Oracle Argus Cloud Service
Administration Guide

Release 8.2.3
F42515-04
August 2022

ORACLE

Oracle Argus Cloud Service Administration Guide, Release 8.2.3

F42515-04

Contents

8 Get support for Oracle Argus Cloud Service

Preface

This preface contains the following sections:

Intended Audience

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

Documentation accessibility

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

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

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.

Access to Oracle Support

To receive support assistance, determine whether your organization is a cloud or on-premises customer. If you're not sure, use Support Cloud.

Cloud customers receive support assistance through Support Cloud

Oracle customers that have purchased support have access to electronic support through Support Cloud.

Contact our Oracle Customer Support Services team by logging requests in one of the following locations:

- English interface of Oracle Health Sciences Customer Support Portal (https://hsgbu.custhelp.com/)
- Japanese interface of Oracle Health Sciences Customer Support Portal (https://hsgbu-jp.custhelp.com/)

You can also call our 24x7 help desk. For information, visit http://www.oracle.com/us/support/contact/health-sciences-cloud-support/index.html or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

On-premises customers receive support assistance through My Oracle Support

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

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 Health 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.

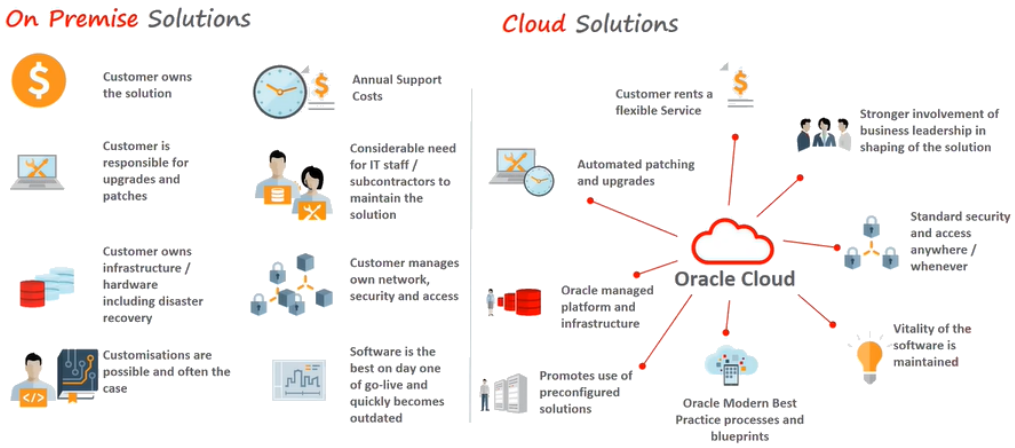
If you subscribe to Oracle Argus Advanced Cloud Service*, an annually reviewed Disaster Recovery environment is also included. Oracle implements the plan in the event of a disaster. The target is a system availability of 99.5 percent and recovery within 24 hours.

> **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

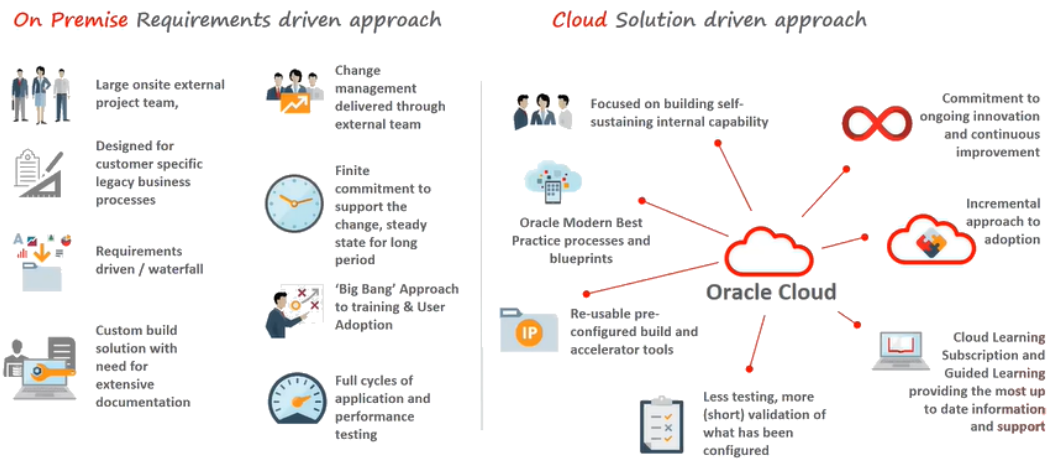
How Oracle Argus Cloud Service differs from the on-premise version

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 2008 R2 Standard/ Enterprise Edition (64 bit)
- MedDRA Dictionary
- WHO-Drug Dictionary
- DFC 6.5 SP3 for Documentum (optional, if Documentum is used)
- RightFax 9.4 (for Transaction Server only)
- Microsoft Office 2010 (32 Bit) (for Transaction Server only)

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) • Triage with duplicate checking • 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 health care 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

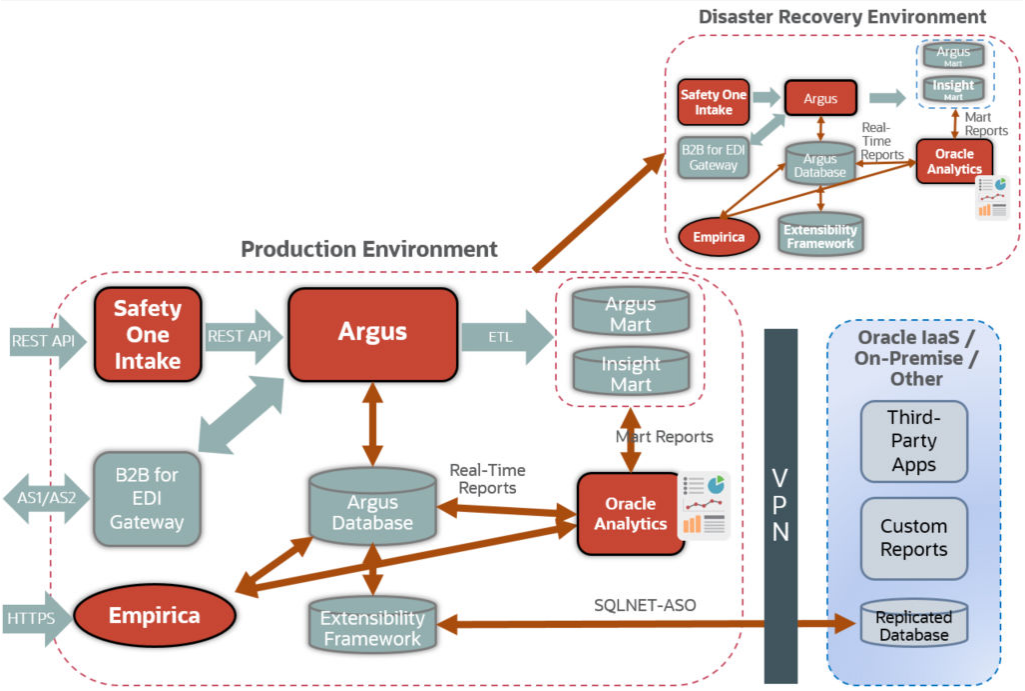
In addition to the base components, you have also access to:

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 Health Sciences Empirica Signal and, as such, it brings the two halves of the Oracle Health 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
(Optional) Data Replication	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.

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 HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

   > **Note:**
   >
   > A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **Application User Access** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.
6. From the **Category** drop-down list, expand **Change - Cloud Environment**, then **Application**, **User**, and select **Add**.
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 this change, 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.

14. 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.
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. 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**.

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 Oracle Health Sciences Identity and Access Management Service (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
- 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
- Set up the VPN tunnel
- 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 HSGBU 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 Health 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 Health Sciences Identity and Access Management Service, 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.

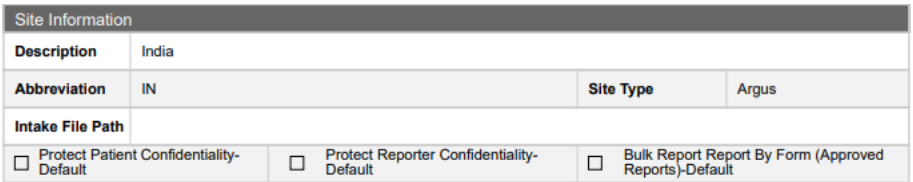
User sites fields descriptions

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.

Field or Control Name	Description
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.

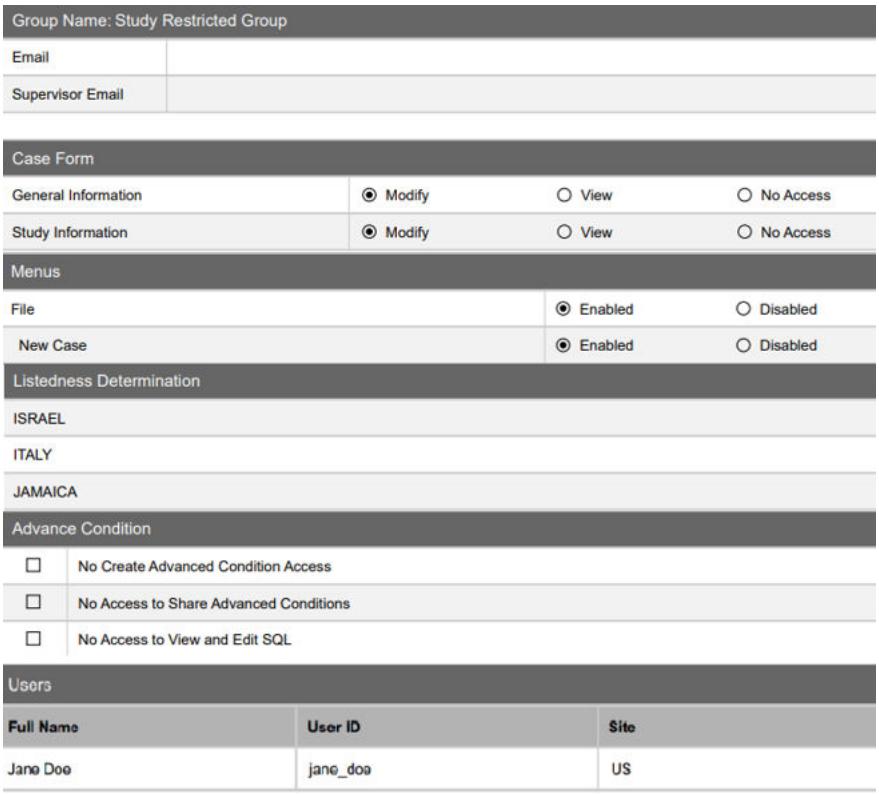
1. Click **Access Management**, then **Argus**, and then **Groups**.
2. Select a **Group** and click to view the group details in the right panel.
3. To display the **Print** dialog that enables you to print either the entire window or only the text covered by the current selection, click **Print**.
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.



Manage users

You need first to provision the user in Oracle Health Sciences Identity and Access Management Service, then you can add the user to Oracle Argus Cloud.

- Create users in Oracle Health Sciences Identity and Access Management Service
  As a customer-delegated administrator, setting up access for your users involves two steps. First, create the user in Oracle Health Sciences Identity and Access Management Service. Second, add the user to the Oracle Argus Cloud Service.
- Add users to Oracle Argus Cloud Service
  Once you have provisioned an user in Oracle Health Sciences Identity and Access Management Service, you can add the user to Oracle Argus Cloud Service.
- Users fields description
  Find here a table that describes the fields in the Users section.
- Assign OIM roles to Argus users
  Users can't start working until they have been assigned one or more product roles.
- Reset a user password
  You can reset a user password in Oracle Identity Self Service.
- Disable a user in Oracle Health Sciences Identity and Access Management Service
  This is the procedure you must follow to disable the user in Oracle Health Sciences Identity and Access Management Service.
- Disable a user in Oracle Argus Cloud Service
  This is the procedure for temporary disabling the user in Oracle Argus Cloud Service.

- 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 Oracle Health Sciences Identity and Access Management Service

As a customer-delegated administrator, setting up access for your users involves two steps. First, create the user in Oracle Health Sciences Identity and Access Management Service. Second, add the user to the Oracle Argus Cloud Service.

To create users in Oracle Health Sciences Identity and Access Management Service:

1. Open a browser and navigate to your company's Oracle Identity Self Service URL. Log in using your Oracle Argus Cloud Service administrator credentials.
2. Click **Administration**, then **Users** in the left pane.
3. Click **Create**.
4. Enter the user attributes listed below (the values in the table are provided only as examples) to create the user.

Item	Value
Last name	Doe
Organization	example
User Type	Full-Time Employee
User Login	johndoe
Password	Enter a password.
Confirm Password	Confirm the password.

5. When you are done entering the user information, click **Submit**.

Add users to Oracle Argus Cloud Service

Once you have provisioned an user in Oracle Health Sciences Identity and Access Management Service, 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.

For more information about the fields in the Add User window, see Users fields description.

> **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 Self Service.
> - When you use Oracle Identity Self Service authentication, you must select **Enable LDAP Login** in the Oracle Argus Cloud Service user creation pane.

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.
User Type	Select the type of user, such as an Oracle Argus Safety Japan user, from the drop-down list.

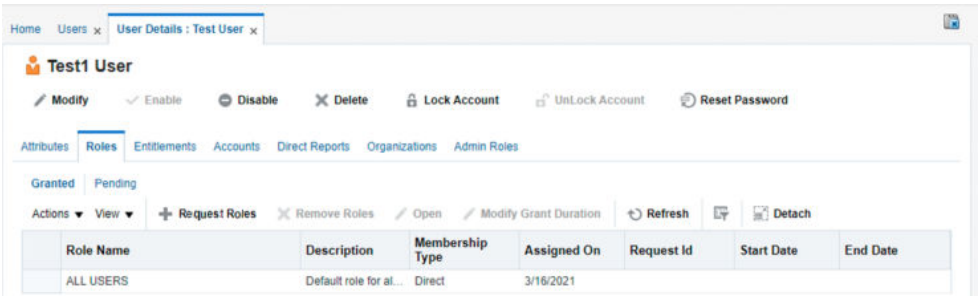
Field or Control Name	Description
User Roles - Select	Attach the user to pre-configured user roles. The following user roles are available: • **Enterprise User** - allows you to configure a workflow manager user as an enterprise user. If the enterprise role is assigned, the user can view cases of any 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. • **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.

Assign OIM roles to Argus users

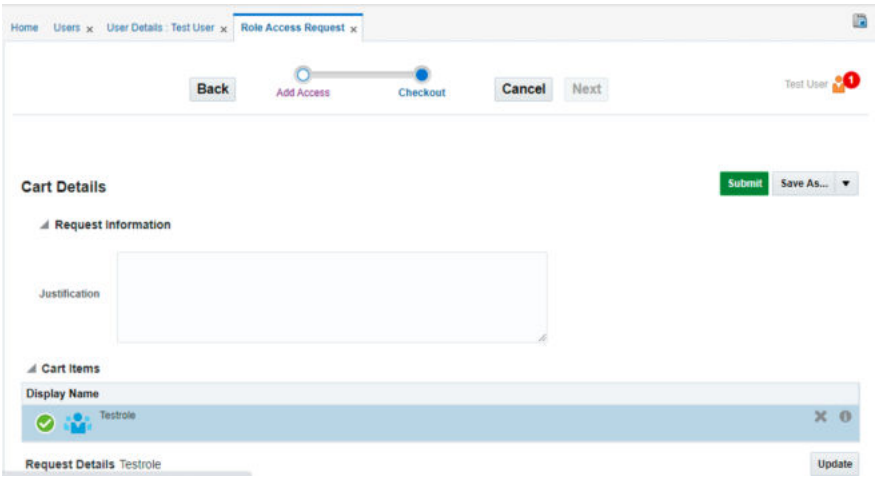
Users can't start working until they have been assigned one or more product roles.

1. Sign in to Oracle Identity Manager with your administration account.
2. In the upper right corner, click **Manage**.
3. On the Home page, click **Users**.
4. Search for the user you want to assign OIM roles, and then, in the User Login column, click the user's name.
5. On the User Details page, select the **Roles** tab.
6. Select **Request Roles**.



The Role Access Request page opens.

7. In the search box, type the name of the role you want to assign and press **Enter**.
8. To the right of the role, click **Add to Cart**.
9. In the upper-right, click **Next**.
10. Then, click **Submit**.



Reset a user password

You can reset a user password in Oracle Identity Self Service.

1. Open a browser and navigate to your company's Oracle Identity Self Service URL. Log in using your Oracle Argus Cloud Service credentials.

2. In the left pane, click **Administration**, then **Users**.
3. In the right pane, enter one of the following for the user whose password you want to reset: user login, first name, last name or email address, then click **Search**.
4. In the results list, click the user whose password you want to reset.
5. In the right pane, click **Reset Password**.
6. Select **Manually change the Password**.
7. Enter and confirm the new password, then click **Reset Password**.

> **Note:**
>
> For cloud environments, the password reset option in Oracle Argus Cloud Service is disabled, as this feature is managed from Oracle Identity Self Service.

Disable a user in Oracle Health Sciences Identity and Access Management Service

This is the procedure you must follow to disable the user in Oracle Health Sciences Identity and Access Management Service.

> **Note:**
>
> You need to have Customer-Delegated Administrator privileges to disable users in Oracle Identity Self Service.

1. Open a browser and navigate to your company's Oracle Identity Self Service URL. Log in using your Oracle Argus Cloud Service credentials.
2. In the left pane, click **Administration** and then **Users**.
3. In the right pane, enter one of the following for the user whose account you want to disable: user login, first name, last name or email address, then click **Search**.
4. In the results list, click the user login of the user whose account you want to disable.
5. Click **Lock Account** to prevent the account from being used.
6. In the Lock Account confirmation dialog box, click **Lock**.
7. On the **Roles** tab, select the role you want to remove.
8. From the **Actions** list, select **Remove**.

   The Remove Roles page opens.
9. Review the roles in the cart. You can click **Remove** to the right of a role to exclude it from the cart.
10. Click **Submit** in the top right.

    The message *Successfully completed the operation* appears.

> **Note:**
>
> If you need to remove delegated administrator roles from this account, contact Health Sciences Support for assistance.

11. Click the x button in the top right corner to close the dialog box.
12. On the User Details page, click **Disable User**.
13. On the Disable Users page, click **Submit** in the top right.

    The message *Successfully completed the operation* appears after the user has been disabled.

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.

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**.

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 HSGBU 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 Manager (OIM).
- 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 HSGBU Customer Support Portal.

1. Log in to the HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **General Information/Action** tile, click **Create a Request**.

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

6. From the **Category** drop-down list, expand **Service Request**, then **Application**, **General**, and select **Action**.
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 to create the enterprise.
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 create the new enterprise, 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: `Create enterprise <enterprise name> in the <environment name> environment.`
14. 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.`
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. 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**.
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**.

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 HSGBU Customer Support Portal.

- Schedule incremental ETLs
  To schedule incremental ETLs, you need to create a change request ticket in HSGBU 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 HSGBU Customer Support Portal.

1. Log in to the HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **General Information/Action** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.
6. From the **Category** drop-down list, expand **Service Request**, then **Application**, **General**, and select **Action**.
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 to run the initial ETL.
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 run the initial ETL, 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: `Run <product name> initial ETL in the <environment name> environment.`
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 **Description** field, enter a detailed description of your request.

16. 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**.

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**.

Schedule incremental ETLs

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

1. Log in to the HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **General Information/Action** tile, click **Create a Request**.

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

6. On the **General Information/Action** tile, click **Create a Request**.

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

7. From the **Category** drop-down list, expand **Service Request**, then **Application**, **General**, and select **Action**.
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 **Action** drop-down list, select **Other**.
12. From the **Oracle Internal** radio buttons, select **No**.
13. 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.
14. In the **Summary** field, enter a short description of your request.

Example: `Schedule <product name> incremental ETLs in the <environment name> environment.`

15. 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.`

16. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
17. 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**.

18. Select appropriate values from the **Severity** and **Implementation Window** drop-down lists.
19. In the **Date Required By** field, select a value from the calendar.
20. 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 HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **General Information/Action** tile, click **Create a Request**.

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

6. From the **Category** drop-down list, expand **Service Request**, then **Application**, **General**, and select **Action**.
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 to re-initialize the ETL process.
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 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.
13. In the **Summary** field, enter a short description of your request.

    Example: `Run re-initial <product name> ETL in the <environment name> environment.`
14. 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.`
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. 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**.
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**.

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 Manager (OIM).

Oracle Argus Cloud Service users can access OBIEE and BIP based on their user type and role.

Once you have identified the specific role for each user account that needs to access OBIEE and BIP, you must associate the role to the user in Oracle Identity Manager.

> **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 OBIEE, they will be able to access the Oracle Argus Analytics application (Privilege will be based on the associated Role).

- OBIEE and BIP user types
  There are three types of OBIEE and BIP users.
- OBIEE and BIP user roles
  There are multiple out-of-the-box OBIEE and BIP roles available for Oracle Argus Cloud Service users.
- OBIEE and BIP users examples
  Some OBIEE and BIP users examples, for a better understanding of the user type and role association.

OBIEE and BIP user types

There are three types of OBIEE and BIP users.

- **Admin**: can create, update, delete, and view reports and dashboards. Moreover, the admin user has OBIEE and BIP Administrator privileges. This user is similar to the Customer Delegated Administrator user in OIM 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.

OBIEE and BIP user roles

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

Associate Oracle Argus Cloud Service user accounts with specific roles in Oracle Identity Manager (OIM), according to their user type.

#	Role	Type	Subject Area	Description
1	FARAdminGroup	Admin	Argus Safety Aggregate Reporting	Admin for FAR (Argus Safety Aggregate Reporting) BIP Reports
2	FARSafetyAuthorGroup	Author	Argus Safety Aggregate Reporting	Author for FAR (Argus Safety Aggregate Reporting) BIP Reports
3	FARSafetyConsumerGroup	Consumer	Argus Safety Aggregate Reporting	Consumer for FAR (Argus Safety Aggregate Reporting) BIP Reports
4	AIAdminGroup	Admin	Argus Insight	Admin for AI (Oracle Argus Insight) BIP Reports
5	AIAuthorGroup	Author	Argus Insight	Author for AI (Oracle Argus Insight) BIP Reports
6	AISafetyConsumerGroup	Consumer	Argus Insight	Consumer for AI (Oracle Argus Insight) BIP Reports
7	PVAAdmin	Admin	Argus Analytics	Admin for Oracle Argus Analytics OBIEE Reports
8	PVASafetyGroup	Author	Argus Analytics	Author for Oracle Argus AnalyticsOBIEE Reports
9	PVASafetyConsumersGroup	Consumer	Argus Analytics	Consumer for Oracle Argus Analytics OBIEE Reports
10	EXPAdminGroup	Admin	Argus Safety Expedited Reports	Admin for Argus Safety Expedited BIP Reports
11	EXPSafetyAuthorGroup	Author	Argus Safety Expedited Reports	Author for Argus Safety Expedited BIP Reports
12	EXPSafetyConsumerGroup	Consumer	Argus Safety Expedited Reports	Consumer for Argus Safety Expedited BIP 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.

OBIEE and BIP users examples

Some OBIEE and BIP 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 Oracle Identity Manager (OIM).

#	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 HSGBU Customer Support Portal.

Obtain a Product Verification Pack

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

1. Log in to the HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. Under the menu bar, on the right side of the screen, click **Create a new Support Request**.
4. From the **Customer** drop-down list, search for your company's name and select it from the list.
5. From the **Product** drop-down list, select **Argus Safety**.
6. From the **Business Service** drop-down list, a business service or **No Value**.
7. From the **Oracle Internal** radio buttons, select **No**.
8. 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.
9. From the **Severity** drop-down list, select **4 - Low**.
10. From the **Issue Category** drop-down list, select **General Inquiry**.

    If you have a ticket reference number that corresponds to this request, enter it in the **Alternative ref number (if applicable) field**.
11. In the **Summary** field, enter your request as a short text.
12. In the **Description** field, provide the SFTP access details to a remote folder where the Oracle support team can copy the requested PVP files.
13. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this request, separated by a semicolon.

14. Click **Submit**.

    You will receive an email confirmation of your submission.

4

Manage dictionaries

You can load your dictionary files to Argus with each dictionary update, then recode your cases to use the new dictionaries.

- About dictionaries
  Your company must purchase a subscription license for the third-party dictionary software, as well as all the consents, permits, and authorizations necessary for Oracle to access and use the software on your company's behalf.
- Load dictionaries
  To upload a dictionary file to Argus, you need to create a change request ticket in HSGBU Customer Support Portal.
- Recode Dictionaries
  Recoding does not take place automatically following a dictionary upgrade. To recode your cases with the latest dictionary, you need to create a change request ticket in HSGBU Customer Support Portal.

About dictionaries

Your company must purchase a subscription license for the third-party dictionary software, as well as all the consents, permits, and authorizations necessary for Oracle to access and use the software on your company's behalf.

Before Oracle can install the optional software, your company must provide evidence of such licenses, as well as a copy of the licensed software, if applicable. Your company is responsible for supporting third-party software, including the purchase of support contracts from third-party vendors, as applicable.

Third-party software includes:

- MedDRA dictionary subscriptions
- MedDRA J and J Drug dictionary subscriptions
- WHO Drug dictionary subscriptions.

Oracle applies regular updates to third-party dictionary software, as follows:

Dictionary	Update interval
MedDRA and MedDRA J	6 months
J Drug	6 months
WHO Drug	12 months

Load dictionaries

To upload a dictionary file to Argus, you need to create a change request ticket in HSGBU Customer Support Portal.

1. Log in to the HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **Application Install/Change/Re-setup/Uninstall** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.
6. From the **Category** drop-down list, expand **Change - Cloud Environment**, then **Application**, and select **Setup**.
7. In the **Select Customer** drop-down, either type the name of your company in the search field or select it from the list, and then click **OK**.
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 load the dictionary files.
11. From the **Action** drop-down list, select **Other**.
12. From the **Oracle Internal** radio buttons, select **No**.
13. From the **Environment** drop-down list, select the environment where you want to load the dictionary files, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.
14. In the **Summary** field, enter a short description of your request.

    Example: `Load <WHO DRUG|MEDDRA|MedDRA J> dictionary in <environment>.`
15. In the **Description** field, enter a detailed description of your request. Make sure you specify if the dictionary files are located on an sFTP server or they are attached to the change request.
16. If you have uploaded the dictionary files to an sFTP server, enter the location in the **sFTP path** field.
17. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
18. Select appropriate values from the **Severity** and **Implementation Window** drop-down lists.
19. In the **Date Required By** field, select a value from the calendar.

20. If you want to attach the dictionary files to the change request, under **Attach Documents**, click **Choose File**, and then browse for your files.

> **Note:**
>
> You can attach ticket files with a maximum size of 20 MB to the change request. If your file exceeds 20 MB, you will need to upload it to a sFTP server location that you specify in the **sFTP path** field.

21. Click **Submit**.

The Oracle team will upload the provided dictionary files to Argus.

> **Note:**
>
> - After the dictionary is uploaded, you need to select it in the Argus Console, so that it is available for coding.
> - You need to create one change request ticket per environment, for one dictionary. Therefore, to upload a dictionary file to the Production, Development, and Validation environments, you need to create three change requests tickets in total.

Recode Dictionaries

Recoding does not take place automatically following a dictionary upgrade. To recode your cases with the latest dictionary, you need to create a change request ticket in HSGBU Customer Support Portal.

> **Note:**
>
> - Recoding applies only to MedDRA and MedDRA J dictionaries.
> - Ensure that you have selected the latest dictionary from the Argus Console, after the Oracle team uploaded it in your environment.

1. Log in to the HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.

4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **Application Install/Change/Re-setup/Uninstall** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.
6. From the **Category** drop-down list, expand **Change - Cloud Environment**, then **Application**, and select **Setup**.
7. In the **Select Customer** drop-down, either type the name of your company in the search field or select it from the list, and then click **OK**.
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. In the **Business Service** drop-down list, select the name of the server where you want the dictionary recode to be performed.
11. From the **Action** drop-down list, select **Other**.
12. From the **Oracle Internal** radio buttons, select **No**.
13. From the **Environment** drop-down list, select the environment where you want the dictionary recode to be performed, and make sure your selection is consistent with the value you selected in the **Business Service** drop-down above.
14. In the **Summary** field, enter a short description of your request.

    Example: `Recode <MEDDRA|MEDDRA J> dictionary in <environment> in <view-only|update> mode.`
15. In the **Description** field, enter a detailed description of your request, including any MedDRA recoding tool parameters, if applicable.

    You can also instruct Oracle to provide you with a log of the recode process.
16. In the **Additional Contacts** field you can enter one or more email addresses to be notified about this change request, separated by a semicolon.
17. Select the appropriate values from the **Severity** and **Implementation Window** drop-down lists.

> **Note:**
>
> - All users are expected to close the opened cases before recoding starts, to avoid any errors.
> - Usually, view-only recoding does not require downtime. However, if you don't want users to open cases while the recoding is in progress, specify that you want the Argus application to be inaccessible during the view-only recoding process and provide the downtime information.
> - Take into account that the process of update-mode recoding requires at least four hours of downtime. For this case, plan the downtime during weekdays for the Validation and Development environments, and during weekend for the Production environment.
> - The downtime duration may vary depending on the data volume in your environment.

18. In the **Date Required By** field, select a value from the calendar.
19. Click **Submit**.

The cases will be updated based on the uploaded dictionary in the specified environment.

To recode your cases based on a dictionary, you need to create two change request tickets for each available environment, one for the view-only mode and one for the update mode. Therefore, for the Production, Development, and Validation environments you need to create six change request tickets in total:

1. One change request ticket for the view-only mode recoding, where you ask Oracle to generate a file with the existing cases that will include the new coding. As a result, you will obtain a file with all the cases that will be changed. You can review the changes and make sure that the cases are properly updated.
2. One change request for update mode recoding, where you ask Oracle to recode the cases based of the new dictionary for the specified environment. As a result, the cases will be updated based on the new dictionary in the environment.

5

Use the Argus Cloud Service utilities

Oracle Argus Cloud Service includes a range of utilities, which you can provide to customer accounts by creating a Change Request in the HSGBU Customer Support Portal.

- Data Refresh
  This utility adds the data refresh and restoration capability to Oracle Argus Cloud.
- ESM logs access on sFTP
  This utility copies the ESM log files to an sFTP server that you can access.
- 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.
- OAM Reports
  Use this utility to generate out-of-the-box (OOB) reports provided by the Oracle Access Management platform.
- Usage Billing
  Use this utility to track your case volume by generating various license usage reports.

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 HSGBU Customer Support Portal, asking for access to the Oracle Argus Data Refresh utility. After logging the CR, you will receive more information about this utility from the Oracle team.

Where can I find more information?

Log in to My Oracle Support and search for the following article: *2682378.1*. Locate the Release Notes for Data Refresh.

ESM logs access on sFTP

This utility copies the ESM log files to an sFTP server that you can access.

What does it do?

The ESM Logs Access on sFTP utility copies ESM log files to a sFTP that you can access, with a predefined time frequency. The utility can also delete the log files after a specified time interval.

How do I get it?

You need to create a change request (CR) in HSGBU Customer Support Portal, asking for access to the ESM Logs Access on sFTP utility, and providing the values for the following parameters:

Parameter	Description	Default Setting	Valid Values	Sample Value
JobInterval	Frequency of copying the ESM log files to the sFTP server, expressed in minutes	Once per 12 hours	From 120 to 1440, in multiples of 30	720
RemoveDestFile Interval	Frequency of deleting the copied log files from the sFTP server, expressed in days	90 days	From 30 to 90	90

Where can I find more information?

Log in to My Oracle Support and search for the following article: *2682378.1*. Locate the Release Notes for ESM logs Access on sFTP.

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 HSGBU Customer Support Portal, asking for access to the Argus Cloud Extensibility and Integrations Framework utility.

Where can I find more information?

Log in to My Oracle Support and search for the following article: *2682378.1*. 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?

To implement this utility in your environment, create a change request (CR) through the HSGBU Customer Support Portal, 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: *2682378.1*. 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.

Metric	Description
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: *2682378.1*. Locate the Release Notes for Monitoring Framework.

OAM Reports

Use this utility to generate out-of-the-box (OOB) reports provided by the Oracle Access Management platform.

What does it do?

The OAM (Oracle Access Manager) Reports utility provides access from the Oracle Argus Cloud Service to the following types of out-of-the-box (OOB) reports built into the Oracle Access Management platform:

- **Account Management** reports, including the `Accounts_Locked_Out` report, that allows you to view details about accounts that have been locked out.
- **Authentication** reports, that allow you to view details regarding user authentications, including:
  - Authentication Statistics report, with details regarding failed and successful authentications
  - AuthenticationFromIPByUser report, with details regarding failed and successful authentications from a particular IP address
  - AuthenticationPerIP report, with details regarding failed and successful authentications from this IP address
  - AuthenticationStatisticsPerServer report, with details regarding failed and successful authentications from a particular server instance.
- **Errors and Exceptions** reports, that contain details regarding errors and exceptions encountered during runtime, including:
  - All Errors and Exceptions report (errors and exceptions encountered during runtime)
  - Authentication Failures report (failed authentications)
  - User Activities report
  - Authentication History report (failed and successful authentications)

  - Authorization History report, with details regarding failed and successful authorizations
  - Multiple Logins From Same IP report (multiple logins from the same IP address).

How do I get it?

You need to create a change request (CR) in HSGBU Customer Support Portal, asking for access to the OAM Reports utility.

Once the Oracle team enables this utility in your Oracle Argus Cloud environment, you can access the OAM reports using BI Publisher:

1. Start BI Publisher.
2. Log in to BI Publisher with your credentials. For example: *https://<hostname>:<port>/xmlpserver*.
3. From the top menu, click **Catalog**.
4. In the left navigation pane, under **Folders**, click **Shared Folders**, then **OAM**. A list of all available reports appears in the right navigation pane.
5. Click **Open** under the report you want to access.

Where can I find more information?

- Log in to My Oracle Support and search for the following article: *2682378.1*. Locate the Release Notes for OAM Reports.
- Read about the OOB reports classification from the official Oracle Access Management documentation.

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 HSGBU Customer Support Portal. After logging the CR, the Oracle AMS 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: *2682378.1*. Locate the Release Notes for Usage Billing.

6

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.
- Set up the VPN tunnel
  VPN means using a public network to make end-to-end connection between two private networks in a secure fashion. VPN tunnel refers to a way to deliver packets through the internet to private RFC 1918 addresses.
- 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.

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 Health 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
- OBIEE/BIP 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 HSGBU 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 OIM 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 HSGBU Customer Support Portal.
- Reset an sFTP user password
  To reset an SFTP user password, you need to create a change request ticket in HSGBU Customer Support Portal.
- Remove an sFTP user account
  To remove an SFTP user account, you need to create a change request ticket in HSGBU Customer Support Portal.

Add an sFTP user

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

1. Log in to the HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **SFTP User Access** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.
6. From the **Category** drop-down list, expand **Change - Cloud Infrastructure**, then **Infrastructure Services**, **SFTP**, **User** and select **Add**.
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 create 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: `Create sFTP user <user name> in <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. 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 xhttps://support.oracle.com/, and search for Doc ID 2467980.1. To access this article, you must be logged in to My Oracle Support.

20. Click **Submit**.

Reset an sFTP user password

To reset an SFTP user password, you need to create a change request ticket in HSGBU Customer Support Portal.

1. Log in to the HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **SFTP User Access** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.
6. From the **Category** drop-down list, expand **Change - Cloud Infrastructure**, then **Infrastructure Services**, **SFTP**, **User** and select **Change**.
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 reset the sFTP user password, 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: `Reset sFTP user password for <user name> in <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**.

Remove an sFTP user account

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

1. Log in to the HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **SFTP User Access** tile, click **Create a Request**.

   The screen **Submit a request to our hosting team** appears.
6. In the **SFTP User Access** tile, click **Create a Request**.
7. From the **Category** drop-down list, expand **Change - Cloud Infrastructure**, then **Infrastructure Services**, **SFTP**, **User** and select **Remove**.
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 **Action** drop-down list, select **Other**.
12. From the **Oracle Internal** radio buttons, select **No**.
13. 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.
14. In the **Summary** field, enter a short description of your request.

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

20. Click **Submit**.

Set up the VPN tunnel

VPN means using a public network to make end-to-end connection between two private networks in a secure fashion. VPN tunnel refers to a way to deliver packets through the internet to private RFC 1918 addresses.

If you want to set up a VPN tunnel, contact your CSDM (Cloud Service Delivery Manager), who will guide you throughout your request. You will be asked to provide several details useful for the VPN setup. After that, the Oracle team will implement the private connection for you.

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.

To configure SMTP:

1. Navigate to **Argus Console**, **System Configuration**, and then to **SMTP Configuration**.
2. In the SMTP Configuration dialog box, enter the following parameters:
   - SMTP Server IP address or name
   - Port number (Default value is 25)
   - User name.
3. Select the **Enable SMTP** check box.
4. Enter the FQDN (Fully Qualified Domain Name).
5. In the Global From Address field, enter a valid e-mail address.

   When e-mails are sent from Oracle Argus Safety, the From address for all e-mails is set to the e-mail specified in the Global From Address field.
6. Select the Authentication mode for the SMTP configuration, from the drop-down list.
7. Enter the SMTP User Name used by the Argus Service to authenticate with for SMTP Emailing.
8. Enter the SMTP Password used by the Argus Service to authenticate with for SMTP Emailing.

   > **Note:**
   >
   > This field is required when **Basic Authentication** is selected as the authentication method.
9. Select the **Custom SMTP Header** check box to customize the SMTP header.
10. Click **Validate and Save**, to connect to the e-mail server as per the configuration data.

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.

7

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 HSGBU 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 HSGBU 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 HSGBU 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 Oracle Identity Manager (OIM).
- 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 Oracle Identity Manager (OIM).

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 HSGBU Customer Support Portal.

1. Log in to the HSGBU Customer Support Portal
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

3. On the upper-side menu, click **Change Requests**.
4. Under the menu bar, on the right side of the screen, click **Create a new Change Request**.
5. On the **Application Install/Change/Re-setup/Uninstall** tile, click **Create a Request**.
6. From the **Category** drop-down, expand **Change - Cloud Environment, Application, Integration** then select **Setup**.
7. From the **Customer** drop-down, search for your company's name and select it from the list.
8. From the **Product** drop-down, select **Argus Safety**.
9. From the **Business Service** drop-down, select the name of the server where you want this change.
10. From the **Action** drop-down, select **Other**.
11. From the **Oracle Internal** radio buttons, select **No**.
12. 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.
13. 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.

14. In the **Description** field, enter more details for 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. 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**.
17. Select the appropriate values from the **Severity** and **Implementation Window** drop-downs.
18. Click the **Date Required By** field and select a value from the calendar.
19. 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 Oracle Identity Manager (OIM).

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 associate the appropriate role to their user account in Oracle Identity Manager.

> **Note:**
>
> If you don't have privileges to assign Axway UI access to users, you need to create a change request ticket in HSGBU 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	<PROD/DEV/VAL>_AXWAYB2BI_View_Reports	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	<PROD/DEV/VAL>_AXWAYB2BI_Admin_Role	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 Oracle Identity Manager (OIM).

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 associate the appropriate role to their user account in Oracle Identity Manager.

> **Note:**
>
> If you don't have privileges to assign Oracle B2B access to users, you need to create a change request ticket in HSGBU 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	OIM Role	Description
Monitor	Read-only	<PROD/DEV/VAL>_SOAB2B_Monitor	Monitor the communication between a customer and their partner: • Search for messages • View messages • Monitor messages, also B2B failed message transmissions • Download messages
Configuration	Configuration	<PROD/DEV/VAL>_SOAB2B_Configure	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 HSGBU 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 HSGBU 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 HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

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

    Example: `Create an Axway trading partner.`
14. In the **Description** field, enter more details for 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. 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**.
17. Select the appropriate values from the **Severity** and **Implementation Window** drop-downs.
18. Click the **Date Required By** field and select a value from the calendar.
19. 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.
20. Click **Choose file** to attach the XLS file that you have downloaded and filled-in.
21. 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 HSGBU 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 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.

- 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 HSGBU Customer Support Portal .
2. On the upper-right side of the screen, click **Switch to old portal**.

> **Note:**
>
> A new Oracle Health Sciences Support Cloud portal is currently rolled out, while the old portal is still available. Until the new portal is completely functional, all the information presented in this guide about the customer support portal is referring to the old portal.

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

    Example: `Create a trading engine node.`
14. In the **Description** field, enter more details for 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. 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**.
17. Select the appropriate values from the **Severity** and **Implementation Window** drop-downs.
18. Click the **Date Required By** field and select a value from the calendar.
19. 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 Axway gateway.

Transmit a report

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, respectively.

3. Click the **Transmit** button to transmit a report. The Transmit to Recipients dialog box is displayed.
4. Select the recipients of the report, as applicable from the **Available Recipients** list.
5. Select the method of transmission from **Method**, as applicable.
6. Enter remarks in Comments.
7. Click **Transmit**.
8. 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

8

Get support for Oracle Argus Cloud Service

Support is provided by your Cloud Service Delivery Manager, the HSGBU 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 HSGBU Customer Support Portal to access the Oracle Support Cloud
  Cloud customers can access HSGBU Support Cloud through the HSGBU Customer Support Portal.
- You can still use Oracle and third-party consulting services
  Implementation, post-go-live, and upgrade services are available through Oracle Health Sciences Consulting (HSC) 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 HSGBU 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 HSGBU 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 Access Manager (OAM) 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:

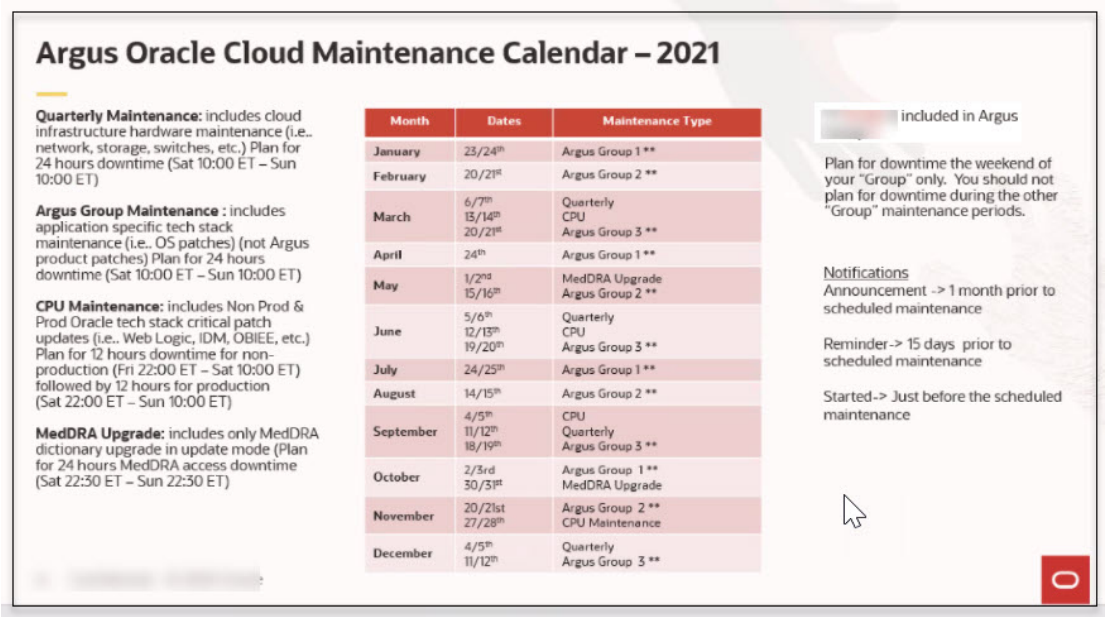
1. Open issue items, such as escalated tickets, patch information, and performance issues
2. Dashboard metrics that show the number of resolved support and change requests
3. Next steps: future and past releases
4. Argus Cloud Maintenance review.

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 HSGBU Cloud Support 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 HSGBU Customer Support Portal to access the Oracle Support Cloud

Cloud customers can access HSGBU Support Cloud through the HSGBU Customer Support Portal.

- Oracle Argus Cloud Service support overview
  The HSGBU Customer Support Portal provides 24x7 access to support.
- About support and change request features
  You can use the HSGBU 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 HSGBU 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 HSGBU Customer Support Portal
  You can access the HSGBU Support Cloud via the HSGBU Customer Support Portal.
- About the three types of access to the HSGBU Support Cloud
  HSGBU 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 HSGBU Support Cloud
  HSGBU 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 HSGBU 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 HSGBU 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 HSGBU 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 HSGBU 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 HSGBU Customer Support portal to access the HSGBU 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 HSGBU 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 HSGBU Support Cloud.

Log in to the HSGBU Customer Support Portal

You can access the HSGBU Support Cloud via the HSGBU 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 Health Sciences Support** button.

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

About the three types of access to the HSGBU Support Cloud

HSGBU 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.
Severity	Choose between: 1-Critical, 2-High, 3-Medium, 4-Low. **Note:** For Change Requests - 1-Critical not applicable.

Field	Description
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 HSGBU Support Cloud

HSGBU 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 HSGBU Support Cloud:

- A welcome email when your HSGBU 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 HSGBU 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 Health Sciences Consulting (HSC) and Oracle Partner Network (OPN) consultants.

If you are working with Oracle Health Sciences Consulting (HSC), 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.