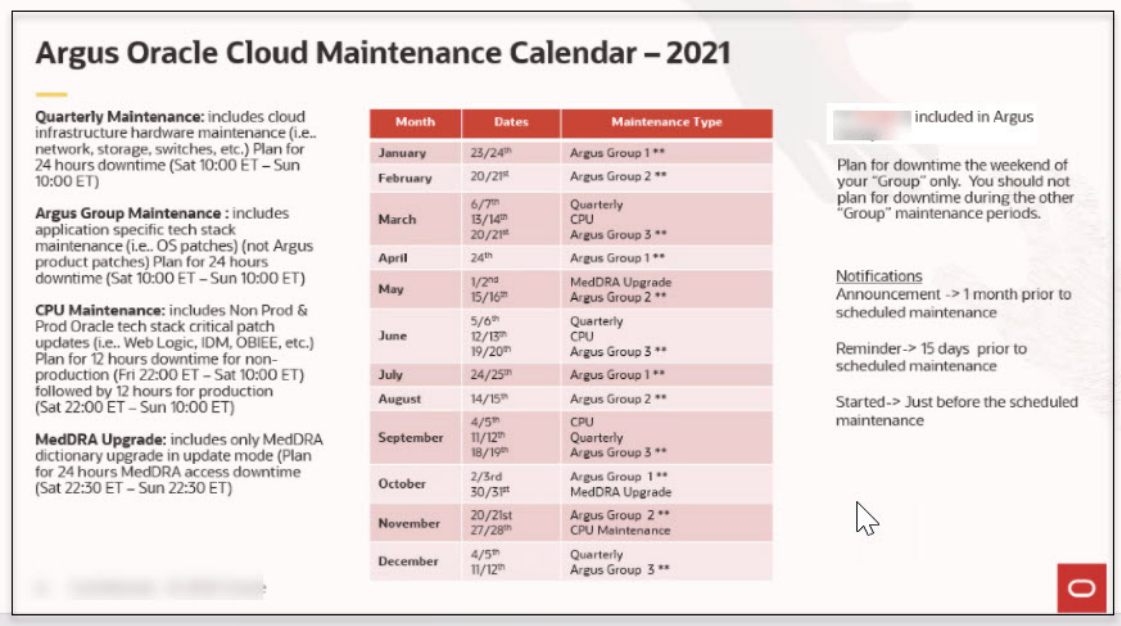
1. Open issue items, such as escalated tickets, patch information, and performance issues
2. Dashboard metrics that show the number of resolved support and change requests
3. Next steps: future and past releases
4. Argus Cloud Maintenance review.

Your Oracle Argus Cloud Maintenance calendar

Based on the different types of maintenance required for each Cloud Service product, there is a schedule for each product and each customer.

Your CSDM will notify you a month ahead of any planned maintenance.

Here is a typical Argus Cloud Maintenance Calendar:



About change management

Oracle Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software to maintain operational stability, availability, security, and performance.

For change requests that you make through the Oracle Life Sciences Support Cloud portal, Oracle follows formal change management procedures to review, test, and approve these changes prior to application in the production service.

Oracle works to ensure that change management procedures are conducted during scheduled maintenance windows, while taking into consideration low traffic periods and geographical requirements. Oracle will provide prior notice of modifications to the standard maintenance period schedule. For customer-specific changes and upgrades, where feasible, Oracle will coordinate the maintenance periods with you.

Use the Life Sciences Customer Support Portal to access the Oracle Support Cloud

Cloud customers can access Life Sciences Support Cloud through the Life Sciences Customer Support Portal.

- Oracle Argus Cloud Service support overview
  The Life Sciences Customer Support Portal provides 24x7 access to support.
- About support and change request features
  You can use the Life Sciences Customer Support portal to log and manage support and change requests, view tutorials, and access the knowledgebase.
- Register your account
  Once your user account for the Oracle Life Sciences Support Cloud has been set up, you will receive a welcome email with a link for registering for an Oracle account. This is how you create your user name and password.
- Log in to the Life Sciences Customer Support Portal
  You can access the Oracle Life Sciences Support Cloud via the Life Sciences Customer Support Portal.
- About the three types of access to the Life Sciences Support Cloud
  Oracle Life Sciences Support Cloud supports three user roles.
- Field entries common to all request types and products
  Required fields differ based on the type of request, but the fields described here are common for all request types and products.
- Email notifications from the Life Sciences Support Cloud
  Oracle Life Sciences Support Cloud sends notifications to keep you informed about your account, incidents logged, and status of support and change request tickets.

Oracle Argus Cloud Service support overview

The Life Sciences Customer Support Portal provides 24x7 access to support.

Oracle support for Oracle Cloud Services consists of:

- Diagnoses of problems or issues with the Oracle Cloud Services.
- Reasonable commercial efforts to resolve reported and verifiable errors in the Oracle Cloud Services so that those Oracle Cloud Services perform in all material respects as described in the associated Program Documentation.
- Support during Change Management activities described in the Oracle Cloud Change Management Policy.
- Assistance with technical service requests 24 hours per day, 7 days a week.

About support and change request features

You can use the Life Sciences Customer Support portal to log and manage support and change requests, view tutorials, and access the knowledgebase.

You have access to the following support features:

- **Support requests:** This includes online service request submission and automated assignment of service requests to Oracle Support engineers, plus the ability to monitor updates on requests on a 24x7 basis.
- **Change requests:** You can log a change request for business services you manage directly; for example if you want the Oracle hosting team to make any changes.
- **Self-service access administration:** Through a change request, authorized sponsor users and approved CROs and partners can request access for themselves and others.
- **Self-service support request escalation:** By your Customer-Delegated Administration (CDA) to the Support Duty Manager.
- Access to Oracle Support's extensive knowledgebase that provides solutions to many issues you might face.

Register your account

Once your user account for the Oracle Life Sciences Support Cloud has been set up, you will receive a welcome email with a link for registering for an Oracle account. This is how you create your user name and password.

The welcome email confirms that you have been approved to access the Oracle Life Sciences Support Cloud. To set up your user name and password, register for an Oracle account. This is a one-time, *required*, registration process. If you already have an Oracle account, you can begin using the LSGBU Customer Support portal to access the Oracle Life Sciences Support Cloud.

1. On the welcome email message, click **Register for an Oracle Account**.
2. Enter the information into the Create Account page and click **Create Account**.
   - Use the same email address as the one used to welcome you to Life Sciences Support Cloud.
   - Enter the company you work for. It doesn't have to be your sponsor company.

   > **Note**
   >
   > To watch a short video on creating and registering an Oracle Account, in your browser, enter **hsgbu.custhelp.com**, click **Tutorials**, then click **User Registration & Login**.

3. When you receive the email message verifying your Oracle account registration, click the **Verify E-mail Address** link.

   You can now log into the LSGBU Support Cloud.

Log in to the Life Sciences Customer Support Portal

You can access the Oracle Life Sciences Support Cloud via the Life Sciences Customer Support Portal.

1. In your browser, enter `https://hsgbu.custhelp.com`. For the Japanese version, enter `https://hsgbu-jp.custhelp.com`.
2. Click the **Log in to Oracle Life Sciences Support** button.

The Welcome to Oracle Life Sciences Support page displays icons associated with your assigned role.

> **Note**
>
> For information on how to get support through Oracle Life Sciences Support Cloud, see the *Oracle Argus Cloud Service User Guide* on the Documentation page.

About the three types of access to the Life Sciences Support Cloud

Oracle Life Sciences Support Cloud supports three user roles.

- **Base:** Base users can log support and change requests, then view, edit, and update them.
- **Customer-Delegated Administrator (CDA):** CDAs can view and edit their own support and change tickets, as well as all tickets logged against business services the user has access to. They can also:
  - Create user accounts for others and associate business services to those users for Support Request access.
  - Escalate tickets.
  - Access reporting dashboards.
- **Helpdesk:** Helpdesk users are team members who can view and edit their own support and change tickets, as well as all tickets logged against business services you have access to.

Field entries common to all request types and products

Required fields differ based on the type of request, but the fields described here are common for all request types and products.

Entries in these fields are required for all request types and products.

Field	Description
Product	Choose from a drop-down list of options.
Category	Choose from a drop-down list of categories that closely match the request being placed.
Business Service	Displays the names of your hosted application in OCI. For example, InForm studies name, Central Coding Instance name, Safety application name, etc.
Customer	Auto-populated based on the business service chosen.
Environment	Choose the environment (Prod/Live, Training, UAT, Development etc.) for which you are requesting the change.
Summary	A one-sentence description of the request.
Description	A more detailed explanation of what is needed for the request.
Alternate email	The requestor is automatically notified of changes during the request's lifecycle. If you wish others to be notified, add each email address to this field separated by a semi-colon.

Field	Description
Severity	Choose between: 1-Critical, 2-High, 3-Medium, 4-Low. **Note** For Change Requests - 1-Critical not applicable.
Implementation Window	US Business Hours = 1:00 PM - 1:00 AM GMT UK Business Hours = 7:00 am - 4:00 PM GMT Maintenance Window = 1:00 AM - 7:00 AM GMT Asian/Pacific MW = 1:00 PM - 7:00 PM GMT As Soon As Possible = These tickets are usually completed during the maintenance window but could be completed in any of the other windows, too.
sFTP Path	For implementation and PDF generation requests only, specify the sFTP path from where the files should be picked up for processing or the path where Oracle should place the files.
Requested Start Date	Date and time to process the request. While Oracle will make every effort to adhere to this date, it cannot be guaranteed for operation reasons. Please work with your Oracle representative for scheduling any important implementations.
Date Required By	An indication of the latest date by which the request should be processed.

Email notifications from the Life Sciences Support Cloud

Oracle Life Sciences Support Cloud sends notifications to keep you informed about your account, incidents logged, and status of support and change request tickets.

You might receive the following email notifications from Oracle Life Sciences Support Cloud:

- A welcome email when your Oracle Life Sciences Support Cloud account is created.
- A verification request after you create your Oracle account.
- Notification that a new incident has been logged by you or another user who included you in the **Additional Contacts** field of their request.
- Updates about the status of your tickets.
- Notification that a ticket has been closed.

To see details about the notification, log into Life Sciences Customer Support Portal.

Note

If you are a sponsor-level user and require notifications for planned and unplanned outages for given business services, you can log a Support Request asking to be notified.

You can still use Oracle and third-party consulting services

Implementation, post-go-live, and upgrade services are available through Oracle Life Sciences Consulting (LSC) and Oracle Partner Network (OPN) consultants.

If you are working with Oracle Life Sciences Consulting (LSC), when you go live with Oracle Argus Cloud Service, HSC hands over the support responsibility to a CSDM. If you're working with a third-party consulting service, they will call upon CSDM as needed.