

# Oracle® Argus Safety

Quickhelp for Administrators

Release 8.1.1

E90675-01

September 2017

---

## Managing Access in Argus Safety

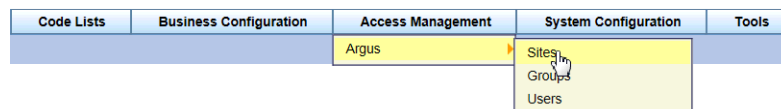
You can configure sites, groups, and users from the Argus Console. Each user must be assigned to at least one group in order to determine their security level. Each group is assigned a specific security level. This security level enables members of the group to view, modify, or restrict access rights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

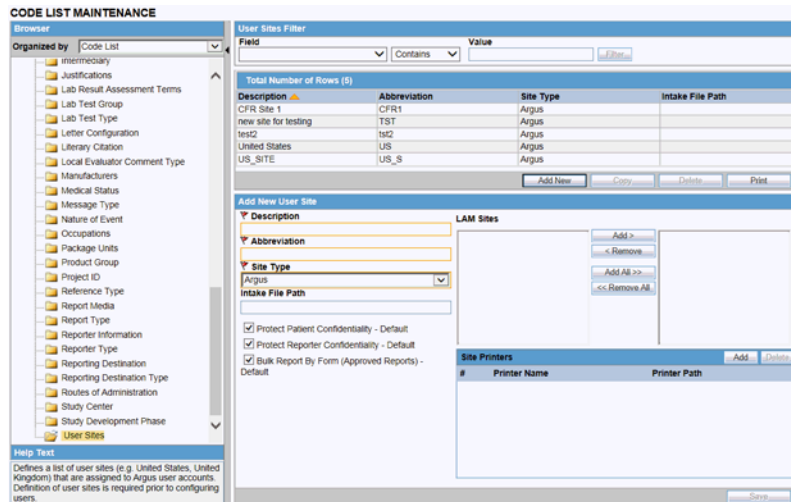
### Adding User Sites

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.



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: <b>Argus</b> or <b>LAM</b> . <b>Note:</b> 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 <b>Add &gt;</b> , <b>Remove &lt;</b> , <b>Add All &gt;&gt;</b> , and <b>Remove All &lt;&lt;</b> buttons.

## Site Printers

Use the **Add** and **Delete** buttons to add/delete the Printer Name, and Printer Path.

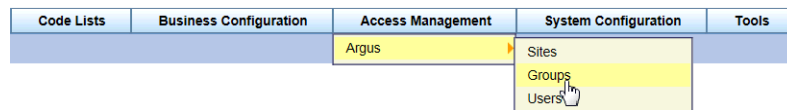
**Note:** The **Printer Name** is displayed in the application when referring to the printer. The name can have up to 20 characters.

For the **Printer Path** textbox, enter the full path of the printer on the network. This path name can have upto 256 characters. The specified path should be accessible from the machine where Argus Safety Service is installed.

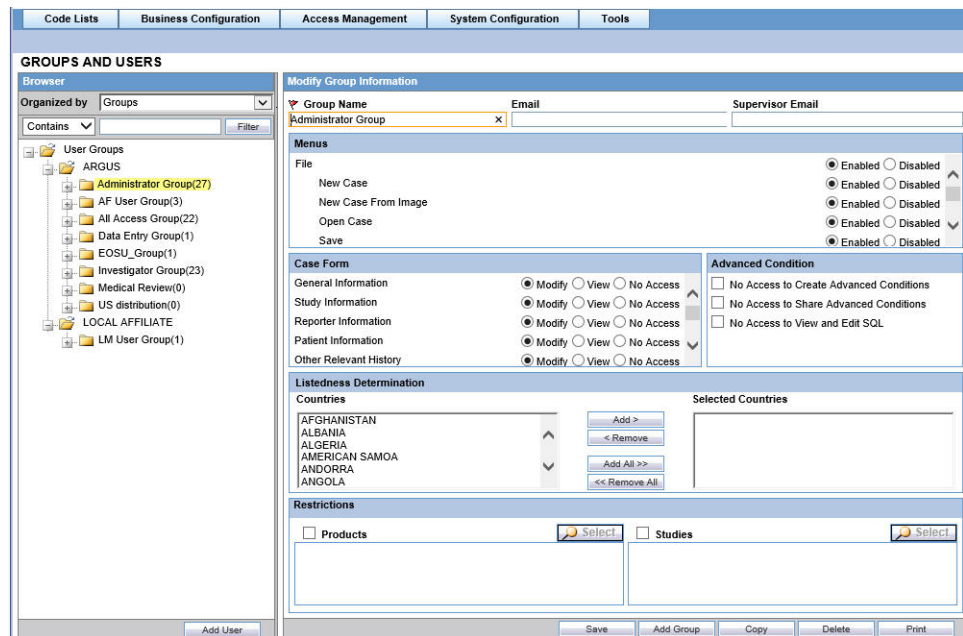
## Adding User Groups

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.



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**.

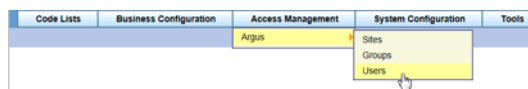
## Configuring Users—Fields and Field Descriptions

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.
<b>Menus</b>	
File/ New Case/New Case From Image/Open Case and so on	Select the Enable or Disable the options, as applicable.
<b>Case Form</b>	
General Information/Study Information/Reporter Information and so on	Select Modify, View, or No Access, as applicable.
<b>Advanced Conditions</b>	
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 <b>Add &gt;</b> , <b>Remove &lt;</b> , <b>Add All&gt;&gt;</b> , and <b>Remove All &lt;&lt;</b> buttons.
Restrictions -Products	Select the Products checkbox. Click <b>Add Product</b> , to open the Available Products dialog box. Select each product you want to add and click <b>OK</b> .
Restrictions -Studies	Select the Studies checkbox. Click <b>Add Study</b> , to open the Available Studies dialog box. Select each study you want to add and click <b>OK</b> .

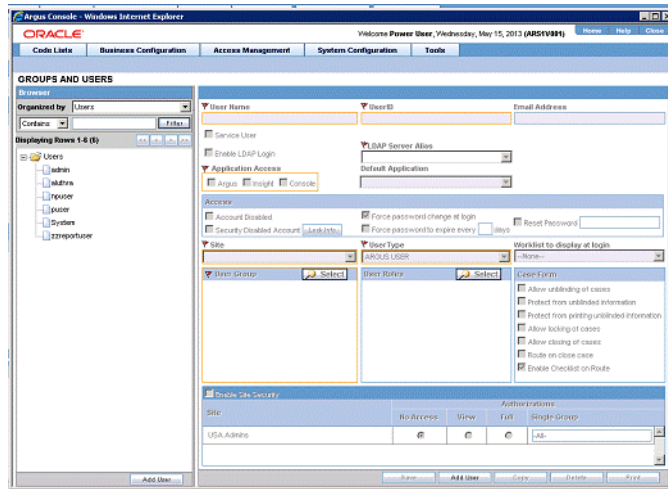
## Adding Users

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 8.1.1  
E90675-01

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

**U.S. GOVERNMENT END USERS:** Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

