Oracle® Argus Safety

Quickhelp for Administrators

Release 8.2

E97700-01

August 2018

Managing Access in Argus Safety

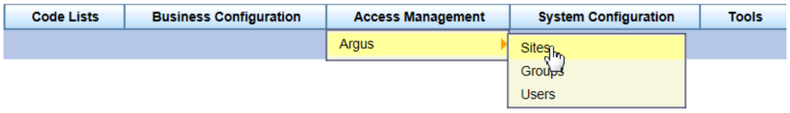
You can configure sites, groups, and users from the Argus Console. Each user must be assigned to at least one group in order to determine their security level. Each group is assigned a specific security level. This security level enables members of the group to view, modify, or restrict access rights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

To configure Argus Safety, begin by creating sites, groups, and users in the following order:

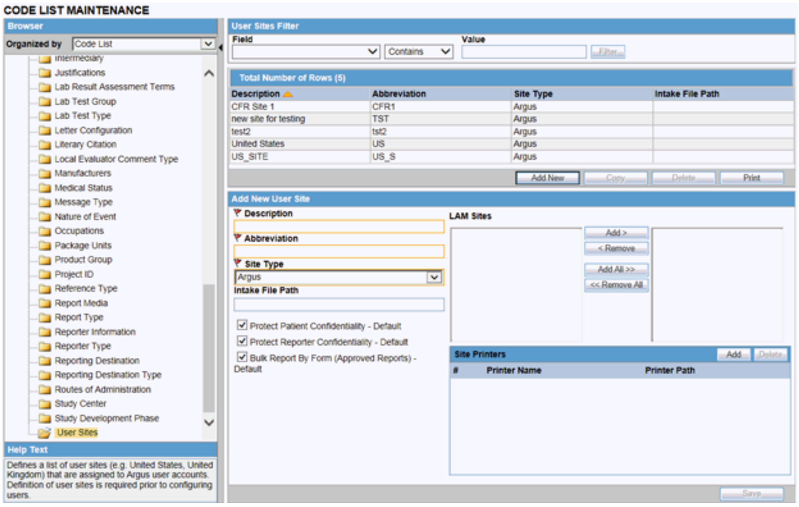
Adding User Sites

You must begin by configuring user sites as every user has to be assigned 1 site (and not more). Site information is also used to automatically assign case IDs.

1. Log into Argus Safety and navigate to the Argus Console.
2. Hover over the **Access Management** menu and click **Sites**.



The Code List Maintenance screen is displayed.



Defines a list of user sites (e.g. United States, United Kingdom) that are assigned to Argus user accounts. Definition of user sites is required prior to configuring users.

Total Number of Rows (5)

Description	Abbreviation	Site Type	Intake File Path
CFR Site 1	CFR1	Argus	
new site for testing	TST	Argus	
test2	tst2	Argus	
United States	US	Argus	
US_SITE	US_S	Argus	

Description

Abbreviation

Site Type: Argus

Intake File Path

☑ Protect Patient Confidentiality - Default

☑ Protect Reporter Confidentiality - Default

☑ Bulk Report By Form (Approved Reports) - Default

#	Printer Name	Printer Path

3. In the left pane, click **User Sites**.

   The list of users appears in the right pane under Total Number of Rows.

4. Click **Add New**.

   The Add New User Site tab is displayed.

5. Enter the required information (fields with a red flag are mandatory) and click **Save**.

Adding User Sites—Fields and Field Descriptions

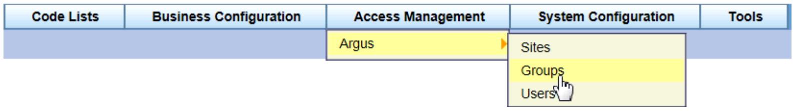
Field	Description
Description	Enter a description of the site.
Abbreviation	Enter an abbreviation (1-4 characters) of the site name.
Site Type	Select one of the options from the drop-down list: **Argus** or **LAM**. **Note:** Each Argus Safety user must be assigned to exactly one user site. You cannot change the site type from LAM to Central if the current central site has an association with a LAM site, the current site is associated with any user, or the current LAM site has any events assigned to it.
Protect Patient Confidentiality -Default	Select this checkbox to protect Patient Confidentiality for the site.
Protect Reporter Confidentiality - Default	Select this checkbox to protect Reporter Confidentiality for the site.
Bulk report By form (Approved reports) -Default	Select this checkbox to protect availability of the Bulk Reports by Form for the site.
LAM Sites	Add or Remove previously created LAM sites using the **Add >**, **Remove <**, **Add All>>**, and **Remove All <<** buttons.

Site Printers	Use the **Add** and **Delete** buttons to add/delete the Printer Name, and Printer Path. **Note:** The **Printer Name** is displayed in the application when referring to the printer. The name can have up to 20 characters. For the **Printer Path** textbox, 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 machine where Argus Safety Service is installed.

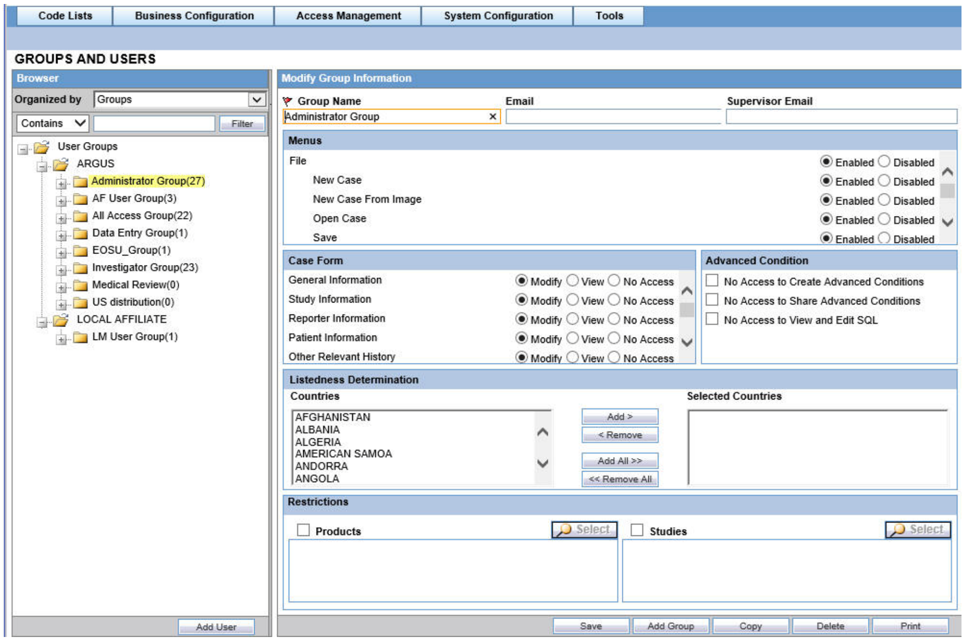
Adding User Groups

The Administrator can add and configure security levels for each work group. Radio buttons let you view the groups and assign access rights for the Case Form, Menu, Case and Report Workflow sections. If a user belongs to multiple groups, the access rights for the user will be the sum-total of the individual group access rights.

1. Hover over the **Access Management** menu and click **Groups**.



The Groups and Users screen is displayed.



GROUPS AND USERS

Organized by: Groups

Contains

- User Groups
  - ARGUS
    - Administrator Group(27)
    - AF User Group(3)
    - All Access Group(22)
    - Data Entry Group(1)
    - EOSU_Group(1)
    - Investigator Group(23)
    - Medical Review(0)
    - US distribution(0)
  - LOCAL AFFILIATE
    - LM User Group(1)

Group Name: Administrator Group

Email:

Supervisor Email:

Menus

File	● Enabled ○ Disabled
New Case	● Enabled ○ Disabled
New Case From Image	● Enabled ○ Disabled
Open Case	● Enabled ○ Disabled
Save	● Enabled ○ Disabled

Case Form

General Information	● Modify ○ View ○ No Access
Study Information	● Modify ○ View ○ No Access
Reporter Information	● Modify ○ View ○ No Access
Patient Information	● Modify ○ View ○ No Access
Other Relevant History	● Modify ○ View ○ No Access

Advanced Condition

□ No Access to Create Advanced Conditions
□ No Access to Share Advanced Conditions
□ No Access to View and Edit SQL

Listedness Determination

Countries

AFGHANISTAN
ALBANIA
ALGERIA
AMERICAN SAMOA
ANDORRA
ANGOLA

Selected Countries

Restrictions

□ Products

□ Studies

2. In the left pane, click **User Groups**.

3. Click **Add Group**.

4. Enter the required information (fields with a red flag are mandatory) and click **Save**.

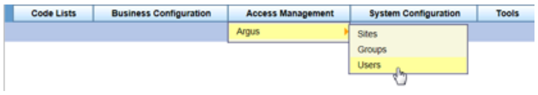
Configuring Users—Fields and Field Descriptions

Field / Control Name	Description
Group Name	Enter a group name. This should be a unique name associated with the group.
Email	Enter the email address, as applicable
Supervisor Email	Enter the supervisor's email address, as applicable.
Menus	
File/ New Case/New Case From Image/Open Case and so on	Select the Enable or Disable the options, as applicable.
Case Form	
General Information/Study Information/Reporter Information and so on	Select Modify, View, or No Access, as applicable.
Advanced Conditions	
No Access to Create Advanced Conditions	Select this checkbox if you do not want the group to have access to create advanced conditions.
No Access to Share Advanced Conditions	Select this checkbox if you do not want the group to have access to share advanced conditions.
No Access to View and Edit SQL	Select this checkbox if you do not want the group to have access to view and edit SQL.
Listedness Determination	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. Add or Remove countries using the **Add >**, **Remove <**, **Add All>>**, and **Remove All <<** buttons.
Restrictions -Products	Select the Products checkbox. Click **Add Product**, to open the Available Products dialog box. Select each product you want to add and click **OK**.
Restrictions -Studies	Select the Studies checkbox. Click **Add Study**, to open the Available Studies dialog box. Select each study you want to add and click **OK**.

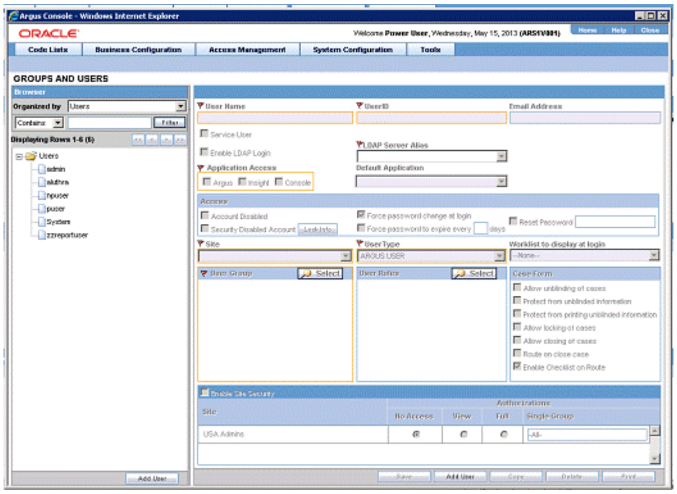
Adding Users

Ensure that you have provisioned users in IDM before you begin the following procedure.

1. Log into Argus Safety and navigate to the Argus Console.
2. Hover over the **Access Management** menu and click **Users**.



The Groups and Users screen is displayed.



3. In the left pane, click **Users**.

   The list of users appears in the right pane.

4. Click **Add New**. The fields in the right pane become editable.

5. Enter the details as needed and click **Save**.

Configuring Users—Fields and Field Descriptions

Field / Control Name	Description
User Name	Enter the full name.
User ID	Enter 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.
Application Access	Configure user access settings for Argus Console and Argus Safety. The default application access for the user can be selected from the list.
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.
LDAP Server Alias	Click on the drop-down arrow and select the LDAP server which is listed.
Access	Configure user access settings for Argus Safety. Select the following checkboxes, as applicable: Account Disabled Forcer Password change at login Security Disabled Account Force Password to expire every_ days Reset Password
Site	Assigns the user to a site. The values in this field are populated from the code list item User Sites.
User Group - Select	Attaches the user to pre-configured user groups.

Field / Control Name	Description
User Type	Select the type of user, such as, Argus J user from the drop-down list.
User Roles - Select	Attaches the user to pre-configured user roles such as Global Admin. By default, a Global Administrator role is granted only to an Administrator, who can grant/revoke this role to other Argus users. Such a user role must be assigned to users who need access to the Argus Global application. You can also select from other roles present within User Roles.
Enable site security	When this checkbox is checked, site-based data security is enabled for the user. If the box is not checked, the user has full access to data from all sites.
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.
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 the Administrator to re-activate the account at a later date.
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 login procedure will always fail the password validation to lock the user 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 into the system do not apply.
Allow unblinding of cases	Enables the user to unblind a study case. For example, a user without unblinding rights will not see the Study Drug field. A user with unblinding rights sees a yellow Unblind tag next to the Concentration of Product field, and the Broken by Sponsor option in the Blinding Status drop-down list is enabled.
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 closing of cases	Enables 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 checkbox is selected. If this checkbox 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.

Disabling a User in Argus Safety

1. Log into Argus Safety and navigate to the Argus Console.

2. Hover over the Access Management menu and click **Users**.

   The Groups and Users screen is displayed.

3. In the left pane, click **Users**.

   The list of users appears in the right pane.

4. In the Access tab, select **Account Disabled** and click **Save**.

Documentation Accessibility

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

Access to Oracle Support

Oracle customers 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.

Oracle Argus Safety Quickhelp for Administrators, Release 8.2
E97700-01