



PS ADMINISTRATION

RELEASE 10.02.00

IMPLEMENTATION GUIDE

PUBLICATION PSAC-IN002C-EN-E-SEPTEMBER-2021
Supersedes publication PSAC-IN002B-EN-E



Contact Rockwell See contact information provided in your maintenance contract.

Copyright Notice © 2021 Rockwell Automation Technologies, Inc. All rights reserved.
This document and any accompanying Rockwell Software products are copyrighted by Rockwell Automation Technologies, Inc. Any reproduction and/or distribution without prior written consent from Rockwell Automation Technologies, Inc. is strictly prohibited. Please refer to the license agreement for details.

Trademark Notices FactoryTalk, PharmaSuite, Rockwell Automation, Rockwell Software, and the Rockwell Software logo are registered trademarks of Rockwell Automation, Inc.

The following logos and products are trademarks of Rockwell Automation, Inc.:

FactoryTalk Shop Operations Server, FactoryTalk ProductionCentre, FactoryTalk Administration Console, FactoryTalk Automation Platform, and FactoryTalk Security.

Operational Data Store, ODS, Plant Operations, Process Designer, Shop Operations, Rockwell Software CPGSuite, and Rockwell Software AutoSuite.

Other Trademarks ActiveX, Microsoft, Microsoft Access, SQL Server, Visual Basic, Visual C++, Visual SourceSafe, Windows, Windows 7 Professional, Windows 10, Windows Server 2008, Windows Server 2012, and Windows Server 2016 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

ControlNet is a registered trademark of ControlNet International.

DeviceNet is a trademark of the Open DeviceNet Vendor Association, Inc. (ODVA).

Ethernet is a registered trademark of Digital Equipment Corporation, Intel, and Xerox Corporation.

OLE for Process Control (OPC) is a registered trademark of the OPC Foundation.

Oracle, SQL*Net, and SQL*Plus are registered trademarks of Oracle Corporation.

All other trademarks are the property of their respective holders and are hereby acknowledged.

Warranty This product is warranted in accordance with the product license. The product's performance may be affected by system configuration, the application being performed, operator control, maintenance, and other related factors. Rockwell Automation is not responsible for these intervening factors. The instructions in this document do not cover all the details or variations in the equipment, procedure, or process described, nor do they provide directions for meeting every possible contingency during installation, operation, or maintenance. This product's implementation may vary among users.

This document is current as of the time of release of the product; however, the accompanying software may have changed since the release. Rockwell Automation, Inc. reserves the right to change any information contained in this document or the software at any time without prior notice. It is your responsibility to obtain the most current information available from Rockwell when installing or using this product.

-
-
- PS Administration - Implementation Guide
-
-

Chapter 1	Read Me First.....	1
	Audience and Expectations	1
	Typographical Conventions	2
	Related Documentation	3
	Solutions and Technical Support.....	4
	Administration User	4
Chapter 2	PS Administration Overview	5
	Users, User Groups, and Access Privileges	6
	Users and User Groups Overview (PharmaSuite).....	7
	Lists	7
	Applications	7
Chapter 3	Installing PS Administration	9
	Prerequisites	9
	Install PS Administration	10
	Access PS Administration.....	14
	Session Timeout	14
	Navigate the UI	16
	Uninstall PS Administration.....	16
Chapter 4	Performing Administrative Tasks for PharmaSuite	17
	Manage Users.....	17
	Create User Filters	19
	Add/Edit Users	23
	Assign Start Forms to Users.....	26
	Assign User Groups to Users	27

Appendix A Default Privileges and User Groups (PS Administration).....	71
Privileges (PS Administration).....	71
User Groups (PS Administration).....	74

Figure 1: PS Administration Welcome Screen	10
Figure 2: License Agreement Screen.....	11
Figure 3: Select Installation Directory Screen	11
Figure 4: Pre-Installation Summary Screen.....	12
Figure 5: Progress Screen.....	12
Figure 6: Install Complete	13
Figure 7: PharmaSuite webstart page	14
Figure 8: Session Timed Out.....	14
Figure 9: Session Expiration.....	15
Figure 10: Example Page Layout	16
Figure 11: Users editor	18
Figure 12: Create User filters.....	19
Figure 13: Add User dialog	23
Figure 14: Edit User dialog	25
Figure 15: Assign Start Form dialog.....	26
Figure 16: Assign User groups dialog.....	27
Figure 17: Change Password dialog	28
Figure 18: Change Password dialog	29
Figure 19: User Groups editor.....	31
Figure 20: Create User Group filters.....	32
Figure 21: Add User Group dialog	34
Figure 22: Assign Access Privileges dialog	36
Figure 23: Access Privileges editor.....	40
Figure 24: Create Access Privilege filters.....	41
Figure 25: Add Access Privilege dialog	44
Figure 26: Edit Access Privilege dialog.....	50
Figure 27: Define Signature dialog.....	52

Figure 28: Signature execution with a signature dialog box for a single signature.....	56
Figure 29: Signature execution with a signature dialog box for a single signature with a pre-defined comment.....	56
Figure 30: Signature execution with a signature dialog box for a double signature to support witness role.....	57
Figure 31: Signature execution with a warning dialog box	57
Figure 32: Signature execution with an error dialog box	57
Figure 33: Assign Performer User Groups dialog.....	58
Figure 34: Applications editor	60
Figure 35: Add Application dialog.....	61
Figure 36: Assign Stations dialog	64
Figure 37: Add Object Property dialog.....	66
Figure 38: Edit Object Property dialog.....	67
Figure 39: Assign User Groups dialog	69

Read Me First

The following sections contain basic information, which will support you in using this guide.

Audience and Expectations

This guide is intended for experienced professionals who understand their company's business needs as well as the technical terms and software dependencies described in this guide.

This guide provides information on installing, configuring, and using PS Administration. Installation should be performed by an administration user (page [4](#)). This guide assumes that the supporting network equipment and software are installed and does not provide installation instructions for related components, like database software or internet connections.

Typographical Conventions

This documentation uses typographical conventions to enhance the readability of the information it presents. The following kinds of formatting indicate specific information:

Bold typeface	Designates user interface texts, such as <ul style="list-style-type: none">■ window and dialog titles■ workflow and widget names■ menu functions■ panel and tab titles■ box labels■ object properties and their values (e.g., status).
[Text in square brackets]	Designates button names.
<i>Italic typeface</i>	Designates technical background information, such as <ul style="list-style-type: none">■ path, folder, and file names■ methods■ classes.
CAPITALS	Designate keyboard-related information, such as <ul style="list-style-type: none">■ key names■ keyboard shortcuts.
Monospaced typeface	Designates code examples.

Related Documentation

In addition to this guide, you should review the following guides:

- [01] *FTPC Deployment Manager Administration Guide* for instructions on installing and deploying PS Administration.
- [02] *FTPC Modular Framework WebSDK Developer's Guide* for basic instructions on the extension mechanism.
- [03] *FTPC Modular Framework WebSDK User's Guide* for documentation on installing and using Modular Framework WebSDK and information on the editors provided with WebSDK.
- [04] *FTPC Plant Operations Server Installation Guide* for instructions on installing and configuring your FTPC application server and clients.
- [05] *PharmaSuite Technical Manual Configuration & Extension - Volume 2* for information on system functionalities such as field attributes, version management, services, audit trail, etc.
- [06] *PharmaSuite Technical Manual Configuration & Extension - Volume 4* for information about the methods for logging and debugging, maintaining configuration keys, and a list of the configuration keys available in PharmaSuite.
- [07] *FTPC Supported Platforms Guide* for a list of required third-party applications and their supported versions.
- [08] *PharmaSuite Supported Platforms Guide* for a list of required third-party applications and their supported versions.
- [09] *FTPC Open Source License Agreements Guide* to view the license agreements for the open source software packages provided with PS Administration.
- [10] *PharmaSuite Release Notes* for latest information on PharmaSuite and PS Administration.
- [11] *PharmaSuite Technical Manual Installation* for information on installing PharmaSuite.
- [12] *PharmaSuite Quality Certificate* for the exact build numbers of the PharmaSuite release.
- [13] *Process Designer and Object Help* for information on FactoryTalk ProductionCentre objects.
- [14] *FTPC Administrator User's Guide* for information on configuring FactoryTalk ProductionCentre features using FTPC Administrator.

Solutions and Technical Support

To contact Technical Support for PharmaSuite, call (440) 646-3434.
Choose technical support for FactoryTalk ProductionCentre from the phone menu.

Administration User

To log into PS Administration, you must be an administration user. A default administration user is created during the FactoryTalk ProductionCentre installation. The default user name and password are:

user name: *admin*

password: *<password>*

After installation, we recommend creating a backup administration user.

IMPORTANT

The **admin** administration user belongs to the **PlantOpsAdmin** user group. By default, this user group has all system privileges (without visible assignments). If the **admin** administration user shall not have all system privileges, a different user must be created and used after the installation instead of the **admin** administration user. This new user must be added to the **PSACFunctionalAdmin** and **PSACUserAdmin** user groups.

Do not change the user name **admin**.

PS Administration Overview

PS Administration is the PharmaSuite client for the administration of database objects, such as access privileges, lists, applications, users, or user groups.

The client provides set and performance editors that allow you perform all the administrative functions for your application.

PharmaSuite provides client-side access control mechanisms. This means that some parts and functionalities of the system can only be accessed by users with suitable access rights. To make use of these mechanisms and grant or deny access to the system, users, user groups, and access rights have to be defined and assigned to each other. Each of these objects can be configured to match custom user requirements, including information about who is allowed to access a certain feature.

TIP

We highly recommend to handle the expiration and change of passwords with care. An operational procedure (SOP) needs to be in place to ensure that

- a password does not expire while a user is logged into any PharmaSuite client and
- a password is not changed while a user is logged into any PharmaSuite client.

We highly recommend to handle the expiration of users with care. An operational procedure (SOP) needs to be in place to ensure that

- a user does not expire while he is logged into any PharmaSuite client.

Users, User Groups, and Access Privileges

Each person accessing the system has to be represented by a **User** object that uniquely identifies the user. Each user has a password to allow authentication.

Depending on his or her role in the production process, a user can belong to several user groups. User groups represent high-level groups of functionality a user is allowed to perform. The assignment between users and user groups can either be done by assigning users to a user group or the other way round by assigning user groups to a user.

A user group can have several access privileges, which are explicitly defined for the user group. Users inherit the access privileges of the user groups to which they are assigned. Access privileges refer to applications as a whole or to system functions in a very granular sense and are thus linked to the launch of an application or to interaction elements on the user interface, such as Production Management Client task pane entries, menu functions, or toolbar actions.

For example, a user may have the right to perform a status transition because he is a member of the **Qualified Person** group. He may not have the right to execute batch processing, because he does not belong to the **DispensingOperatorGroup** group. The assignment between user groups and access privileges is created by assigning user groups to access privileges or the other way round by assigning access privileges to user groups. The assignment of access privileges to user groups is only available in PS Administration and not in Process Designer.

Each PharmaSuite user must be assigned to the **MinimalAccess** group to be able to start PharmaSuite applications. Other groups may be required, depending on the actions the user is to perform.

TIP

PharmaSuite has a default set of user groups and access privileges, which can be viewed and accessed in PS Administration. During the initial configuration of the system the default set can be adapted to specific customer requirements by defining new privileges, groups, and assignments between groups and privileges, as well as assignments between privileges and functions (i.e. GUI elements). The latter can be achieved, for example, by modifying the XML configurations of the appropriate Production Management use cases.

In order to correctly add new users to the PharmaSuite system, the mapping of privileges to user groups and of user groups to user roles must be available.

Users that are no longer needed cannot be deleted once they have been used, thereby supporting uniqueness over time.

For an overview of the available PharmaSuite access privileges, please refer to *"Managing Electronic Signatures and Access Rights"* in *PharmaSuite Technical Manual Configuration & Extension - Volume 2*, [05] (page 3).

Users and User Groups Overview (PharmaSuite)

The following table provides an overview of the default set of PharmaSuite users and user groups:

User group	User		
	pecadmin	pmcadmin	shopopsserver
Application Administrator	Yes	Yes	No
DispensingOperatorGroup	Yes	No	No
LogisticalOperatorGroup	Yes	No	No
Master Data Administrator	No	Yes	No
MinimalAccess	Yes	Yes	Yes
Qualified Person	Yes	Yes	No
Recipe Author	No	Yes	No
Supervisor (Process Order)	Yes	No	No
Supervisor (Shop Floor)	Yes	No	No
WIPOperatorGroup	Yes	No	No
Workflow Author	No	Yes	No

Lists

Lists store frequently used list options as a single object. Ordered lists are created once and are then usable in other sections of editors. Use cases include lists of report designs, checks, etc.

Applications

For PharmaSuite, an **Application** object serves primarily as a place to define and manage configuration items (keys). Configuration items are items that are referenced: Instead of hard-coding a value, the value is entered in the **Application** object and only referenced in the code.

- Example: The system is delivered with a standard logo displayed in the Production Execution Client. By overwriting the configuration key referencing the standard logo, a customer logo can be referenced and made visible instead, just by configuration.
- Applications can be added to other applications in a hierarchy, to allow for project-specific and site-specific property values that override configurations delivered with the product.

- To apply the configurations of an application, resources such as users, user groups, or stations are assigned to it. A configuration that is desired for the system as a whole - the typical PharmaSuite use-case - for example to activate a customer logo, requires all stations to be assigned to the application.

TIP

For general information about application configurations, hierarchical configurations in PharmaSuite, the dynamic change of a configuration, and the characteristics of configuration keys, please refer to "*Managing Configurations*" in *PharmaSuite Technical Manual Configuration & Extension - Volume 4*, [06] (page 3).

For an overview of the available PharmaSuite configuration keys, please refer to "*Configuration Keys of PharmaSuite*" in *PharmaSuite Technical Manual Configuration & Extension - Volume 4*, [06] (page 3).

Installing PS Administration

PS Administration is provided as an executable file. The *sw-ApplicationSolutionsModules-PharmaSuiteAdministration-<app_server>-<version>.<build>.exe* file provides the zip files for PS Administration.

TIP

Not included are the Modular Framework WebSDK and Deployment Manager files, which are needed to install PS Administration, see section "Prerequisites" (page 9).

Please note that the PS Administration version/build number displayed by your installer may be higher than the one shown on the screen captures in this manual. For the exact build number valid for the PS Administration release you are about to install, refer to "Released Product Information" in the *PharmaSuite Quality Certificate* of this release.

Prerequisites

Before installing PS Administration, you must have the following in place:

- A compatible version of FTPC and its related components (network connections, databases, etc.) have been installed. See the *FTPC Plant Operations Server Installation Guide* for your JBoss application server for instructions, [04] (page 3). See the *FTPC Supported Platforms Guide* for a list of required third-party applications and their supported versions, [07] (page 3).
- A compatible version of PharmaSuite has been installed. See the *PharmaSuite Technical Manual Installation* for instructions, [11] (page 3). See the *PharmaSuite Supported Platforms Guide* for a list of required third-party applications and their supported versions, [08] (page 3).
- Installer for the Modular Framework WebSDK products (which includes the extensions as well as the Deployment Manager files). For details on the compatibility, see *PharmaSuite Supported Platforms Guide*, [08] (page 3).
- You have the user name and password of the currently logged-on administrative user of the machine housing the installation.
- Your screen resolution is set to 1280 * 1024 or higher.

Install PS Administration

To install PS Administration, perform the following steps:

1. Double-click the *sw-ApplicationSolutionsModules-PharmaSuiteAdministration-<app_server>-<version>.<build>.exe* file.
2. On the **Welcome** screen, click [Next].

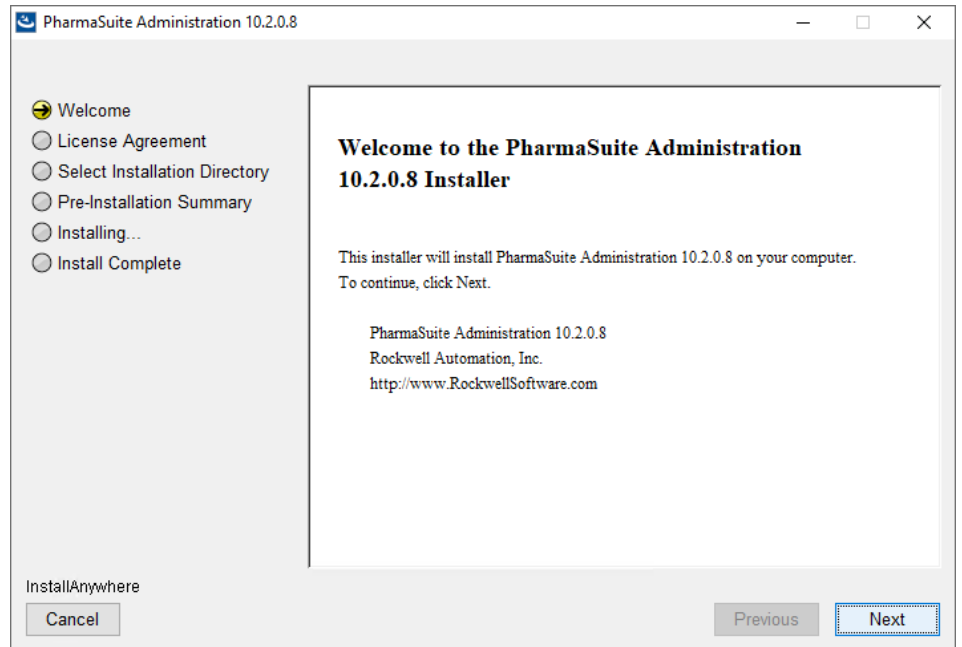


Figure 1: PS Administration Welcome Screen

3. On the **License Agreement** screen, accept the license agreement, and then click [Next].

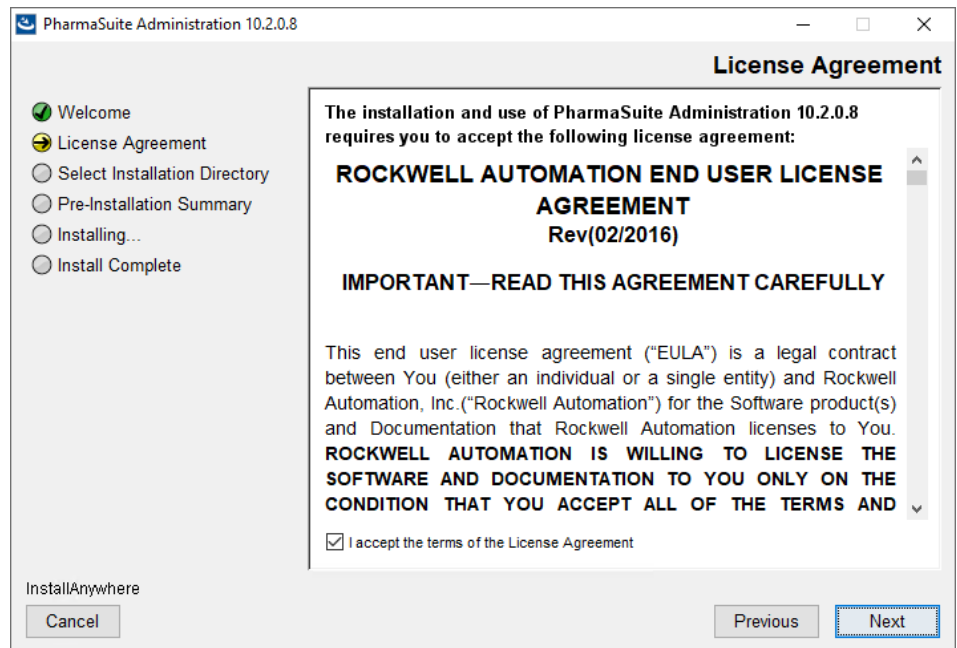


Figure 2: License Agreement Screen

4. On the **Select Installation Directory** screen, specify the folder to which you want the PS Administration zip files to be placed and click [Next]. The default directory is *C:\Rockwell\PSAdministration*.

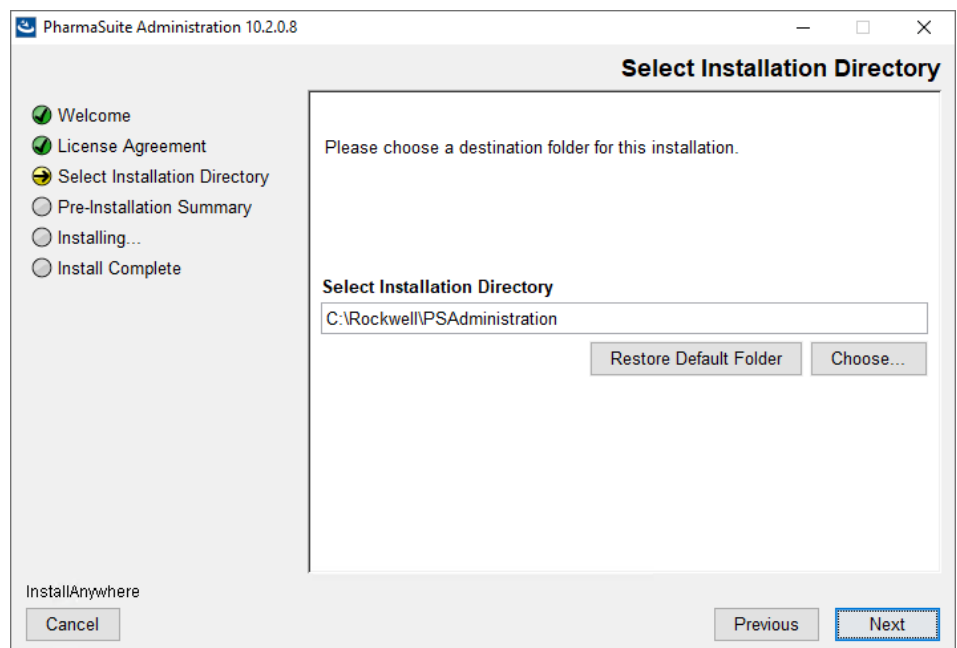


Figure 3: Select Installation Directory Screen

5. Review the information displayed in the **Pre-installation Summary** screen to ensure that you have the correct location defined and then click [Install] to begin the installation.

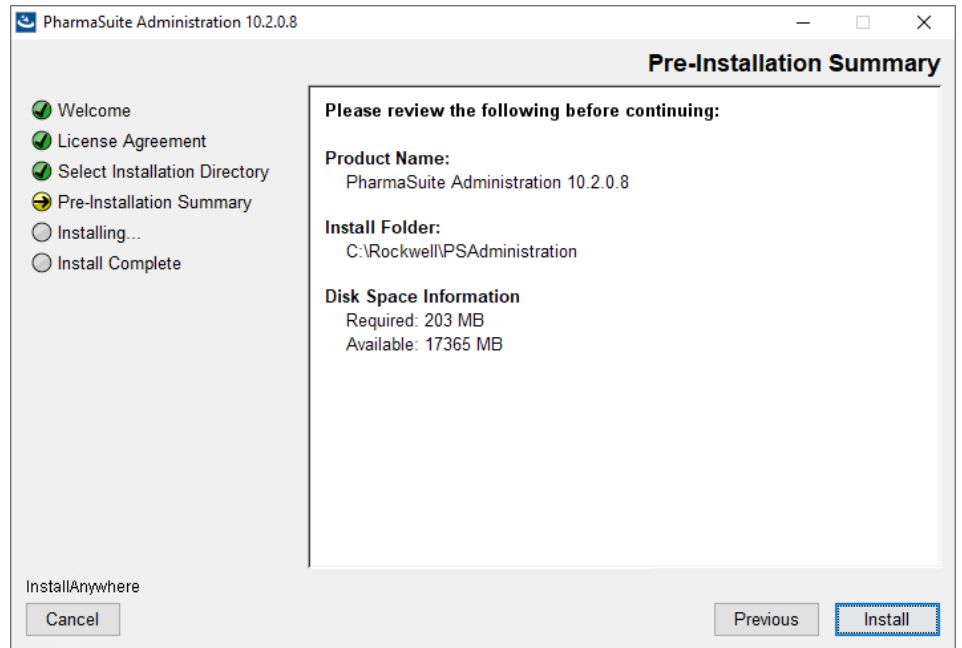


Figure 4: Pre-Installation Summary Screen

A **Progress** screen allows you to track the installation progress.

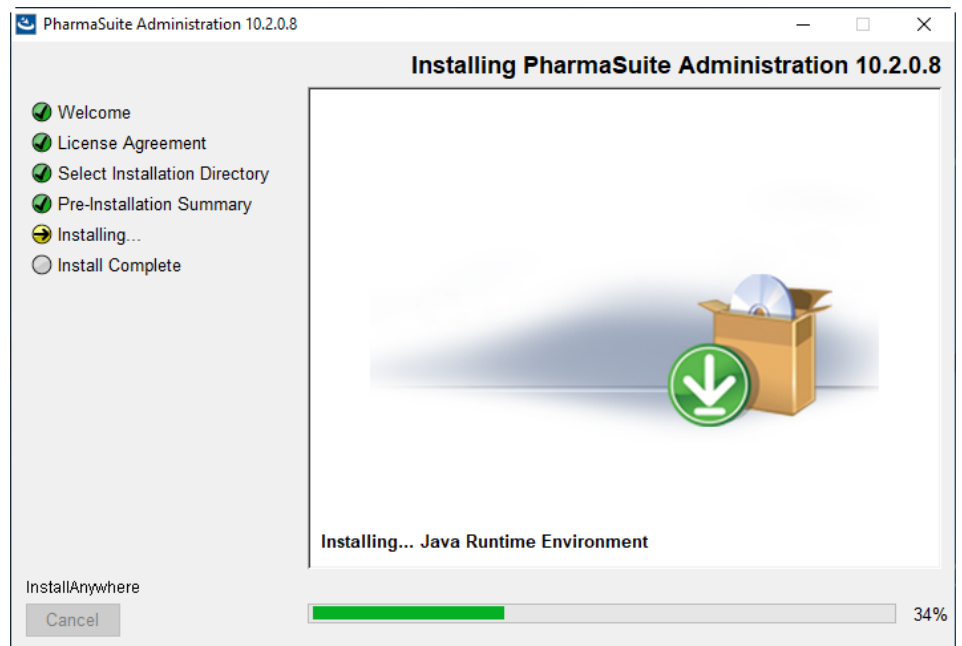


Figure 5: Progress Screen

6. Once the installation is completed, click [Done] to close the **Install Complete** dialog.

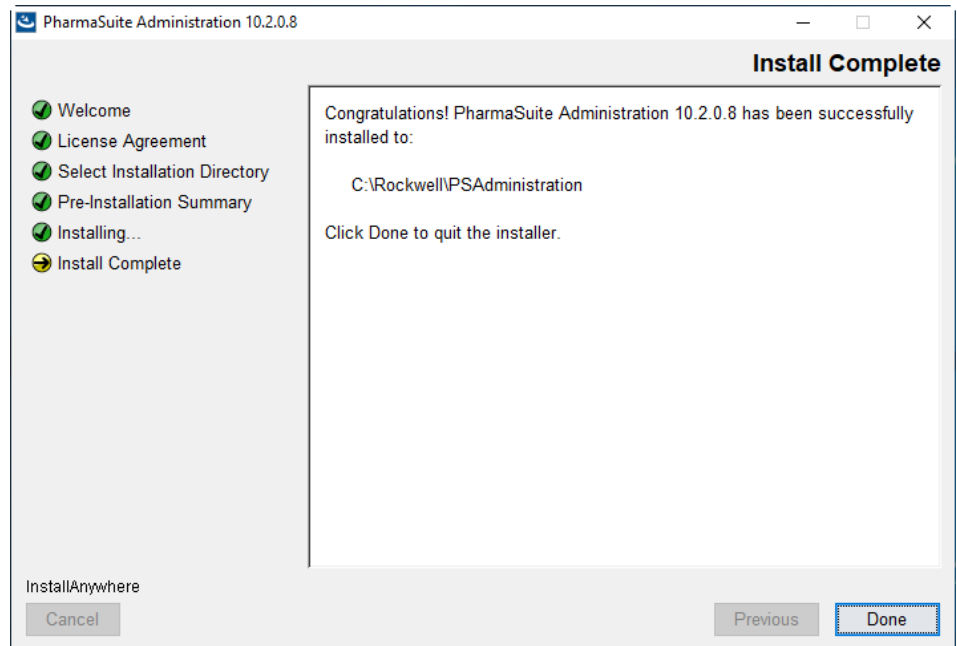


Figure 6: Install Complete

7. The target installation location contains the PS Administration zip files you need in the subsequent steps.
8. Use Deployment Manager to install and deploy FTPC Modular Framework WebSDK, PS Administration, and their extensions. See the *FTPC Deployment Manager Administration Guide* for instructions, [01] (page 3).

TIP

Please note that when running Deployment Manager for installation directly on the server that also runs JBoss, you need to temporarily rename the *jboss-cli.xml* file to something else.

The files should be installed in the following order:

1. FTPCApps-module-<app_server>.zip
2. ModularFramework_Extensions.zip
3. PSAdminClient-module.zip

Deployment Manager is also used to uninstall and upgrade PS Administration.

TIP

Before using PS Administration, we recommend keeping a list of changes that have been made to your installation and environment so that these changes can be quickly reapplied during a reinstallation or upgrade.

Access PS Administration

To access PS Administration, run the PharmaSuite webstart page in a browser window and select the application.

To access the UI, the logged-in user must be a member of the **PlantOpsOperator** user group.

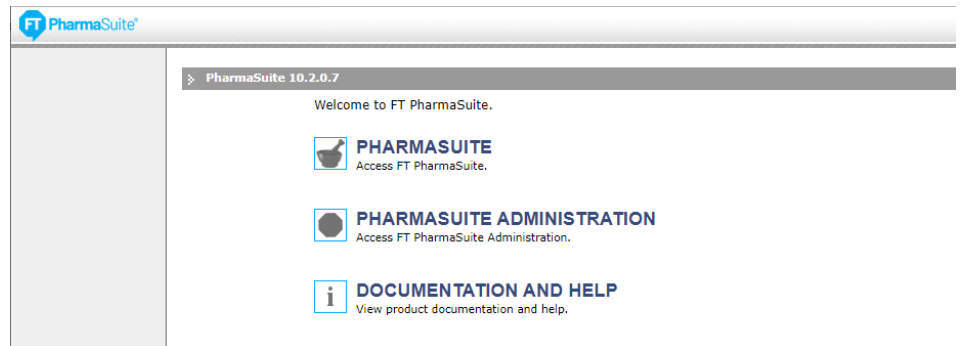


Figure 7: PharmaSuite webstart page

Enter *admin/<password>* as the user name and password, and then click [Login].

Session Timeout

The PS Administration UI has the following timeout behavior:

1. If the system detects that the session has been inactive for 20 minutes, the following message displays:
Your session is inactive and will be closed in 2 minute(s).
2. If the session remains inactive for another two minutes, the following message displays:
Your session timed out and you have been logged out.

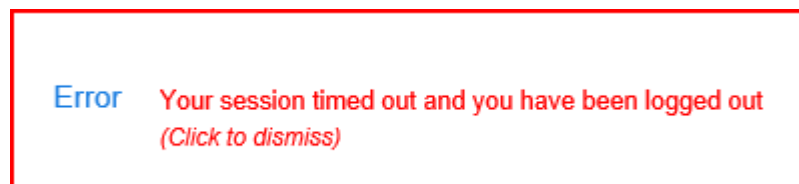


Figure 8: Session Timed Out

At this point, click on the error message to close it. You will be prompted to log on to the session again.

3. If there is still no activity for an additional 30 minutes (i.e., the user does not click on the error message), the session will eventually expire, and a message displays at the top of the UI informing the user to either press ESC or click on the message to restart. At this point, the login dialog is no longer effective. The user must refresh the browser, hit ESC, or click on the error message at the top of the UI to refresh.

TIP

The default 20-minute idle time limit and two-minute grace period can be modified by editing the *idleTimeMinutes* and *idleGracePeriod* parameters in the *web.xml* file, which is located in *FTPCApps.war\WEB-INF*.

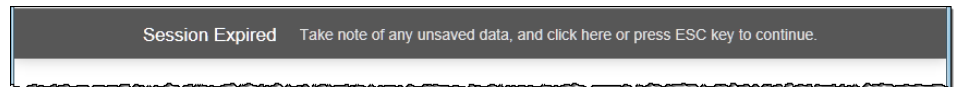


Figure 9: Session Expiration

Navigate the UI

PS Administration pages follow a consistent theme:

- The **navigation bar** that is displayed on each page displays the logged-in user and contains links to the language selection (only available if more than one language is installed), logoff link and the About dialog. Clicking [About] will display system-related information, such as the current system version and build and database-related information.
- The **editor list** contains a list of editors for the current interface. The editor list can be collapsed or expanded by clicking the arrow located at the top-left corner of the page.
- The **editor view** displays details of the selected editor.

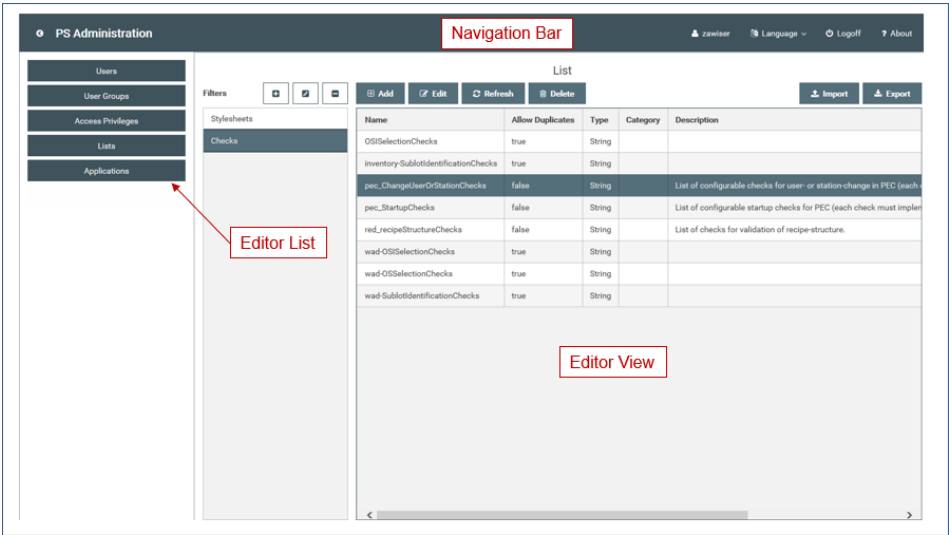


Figure 10: Example Page Layout

Uninstall PS Administration

To uninstall PS Administration, perform the following steps:

1. Go to the *Uninstall* directory of your PS Administration installation directory. This is located at *C:\Rockwell\PSAdministration\Uninstall* by default.
2. Double-click *Uninstaller.exe*.
3. On the **Welcome** screen, click [Uninstall].
4. When the uninstallation is complete, click [Done].

Performing Administrative Tasks for PharmaSuite

PS Administration provides editors that allow you to perform the following administrative tasks for PharmaSuite:

- **Manage Users** (page [17](#))
For details on managing users not targeted for being used with PharmaSuite, please refer to "*Manage Users*" and "*Change Profile Information*" in the *FTPC Modular Framework WebSDK User's Guide*, [03] (page [3](#)).
- **Manage User Groups** (page [31](#))
For details on managing user groups not targeted for being used with PharmaSuite, please refer to "*Manage User Groups*" in the *FTPC Modular Framework WebSDK User's Guide*, [03] (page [3](#)).
- **Manage Access Privileges** (page [38](#))
- **Manage Lists**
For details on managing lists, please refer to "*Manage Lists*" in the *FTPC Modular Framework WebSDK User's Guide*, [03] (page [3](#)).
- **Manage Applications** (page [59](#))

Manage Users

Click [Users] to display a list of available users. To view the **Users** editor, the logged-in user must have the *PSAC_viewUser* privilege. Click [Refresh] to refresh the list of users. A default administrative user with the user name/password *admin/<password>* is provided for you. This user cannot be disabled.

You can import and export the data and configurations of users via .xlsx spreadsheet. To do so, click [Import] or [Export], respectively. The logged-in user must have the *PSAC_importUser* and *PSAC_exportUser* privileges, respectively. For details on importing and exporting configurations, please refer to "*Import/Export Configurations*" in the *FTPC Modular Framework WebSDK User's Guide*, [03] (page [3](#)).

TIP

To import a user, the following prerequisites must be fulfilled:

- A name must be defined.
- The parameter values assigned to the user must be available in the target system.
- A user for whom a parameter is to be updated must be available in the target system.
- The user groups assigned to the user must be available in the target system.
- The start form assigned to the user must be available in the target system.

IMPORTANT

When a user is exported, his/her status (Enabled/Disabled) is exported in the localized version. For this reason, users can only be imported to the same locale that was used during export and the terms used for the status must be identical.

Filters

Filter 1

Filter 2

Filter 3

Filter 4

Filter 5

J Filter

Users

Add

Edit

Refresh

Enable User

Change Password

Assign Start Form

Import

Export

User Name	First Name	Last Name	Description	User Expiration	Email	Status	Password Expiration	Start Form Name
JSmith	Jonathan	Smith		Dec 31, 2099 12:00 AM		Enabled	Dec 31, 2018 12:00 AM	ApplicationStart_DataManager
Jdoe09	John	Doe		Dec 31, 9999 12:00 AM		Disabled	Dec 31, 9999 12:00 AM	ApplicationStart_ProductionManagementClient

Assign User Groups

User Group Name	Description
Master Data Administrator	
MinimalAccess	Every PharmaSuite user should be a member of this group
PlantOpsOperator	PlantOps Operators

Figure 11: Users editor

Create User Filters

Creating a filter provides a method for you to selectively display all previously created users. To create filters, the logged-in user must have the *PSAC_viewUser* privilege.

To create a new filter, proceed as follows:

1. Click the **Add Filter** icon.

The system displays the **Create Filter** dialog.

The 'Create Filter' dialog box is shown with the following configuration:

- Filter Owner:** Global
- Filter *:** Users (starting with M)
- User Name:** Starts With, M
- First Name:** Any
- Last Name:** Any
- Description:** Any
- User Expiration:** Any
- Email:** Any
- Status:** Equals, ☒ Enabled, ☐ Disabled
- Password Expiration:** Any
- Sort by:** User Name, Ascending

Buttons: Save, Cancel

Figure 12: Create User filters

2. Define the following properties:

TIP

To enter multiple string criteria, type them all out and use commas as separators.

■ **Filter Owner**

Select one of the following filter criteria from the drop-down menu.

■ **Global (default):** All users can apply the created filter. To add, edit, or delete a global filter, a user must have the *editGlobalFilter* access privilege.

■ **Current User:** This is a user-specific filter. It is only visible for the user who has created the filter and can thus only be applied, edited, or deleted by this user.

■ **Filter**

Specifies the name of the filter. The name is a mandatory property.

■ **User Name**

Select one of the following conditions and then enter a complete or partial user name by which to filter, if required.

■ Any (default)

■ Contains

■ Equals

■ Starts With

■ **First name**

Select one of the following conditions and then enter a complete or partial first name by which to filter, if required.

■ Any (default)

■ Contains

■ Equals

■ Starts With

■ **Last name**

Select one of the following conditions and then enter a complete or partial last name by which to filter, if required.

■ Any (default)

■ Contains

■ Equals

■ Starts With

■ Description

Select one of the following conditions and then enter a complete or partial description by which to filter, if required.

- Any (default)
- Contains
- Equals
- Starts With

■ User Expiration

Select one of the following conditions and then select an expiry date from the calendar widget by which to filter, if required.

- Any (default)
- Before (exclusive)
- After (inclusive)

■ Email

Select one of the following conditions and then enter a complete or partial email address by which to filter, if required.

- Any (default)
- Contains
- Equals
- Starts With

■ Status

Select one of the following conditions and then select a status by which to filter, if required. The available statuses are **Enabled** and **Disabled**.

- Any (default)
- Equals

■ Password Expiration

Select one of the following conditions and then select an expiry date from the calendar widget by which to filter, if required.

- Any (default)
- Before (exclusive)
- After (inclusive)

■ **Sort by**

Select one of the available filter criteria (**User Name** (default), **First Name**, **Last Name**, **Description**, **User Expiration**, **Email**, **Status**, **Password Expiration**) and then the sort order that will be applied to the list of the filter results, if required.

■ Ascending (default)

■ Descending

3. When you have completed your data entry, you can

■ either click [Save] to close the dialog and apply the new filter

■ or click [Cancel] to close the dialog without saving the entered data.

To edit a filter, proceed as follows:

1. Select the filter you want to change.

2. Click the **Edit Filter** icon.

TIP

Please note that **Global** filters can only be changed by users who have the *editGlobalFilter* access privilege.

3. Make your changes and

■ either click [Save] to apply the changed filter

■ or click [Cancel] to retain the old filter without changes.

To delete a filter, proceed as follows:

1. Select the filter you want to delete.

2. Click the **Delete Filter** icon.

The system will ask you to confirm the deletion.

TIP

Please note that **Global filters** can only be deleted by users who have the *editGlobalFilter* access privilege.

3. Click [OK] to delete the filter.

Selecting a filter will automatically refresh the grid with information from the database.

Add/Edit Users

Perform the following steps to add or edit users. To do so, the logged-in user must have the *PSAC_addUser* and *PSAC_editUser* privileges, respectively.

To create a new user, proceed as follows:

1. Click [Add].

The system displays the **Add User** dialog.

Figure 13: Add User dialog

2. Define the following properties:

- **User Name**

Enter the user name used to log into the system. This name must be unique among all users (enabled and disabled) in the system. Once a user is created and saved to the database, this property becomes read-only during any future edits. The user name is a mandatory property.

- **First Name**

Enter the first name of the user. The first name is a mandatory property.

- **Last Name**

Enter the last name of the user. The last name is a mandatory property.

- **Description**

Enter the description of the user, if required.

■ **User Expiration**

Select the expiry date of the user. Once a user is saved, the expiry date is set to 12/31/9999 12:00 AM.

■ **Email**

Enter the email address of the user, if required.

■ **Status**

Select a status from the drop-down menu. The following options are available: **Enabled**, **Disabled**. The status is a mandatory property with **Enabled** as default setting.

■ **Password**

Enter a password for the user name. The password is a mandatory property.

TIP

Passwords must meet the criteria for FactoryTalk ProductionCentre passwords as configured in FTPC Administrator. See the *FTPC Administrator User's Guide* for details, [14] (page 3).

■ **Confirm Password**

Re-enter the password for confirmation. Confirm password is a mandatory property.

■ **Password Expiration**

Select the expiry date of the password. Once a user is saved, the expiry date is set to 12/31/9999 12:00 AM.

TIP

You can force a user to change his password when he logs in for the first time by setting the password expiration to the current date (or a date in the past).

3. When you have completed your data entry, you can

- either click [Save] if you are going to add more users.

The system saves the data and keeps the dialog open for adding another user.

- or click [Save and Close] to close the dialog.

- or click [Cancel] to close the dialog without saving the entered data.

To edit an existing user, proceed as follows:

1. From the list of users, select the user you want to edit.
2. Click [Edit].

The system displays the **Edit User** dialog.

The **User Name** is read-only and cannot be changed.

The **Password** properties do not appear in this dialog. Passwords can only be changed with the **Change Password** function (page 28).

The **Status** of the user is read-only and can be changed with the **Disable/Enable User** function (page 30).

Figure 14: Edit User dialog

3. Change the data as required.
4. When you have completed your data entry, you can
 - click [Save] to close the dialog after changing the data of your user
 - or click [Cancel] to close the dialog without saving the entered data.

Once you have saved a user, you can proceed with assigning a start form (page 26) and assigning user groups (page 27), if applicable. All users are automatically added to the **PlantOpsOperator** user group. Each PharmaSuite user must be assigned to the **MinimalAccess** group to be able to start PharmaSuite applications.

Assign Start Forms to Users

Perform the following steps to assign a form to a user that will be displayed as the initial form when the user logs in. To do so, the logged-in user must have the *PSAC_editUser* privilege.

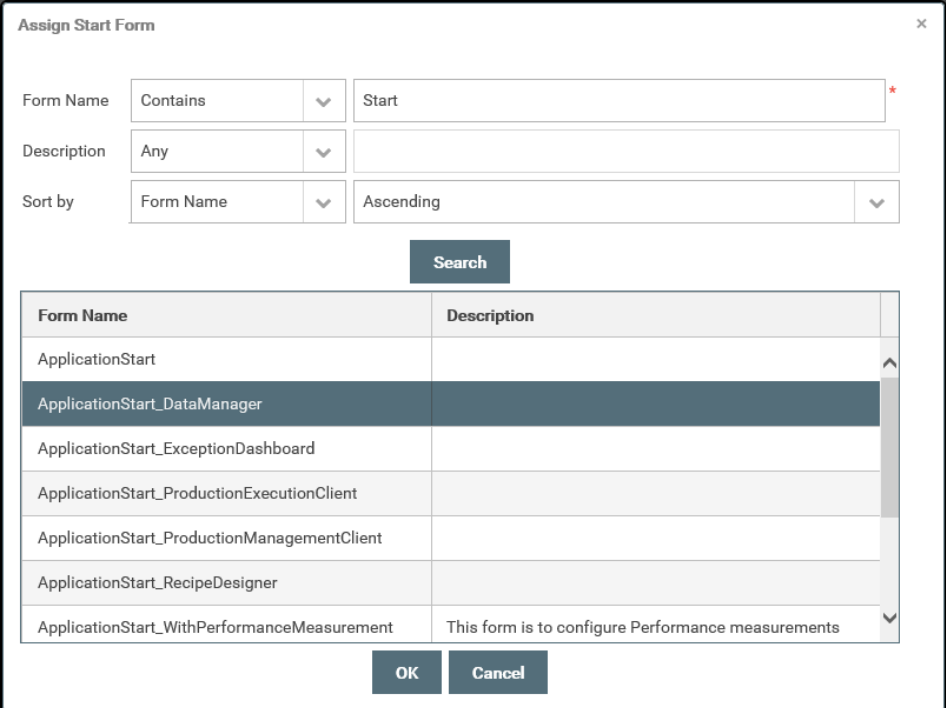
To assign forms to users, proceed as follows:

1. From the list of users, select the user to which you want to assign a start form.
2. Click [Assign Start Form].
3. To add a start form, select the form you want to assign to the user. To remove the start form, unselect the form you want to remove from the user.

TIP

To change the start form, select another form to unselect the current start form.

Use the filter to narrow down the list of forms displayed.



The 'Assign Start Form' dialog box contains a search section with three dropdown menus: 'Form Name' (set to 'Contains'), 'Description' (set to 'Any'), and 'Sort by' (set to 'Form Name' and 'Ascending'). A 'Search' button is located below these filters. The main area is a table with two columns: 'Form Name' and 'Description'. The table lists several forms, with 'ApplicationStart_DataManager' currently selected. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Form Name	Description
ApplicationStart	
ApplicationStart_DataManager	
ApplicationStart_ExceptionDashboard	
ApplicationStart_ProductionExecutionClient	
ApplicationStart_ProductionManagementClient	
ApplicationStart_RecipeDesigner	
ApplicationStart_WithPerformanceMeasurement	This form is to configure Performance measurements

Figure 15: Assign Start Form dialog

4. Make your changes and
 - either click [OK] to close the dialog and apply the assignment
 - or click [Cancel] to retain the old assignment without changes.

Assign User Groups to Users

Perform the following steps to assign user groups to users. To do so, the logged-in user must have the *PSAC_assignUserGroupToUser* privilege.

To assign user groups to users, proceed as follows:

1. From the list of users, select the user to which you want to assign user groups.
2. Click [Assign User Groups].

TIP

All users are automatically added to the **PlantOpsOperator** user group and cannot be removed from this group.

3. To add assignments, in the first column, select the checkbox of each user group you want to assign to the user. To remove assignments, in the first column, unselect the checkbox of each user group you want to remove from the user. Use the filter to narrow down the list of user groups displayed. You can also add a new user group to the list by clicking [Create User Group]. See "Add/Edit User Groups" for more details on adding user groups (page 34).

The dialog box titled "Assign User Groups" contains a search section with three dropdown menus: "User Group Name" (set to "Any"), "Description" (set to "Contains"), and "Sort by" (set to "User Group Name" and "Ascending"). A "Search" button is located below these filters. A "Create User Group" button is positioned to the right of the search filters. Below the search section is a table with the following data:

	User Group Name	Description
<input checked="" type="checkbox"/>	PlantOpsOperator	PlantOps Operators
<input type="checkbox"/>	PSACFunctionalAdmin	User group for Functional Administration
<input checked="" type="checkbox"/>	PSACUserAdmin	User group for User Administration
<input type="checkbox"/>	PlantOpsAdmin	PlantOps Administrators
<input checked="" type="checkbox"/>	SecurityAdministrator	SecurityAdministrators can perform all actions associated with users and user groups
<input type="checkbox"/>	SystemAdministrators	SystemAdministrators can perform all other system administration functions.

At the bottom of the dialog box are "Save" and "Close" buttons.

Figure 16: Assign User groups dialog

4. Make your changes and
 - either click [Save] to close the dialog and apply the assignments
 - or click [Close] to retain the old assignments without changes.

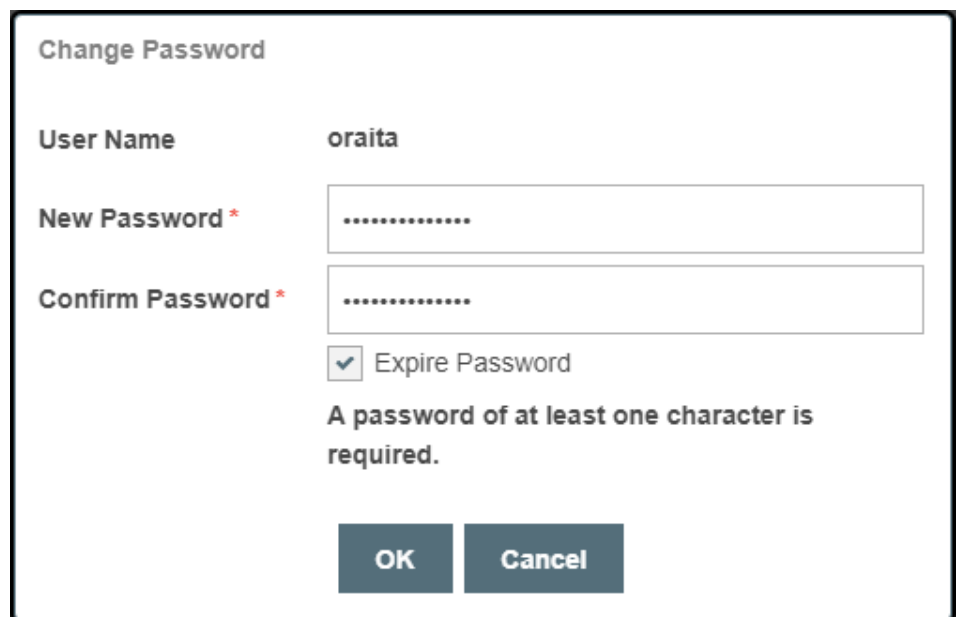
Change Passwords

Perform the following steps to change the password of an existing user. To do so, the logged-in user must have the *PSAC_changeUserPassword* privilege.

To change a user's the password, proceed as follows:

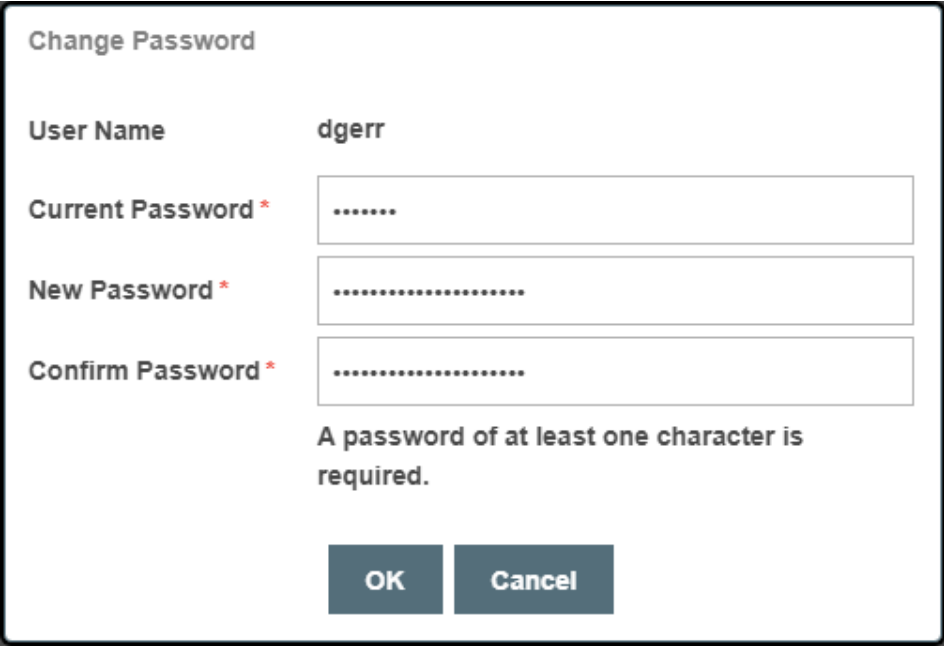
1. From the list of users, select the user whose password you want to change.
2. Click [Change Password].

The system displays the **Change Password** dialog.



The image shows a 'Change Password' dialog box. It has a title bar 'Change Password'. Inside, there are two labels: 'User Name' with the value 'oraita' and 'New Password *' with a text input field containing dots. Below 'New Password *' is a 'Confirm Password *' label with another text input field containing dots. There is a checkbox labeled 'Expire Password' which is checked. Below the checkbox is a message: 'A password of at least one character is required.' At the bottom right are two buttons: 'OK' and 'Cancel'.

Figure 17: Change Password dialog



The image shows a 'Change Password' dialog box. It has a title bar 'Change Password'. Inside, there are four labels with corresponding input fields: 'User Name' with the value 'dgerr', 'Current Password *' with a masked field '.....', 'New Password *' with a masked field '.....', and 'Confirm Password *' with a masked field '.....'. Below the input fields is a message: 'A password of at least one character is required.' At the bottom are two buttons: 'OK' and 'Cancel'.

Figure 18: Change Password dialog

3. Define the following properties:

■ **Current Password**

Enter the current password. This property is only visible if you are changing the password of the currently logged-in user.

■ **New Password**

Enter a new password for the user name. The new password is a mandatory property.

TIP

The new password cannot be the same as any of the previous three passwords. Passwords must meet the criteria for FactoryTalk ProductionCentre passwords as configured in FTPC Administrator. See the *FTPC Administrator User's Guide* for details, [14] (page 3).

■ **Confirm Password**

Re-enter the new password. Confirm password is a mandatory property.

■ **Expire Password**

Check this box if you want the user's new password to expire immediately. This box is checked by default as it is expected that the user will change the password upon the next login. This property is not available for the currently logged-on user.

4. When you have completed your data entry, you can
 - either click [OK] to close the dialog
 - or click [Cancel] to close the dialog without saving the entered data.

TIP

Clicking [OK] without entering a new password or after the 10-minute grace period has elapsed will display an error message. Closing the error message will automatically log out the current user, who must consequently contact an administrative user to reset the password.

When the user logs in with the new password, a dialog displays telling the user that the password has expired. The dialog prompts the user to enter the current password, define a new password, and confirm the new password. The user now has 10 minutes to change the password before being locked out of the application (this 10-minute grace period is defined by the FTPC Custom Security Provider). Once the password has been changed, the user is automatically logged out and must log back in using the new password.

If the user logs in to a screen that requires a station, the password dialog displays after the station selection dialog.

Disable/Enable Users

Perform the following steps to disable or enable users. To do so, the logged-in user must have the *PSAC_disableUser* privilege.

To disable a user, proceed as follows:

1. From the list of users, select the user you want to disable.

TIP

You can only disable users that are enabled. An operational procedure (SOP) needs to be in place to ensure that only users who are not logged into any PharmaSuite client are selected for being disabled.

2. Click [DISABLE USER].
The system will ask you to confirm that you want the user disabled. Once confirmed, the user's status changes to **Disabled**.

To enable a user, proceed as follows:

1. From the list of users, select the user you want to enable.

TIP

You can only enable users that are disabled.

2. Click [ENABLE USER].
The system will ask you to confirm that you want the user enabled. Once confirmed, the user's status changes to **Enabled**.

Manage User Groups

Click [User Groups] to display a list of available user groups. To view the **User Groups** editor, the logged-in user must have the *PSAC_viewUserGroup* privilege. Click [Refresh] to refresh the list of user groups.

You can import and export the data and configurations of user groups via .xlsx spreadsheet. To do so, click [Import] or [Export], respectively. The logged-in user must have the *PSAC_importUserGroup* and *PSAC_exportUserGroup* privileges, respectively. For details on importing and exporting configurations, please refer to "Import/Export Configurations" in the *FTPC Modular Framework WebSDK User's Guide*, [03] (page 3).

TIP

To import a user group, the following prerequisites must be fulfilled:

- A name must be defined.
- The parameter values assigned to the user group must be available in the target system.
- The users assigned to the user group must be available in the target system.
- The access privileges assigned to the user group must be available in the target system.
- For importing a user group with assigned access privileges, the user who performs the import must have the *PSAC_assignUserGroupToAccessPrivilegePerformers* and *PSAC_assignUserGroupToAccessPrivilegeVerifiers* privileges, respectively.

The screenshot displays the 'User Groups' management interface. On the left, a 'Filters' panel shows 'Administrative' selected. The main area contains a table of user groups:

User Group Name	Description
PSACFunctionalAdmin	User group for Functional Administration
PSACUserAdmin	User group for User Administration
PlantOpsAdmin	PlantOps Administrators
SecurityAdministrators	SecurityAdministrators can perform all actions associated with users and user groups.
SystemAdministrators	SystemAdministrators can perform all other system administration functions.
UserAdministrators	UserAdministrators can disable and change the password of existing users.

Below the table are two sections for configuration:

- Assign Access Privileges:** A table with columns 'Access Privilege Name' and 'Description'.

Access Privilege Name	Description
PSAC_viewUser	Allows access into the User Management editor.
PSAC_viewUserGroup	Allows access to the User Group Management editor.
PSAC_addUser	Allows creating new users.
PSAC_addUserGroup	Allows creating new user groups.
- Assign Users:** A table with columns 'User Name' and 'Description'.

User Name	Description
001702U01	
001702U02	
001703U01	
001703U02	

Figure 19: User Groups editor

Create User Group Filters

Creating a filter provides a method for you to selectively display all previously created user groups. To create filters, the logged-in user must have the *PSAC_viewUserGroup* privilege.

To create a new filter, proceed as follows:

1. Click the **Add Filter** icon.
The system displays the **Create Filter** dialog.

Figure 20: Create User Group filters

2. Define the following properties:

TIP

To enter multiple string criteria, type them all out and use commas as separators.

■ Filter Owner

Select one of the following filter criteria from the drop-down menu.

- **Global (default):** All users can apply the created filter. To add, edit, or delete a global filter, a user must have the *editGlobalFilter* access privilege.
- **Current User:** This is a user-specific filter. It is only visible for the user who has created the filter and can thus only be applied, edited, or deleted by this user.

■ Filter

Specifies the name of the filter. The name is a mandatory property.

■ **User Group Name**

Select one of the following conditions and then enter a complete or partial user group name by which to filter, if required.

- Any (default)
- Contains
- Equals
- Starts With

■ **Description**

Select one of the following conditions and then enter a complete or partial description by which to filter, if required.

- Any (default)
- Contains
- Equals
- Starts With

■ **Sort by**

Select one of the available filter criteria (**User Group Name** (default), **Description**) and then the sort order that will be applied to the list of the filter results, if required.

- Ascending (default)
- Descending

3. When you have completed your data entry, you can
 - either click [Save] to close the dialog and apply the new filter
 - or click [Cancel] to close the dialog without saving the entered data.

To edit a filter, proceed as follows:

1. Select the filter you want to change.
2. Click the **Edit Filter** icon.

TIP

Please note that **Global** filters can only be changed by users who have the *editGlobalFilter* access privilege.

3. Make your changes and
 - either click [Save] to apply the changed filter
 - or click [Cancel] to retain the old filter without changes.

To delete a filter, proceed as follows:

1. Select the filter you want to delete.
2. Click the **Delete Filter** icon.
The system will ask you to confirm the deletion.

TIP

Please note that **Global filters** can only be deleted by users who have the *editGlobalFilter* access privilege.

3. Click [OK] to delete the filter.

Selecting a filter will automatically refresh the grid with information from the database.

Add/Edit User Groups

Perform the following steps to add or edit user groups. To do so, the logged-in user must have the *PSAC_addUserGroup* and *PSAC_editUserGroup* privileges, respectively.

To create a new user, proceed as follows:

1. Click [Add].
The system displays the **Add User Group** dialog.

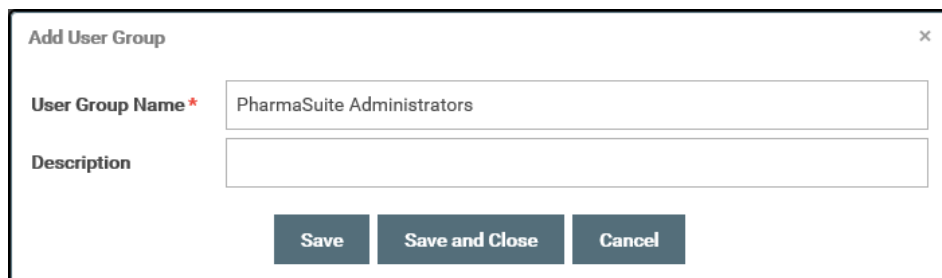


Figure 21: Add User Group dialog

2. Define the following properties:
 - **User Group Name**
Enter the name of the user group name. The user group name is a mandatory property.
 - **Description**
Enter the description of the user group, if required.
3. When you have completed your data entry, you can
 - either click [Save] if you are going to add more user groups.
The system saves the data and keeps the dialog open for adding another user group.
 - or click [Save and Close] to close the dialog.
 - or click [Cancel] to close the dialog without saving the entered data.

To edit an existing user group, proceed as follows:

1. From the list of user groups, select the user group you want to edit.
2. Click [Edit].
The system displays the **Edit User Group** dialog.
The **User Group Name** of the user group is read-only and cannot be changed.
3. Change the data as required.
4. When you have completed your data entry, you can
 - click [Save] to close the dialog after changing the data of your user group
 - or click [Cancel] to close the dialog without saving the entered data.

Once you have saved a user group, you can proceed with assigning access privileges (page 35) and assigning users (page 37), if applicable. All users are automatically added to the **PlantOpsOperator** user group.

Assign Access Privileges to User Groups

Perform the following steps to assign access privileges to user groups. To do so, the logged-in user must have the *PSAC_assignUserGroupToAccessPrivilegePerformers* privilege.

To assign access privileges to user groups, proceed as follows:

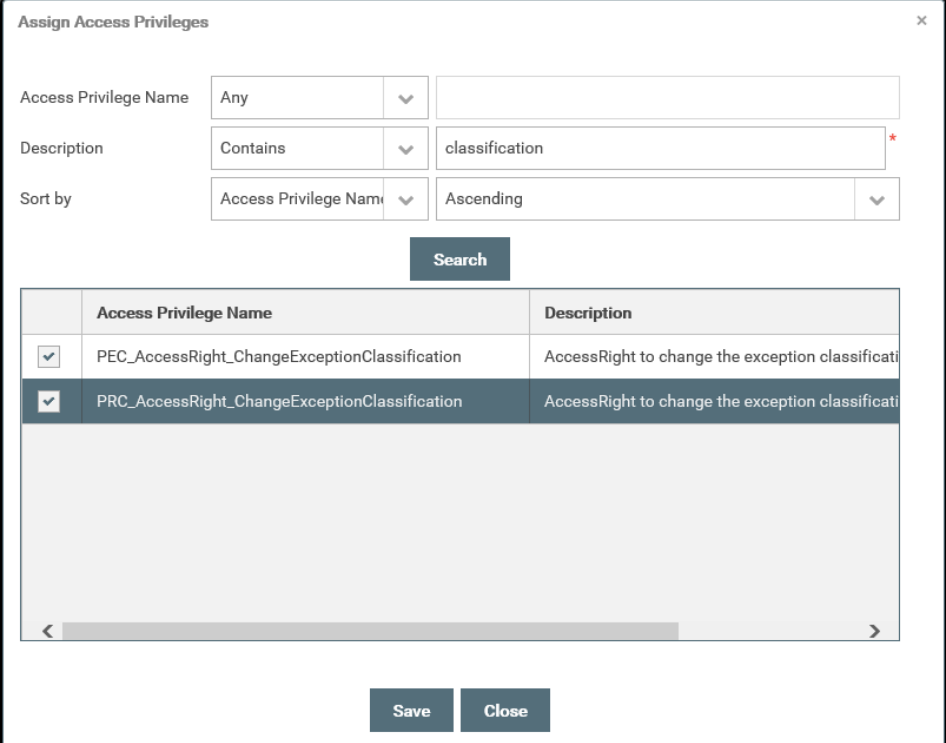
1. From the list of user groups, select the user group to which you want to assign access privileges.
2. Click [Assign Access Privileges].

3. To add assignments, in the first column, select the checkbox of each access privilege you want to assign to the user group. To remove assignments, in the first column, unselect the checkbox of each access privilege you want to remove from the user group.

Use the filter to narrow down the list of access privileges displayed.

TIP

The user group is assigned as performer user group to the access privilege.



The dialog box titled "Assign Access Privileges" contains a search filter section at the top. It includes three rows of filters: "Access Privilege Name" with a dropdown set to "Any", "Description" with a dropdown set to "Contains" and a text input field containing "classification", and "Sort by" with a dropdown set to "Access Privilege Name" and a secondary dropdown set to "Ascending". A "Search" button is located below the filters. The main area of the dialog is a table with two columns: "Access Privilege Name" and "Description". The table contains two rows, both of which are selected (indicated by checked checkboxes in the first column). The first row is "PEC_AccessRight_ChangeExceptionClassification" with the description "AccessRight to change the exception classificati". The second row is "PRC_AccessRight_ChangeExceptionClassification" with the description "AccessRight to change the exception classificati". Below the table is a horizontal scrollbar. At the bottom of the dialog are "Save" and "Close" buttons.

	Access Privilege Name	Description
<input checked="" type="checkbox"/>	PEC_AccessRight_ChangeExceptionClassification	AccessRight to change the exception classificati
<input checked="" type="checkbox"/>	PRC_AccessRight_ChangeExceptionClassification	AccessRight to change the exception classificati

Figure 22: Assign Access Privileges dialog

4. Make your changes and
 - either click [Save] to close the dialog and apply the assignments
 - or click [Close] to retain the old assignments without changes.

Assign Users to User Groups

Perform the following steps to assign users to user groups. To do so, the logged-in user must have the *PSAC_assignUserGroupToUser* privilege.

To assign users to user groups, proceed as follows:

1. From the list of user groups, select the user group to which you want to assign users.
2. Click [Assign Users].

TIP

All users are automatically added to the **PlantOpsOperator** user group and cannot be removed from this group.

3. To add assignments, in the first column, select the checkbox of each user you want to assign to the user group. To remove assignments, in the first column, unselect the checkbox of each user you want to remove from the user group. Use the filter to narrow down the list of users displayed.
You can also add a new user to the list by clicking [Create User]. See "Add/Edit Users" for more details on adding users (page 23).
4. Make your changes and
 - either click [Save] to close the dialog and apply the assignments
 - or click [Close] to retain the old assignments without changes.

Delete User Groups

Perform the following steps to delete user groups. To do so, the logged-in user must have the *PSAC_deleteUserGroup* privilege.

To delete a user group, proceed as follows:

1. From the list of user groups, select the user group you want to delete.
2. Click [Delete].
The system will ask you to confirm the deletion.
3. Click [OK] to delete the user group.

TIP

User groups can only be deleted if there are no users in the group. Certain base Plant Operations user groups (e.g. **PlantOpsAdmin**, **PlantOpsDesigner**, etc.) cannot be deleted at all.

Manage Access Privileges

Access rights and electronic signatures are both defined by means of access privileges. An access privilege object allows you to define which user groups have permission to perform which transactions.

Access privileges for electronic signatures define electronic signature requirements. PharmaSuite requires users to enter electronic signatures for a number of pre-defined events for various contexts and situations while working with the system. Each of these signatures can be configured to match custom user requirements, including information about who is allowed to sign (definition of a required user group for the first and second signatures), if anyone has to sign at all (enable or disable the signature function), or if a comment has to be provided (optional or mandatory comments).

Access rights can be used to limit access to PharmaSuite applications, stations, use cases, actions, or data handlers, depending on the type of the access right. Additionally, the access rights also apply to PS Administration and installed Fit-for-purpose applications.

Click [Access Privileges] to display a list of available access privileges. To view the **Access Privileges** editor, the logged-in user must have the *PSAC_viewAccessPrivilege* privilege. Click [Refresh] to refresh the list of access privileges.

You can import and export the data and configurations of access privileges via .xlsx spreadsheet. To do so, click [Import] or [Export], respectively. The logged-in user must have the *PSAC_importAccessPrivilege* and *PSAC_exportAccessPrivilege* privileges, respectively. For details on importing and exporting configurations, please refer to "Import/Export Configurations" in the *FTPC Modular Framework WebSDK User's Guide*, [03] (page 3).

TIPS

Please be aware that changes to existing access privileges will affect the privileges of all users that belong to a group with the changed access privilege.

Creating a new signature or requesting another one involves changes to existing code. Thus, these changes need to be covered in the scope of system adaptation.

During system configuration, access privileges can be assigned to a range of functions. Examples on how to assign access privileges to system functions such as

- Application start
- Station-specific login
- Activity set start
- PMC Client actions
- PMC Client data handler
- Multi-reference (filter) selector
- Flexible State Model (status transitions)
- Flexible State Model (version graphs)
- Electronic signatures (exception management)

are provided in the related PharmaSuite manuals, along with more detailed information about the specific functions.

To import an access privilege, the following prerequisites must be fulfilled:

- A name must be defined.
- The name value must not exceed the maximum length of 64 characters.
- The description value must not exceed the maximum length of 255 characters.
- A performer user group must be defined.
- For **Signature** access privileges with defined verifier signatures, a verifier user group must be defined.
- The user groups assigned to the access privilege must be available in the target system.
- For signatures of **Signature** access privileges, the message pack used by the signatures must be available in the target system and the specified message ID must be available in the message pack.
- For signatures of **Signature** access privileges, the pre-defined comment used by the signature must be available in the target system.

Filters

Filter 1

Filter 2

Filter 3

Production Response Client

Access Privileges

Add

Edit

Refresh

Delete

Import

Export

Privilege Name	Description	Category	Performer Signature	Verifier Signature	Access
PRC_AccessRight_ChangeExceptionClassification	AccessRight to change the exception classification in Production Review Client (PRC)				Undef
PRC_AccessRight_ChangeRiskClassOrStatus	AccessRight to change the risk class or status in Production Review Client (PRC)				Undef
PRC_AccessRight_EDBOverview_Perspective_EditM	AccessRight for equipment perspective (edit mode) in Master Data Client				Undef
PRC_AccessRight_PerformProductionReview	AccessRight to perform the production review in Production Review Client (PRC)				Undef
PRC_AccessRight_PerformQAReview	AccessRight to perform the QA review in Production Review Client (PRC)				Undef
PRC_SIGNATURE_COMMENT_ENTERED	Signature when exception comment entered		Sig_Reason_Confirm		
PRC_SIGNATURE_EXCEPTION_ENTERED	signature when exception record entered		Sig_Reason_Confirm		
PRC_SIGNATURE_EXCEPTION_SENT	Signature when an exception is sent to an external system		Sig_Reason_Confirm		

Assign Performer User Groups

Assign Verifier User Groups

Define Signature

Delete Signature

Name	Description	Type	Signature Defined
Supervisor (Shop Floor)		Performer	Yes
DispensingOperatorGroup		Performer	Yes
LogisticalOperatorGroup		Performer	Yes
WIPOperatorGroup		Performer	Yes

Figure 23: Access Privileges editor

Create Access Privilege Filters

Creating a filter provides a method for you to selectively display all previously created access privileges. To create filters, the logged-in user must have the *PSAC_viewAccessPrivilege* privilege.

To create a new filter, proceed as follows:

1. Click the **Add Filter** icon.
The system displays the **Create Filter** dialog.

Create Filter

Filter Owner Global

Filter * Production Response Client

Privilege Name Starts With PRC

Description Any

Category Any

Privilege Type Any

Sort by Privilege Name Ascending

Save **Cancel**

Figure 24: Create Access Privilege filters

2. Define the following properties:

TIP

To enter multiple string criteria, type them all out and use commas as separators.

■ **Filter Owner**

Select one of the following filter criteria from the drop-down menu.

■ **Global (default):** All users can apply the created filter. To add, edit, or delete a global filter, a user must have the *editGlobalFilter* access privilege.

■ **Current User:** This is a user-specific filter. It is only visible for the user who has created the filter and can thus only be applied, edited, or deleted by this user.

■ **Filter**

Specifies the name of the filter. The name is a mandatory property.

■ **Privilege Name**

Select one of the following conditions and then enter a complete or partial privilege name by which to filter, if required.

■ Any (default)

■ Contains

■ Equals

■ Starts With

■ **Description**

Select one of the following conditions and then enter a complete or partial privilege description by which to filter, if required.

■ Any (default)

■ Contains

■ Equals

■ Starts With

■ **Category**

Select one of the following conditions and then select a category by which to filter, if required. All categories that are available in the system show as options. Selecting the option without category text will filter for access privileges without a category.

■ Any (default)

■ Equals

■ **Privilege Type**

Select one of the following conditions and then select a privilege type by which to filter, if required. The available types are **Undefined**, **Access Right**, and **Signature**.

■ Any (default)

■ Equals

■ **Sort by**

Select one of the available filter criteria (**Privilege Name** (default), **Description**, **Category**, **Privilege Type**) and then the sort order that will be applied to the list of the filter results, if required.

■ Ascending (default)

■ Descending

3. When you have completed your data entry, you can
 - either click [Save] to close the dialog and apply the new filter
 - or click [Cancel] to close the dialog without saving the entered data.

To edit a filter, proceed as follows:

1. Select the filter you want to change.
2. Click the **Edit Filter** icon.

TIP

Please note that **Global** filters can only be changed by users who have the *editGlobalFilter* access privilege.

3. Make your changes and
 - either click [Save] to apply the changed filter
 - or click [Cancel] to retain the old filter without changes.

To delete a filter, proceed as follows:

1. Select the filter you want to delete.
2. Click the **Delete Filter** icon.
The system will ask you to confirm the deletion.

TIP

Please note that **Global filters** can only be deleted by users who have the *editGlobalFilter* access privilege.

3. Click [OK] to delete the filter.

Selecting a filter will automatically refresh the grid with information from the database.

Add/Edit Access Privileges

Perform the following steps to add or edit access privileges. To do so, the logged-in user must have the *PSAC_addAccessPrivilege* and *PSAC_editAccessPrivilege* privileges, respectively.

To create a new access privilege, proceed as follows:

1. Click [Add].
The system displays the **Add Access Privilege** dialog.

Add Access Privilege

Privilege Name *

PRC_SIGNATURE_COMMENT_ENTERED

Description

Signature when exception comment entered

Category

Privilege Type *

Signature

Performer User Group *

Supervisor (Shop Floor), Dispensing

Access Right Data

Signature Data

Verifier User Group

Signature Type *

Signature

EBR-relevant

No

☐ Signature Internationalization Disabled

☐ Global Signature

Save

Save and Close

Cancel

Figure 25: Add Access Privilege dialog

2. Define the following properties:

■ **Privilege Name**

Enter the name of the access privilege. The name is a mandatory property.

■ **Description**

Enter the description of the access privilege, if required.

■ **Category**

Select a category from the drop-down menu, if required. The following options are available:

■ PS Administration-specific: **PSAdminClient**.

■ PharmaSuite-specific: **S88_eqm**, **S88_recipe**, **S88_OperatorExceptionTexts**, **S88_ReviewerExceptionTexts**, and **S88_SignatureComments**.

TIP

The **Admin**, **Report**, and **Setup** categories are system-defined categories and not available for selection.

■ **Privilege Type**

Select a privilege type from the drop-down menu. The following options are available:

■ **Undefined**

The **Undefined** type is a system-defined type for access privileges provided along with FactoryTalk ProductionCentre. They are relevant to PharmaSuite and other installed fit-for-purpose applications and can be maintained with PS Administration.

TIP

No further properties are available.

■ **Access Right**

Defines which user group is allowed to access or execute a specific feature of PharmaSuite.

TIP

Further properties are available in the **Access Right Data** tab.

■ **Signature**

Defines that a signature is to be entered and which information it has to include when a user executes a specific step or accepts an exceptional situation.

TIP

Further properties are available in the **Signature Data** tab.

The type is a mandatory property.

■ **Performer User Group**

Click [...] to open the **Select Performer User Groups** dialog. In the first column, select the checkbox of each user group you want to select and click [OK]. Users of the selected groups are allowed to access the functionality protected by the access right or to type the first signature for the signature, respectively. The performer user group is a mandatory property. To clear the box, click the eraser button.

TIP

The selected user groups are displayed in the list of assigned user groups. You can also use [Assign Performer User Groups] from the button bar below the list of access privileges to assign performer user groups.

- The left tab contains the access right data:

Access Right Type

Select an access right type from the drop-down menu, if required. The following options are available:

- **Undefined** (default)
Defines access rights for starting either modes (read-only or read/write) of a PharmaSuite client (e.g. Recipe and Workflow Designer, Data Manager) or for certain master data objects supporting access rights during execution (e.g. stations).
- **Use Case**
Defines access rights for special use cases in the Production Management Client.
- **Action**
Defines access rights for special actions of use cases in the Production Management Client.
- **Data Handler**
Defines access rights for special data handlers of use cases in the Production Management Client.
- **Activity Set**
Defines access rights for special actions in the Production Execution Client.
- **Confidential Object**
Defines access rights to protect the intellectual property of recipes, workflows, orders, and related data from unauthorized access in Recipe and Workflow Designer, the Production Management Client, the Production Execution Client, and the Production Response Client. See also "Create Access Rights for Confidential Objects" (page 55).

■ **Work Center-relevant**

Select the **Work Center-relevant** option if the access right shall be available as a selectable access right for stations in Data Manager - Work Center.

TIP

The access right must be of the **Undefined** access right type.

- The right tab contains the signature data:

Verifier User Group

Click [...] to open the **Select Verifier User Groups** dialog. In the first column, select the checkbox of each user group you want to select and click [OK], if required.

Users of the selected user groups are allowed to act as second signatories (verifiers).

To clear the box, click the eraser button.

TIP

The selected user groups are displayed in the list of assigned user groups. You can also use [Assign Verifier User Groups] from the button bar below the list of access privileges to assign verifier user groups.

■ **Signature Type**

Select a signature type from the drop-down menu, if required. The following options are available:

■ **Disabled**

Disables the signature. With this setting no user interaction will occur at the processing time. It allows you to skip signatures that are not required. Not applicable to electronic signatures for exception records and in the Production Execution Client.

■ **Logging**

Defines a logging-only signature (also referred to as a silent signature). There is no interaction required at processing time. However, the signature will automatically record the currently logged-in user. When generating a report, the signature of the current user will be displayed in the list of signatures.

Not applicable to electronic signatures for exception records and in the Production Execution Client.

■ **Signature**

Defines a normal signature. At the processing time, a pop-up dialog box will be displayed and the user (or users in case of a double signature) will be required to sign, providing comments as defined by the signature details outlined below.

■ **Exception**

Defines an exception signature. This signature behaves exactly like the normal signature type. The only difference is that it gets an additional flag to mark it as an exception type signature. This allows you to generate reports that list only the signatures performed for severe exceptions, for example.

Not applicable to electronic signatures for exception records and in the Production Execution Client.

■ **Warning**

Defines a warning. At processing time, a message dialog with two buttons (**OK** and **Cancel**) will be displayed. In case the warning is accepted, the currently logged-in user will be recorded like for the logging-only signature. Selecting **Cancel** will behave like canceling a signature.

Not applicable to electronic signatures for exception records and in the Production Execution Client.

■ **Error**

Defines an error. At processing time, a message dialog with an **OK** button will be displayed. It will behave like canceling the signature. The user will not be allowed to proceed.

Not applicable to electronic signatures for exception records and in the Production Execution Client.

■ **EBR-relevant**

Select an option specific to the relevance for EBR from the drop-down menu, if required. The following options are available:

■ **No (default)**

■ **Yes**

The **Signature** access privilege is available in the Universe of Recipe and Workflow Designer and can be assigned as a default signature for phase-related exceptions.

■ **Invisible**

For internal use only. The **Signature** access privilege is relevant for EBR but is not visible in the Universe of Recipe and Workflow Designer.

■ **Signature Internationalization Disabled**

Select the **Signature Internationalization Disabled** option if the behavior prior to PharmaSuite 8.3 regarding localization shall be enabled. It is relevant for **Signature** access privileges that can be used in the context of EBR (i.e. with **EBR-relevant** set to **Yes** or **Invisible**).

■ **Global Signature**

Select the **Global Signature** option if the **Signature** access privilege shall be used in the Production Execution Client and not be configurable in Recipe and Workflow Designer, e.g. a pre-defined phase completion signature.

3. When you have completed your data entry, you can

- either click [Save] if you are going to add more access privileges.
The system saves the data and keeps the dialog open for adding another access privilege.
- or click [Save and Close] to close the dialog.
- or click [Cancel] to close the dialog without saving the entered data.

To edit an existing access privilege, proceed as follows:

1. From the list of access privileges, select the access privilege you want to edit.

2. Click [Edit].

The system displays the **Edit Access Privilege** dialog.

The **Privilege Name** of the access privilege is read-only and cannot be changed.

Edit Access Privilege

Privilege Name PRC_SIGNATURE_COMMENT_ENTERED

Description Signature when exception comment entered

Category ▼

Privilege Type* Signature ▼

Performer User Group* Supervisor (Shop Floor), Dispensing ...

Access Right Data **Signature Data**

Verifier User Group ...

Signature Type* Signature ▼

EBR-relevant ▼

☐ Signature Internationalization Disabled

☐ Global Signature

Save **Cancel**

Figure 26: Edit Access Privilege dialog

3. Change the data as required.
4. When you have completed your data entry, you can
 - click [Save] to close the dialog after changing the data of your access privilege
 - or click [Cancel] to close the dialog without saving the entered data.

Once you have saved a **Signature** access privilege, you can proceed with defining its signatures (page 51).

DEFINE SIGNATURES

Perform the following steps to define signatures of a **Signature** access privilege. To do so, the logged-in user must have the *PSAC_editSignature* privilege.

TIP

During signature execution the system displays a **Description** and a **Reason** specific to the signature. Both can either be taken from a message pack or edited manually when the signature is defined.

A reason can also be used to describe a role.

In case of an electronic signature for exception records in the Production Execution Client, the description will not be displayed when the electronic signature is requested. It is clear from the context that the operator confirms an exception. However, the defined values are stored in the database and are available in the batch record.

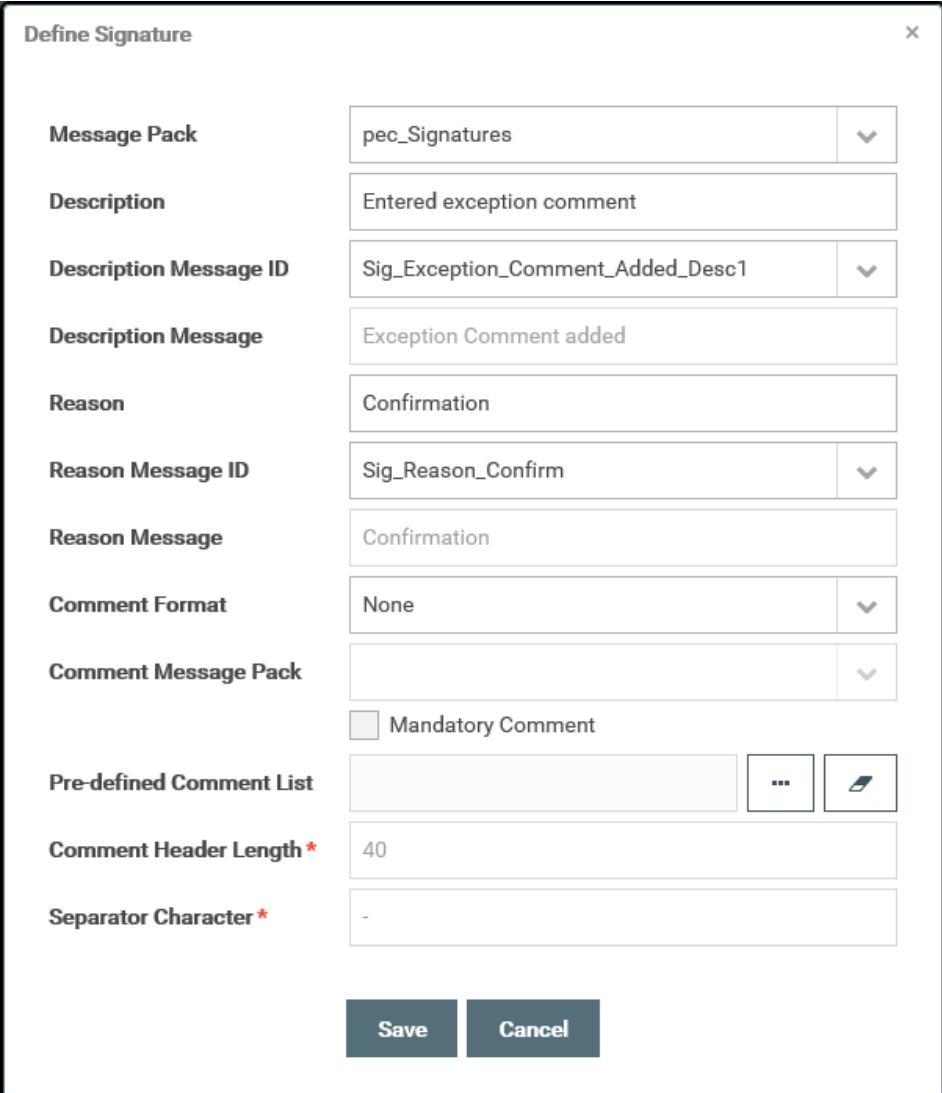
To define a signature, proceed as follows:

1. From the list of access privileges, select the **Signature** access privilege for which you want to define a signature.
2. From the list of assigned user groups below the list of access privileges, select the user group type (performer, verifier) for which you want to define a signature.

TIPS

All user groups of a type (performer, verifier) are selected automatically. When changing the definition of a single signature to a double signature you need make sure that the data of the second signature is set to be displayed on the user interface. For more information on managing signature visibility, please refer to "*Managing Electronic Signatures and Access Rights*" in *PharmaSuite Technical Manual Configuration & Extension - Volume 2*, [05] (page 3).

3. In the button bar below the list of access privileges, click [Define signature]. The system displays the **Define Signature** dialog.



The **Define Signature** dialog box contains the following fields and controls:

- Message Pack:** A drop-down menu with the value "pec_Signatures".
- Description:** A text input field containing "Entered exception comment".
- Description Message ID:** A drop-down menu with the value "Sig_Exception_Comment_Added_Desc1".
- Description Message:** A text input field containing "Exception Comment added".
- Reason:** A text input field containing "Confirmation".
- Reason Message ID:** A drop-down menu with the value "Sig_Reason_Confirm".
- Reason Message:** A text input field containing "Confirmation".
- Comment Format:** A drop-down menu with the value "None".
- Comment Message Pack:** A drop-down menu (currently empty).
- Mandatory Comment:** An unchecked checkbox.
- Pre-defined Comment List:** A text input field (empty) with a menu icon (three dots) and a save icon (pencil) to its right.
- Comment Header Length ^{*}:** A text input field containing "40".
- Separator Character ^{*}:** A text input field containing "-".
- Buttons:** "Save" and "Cancel" buttons at the bottom right.

Figure 27: Define Signature dialog

4. Define the following properties:
 - **Message Pack**
Select a message pack for the signature (description, reason) from the drop-down menu.
 - **Description**
Enter a description for the signature to be displayed during the signature execution. The description is a mandatory property.
 - **Description Message ID**
Select a message ID from the selected message pack for the description of the signature from the drop-down menu.

- **Description Message**
Display of the description message as defined in the message ID. The message is a read-only property.
- **Reason**
Enter a reason for the signature to be displayed during the signature execution. The reason is a mandatory property.
- **Reason Message ID**
Select a message ID from the selected message pack for the reason of the signature from the drop-down menu.
- **Reason Message**
Display of the reason message as defined in the message ID. The message is a read-only property.
- **Comment Format**
Select a format from the drop-down menu. The following options are available:
 - **None** (default)
The user is not allowed to enter a comment.
 - **Text**
In case the **Mandatory Comment** option is not selected, the user may optionally enter a comment.
In case the **Mandatory Comment** option is selected, the user must enter a comment.
 - **List**
The user can select a comment from a list. The list of comments is defined with the **Comment Message Pack** property.
- **Comment Message Pack**
The drop-down menu is only enabled when the **Comment Format** property is set to **List**.
Select a message pack to determine a list of selectable comments which are provided when the transaction is saved.
- **Mandatory Comment**
Select the **Mandatory Comment** option if the user must enter a comment.

■ **Pre-defined Comment List**

Click [...] to open the **Select Pre-defined Comment List** dialog. Select the list of comment texts and click [OK]. The comment texts of the selected list are available for selection when an electronic signature is requested.

To clear the box, click the eraser button.

TIP

Pre-defined comments are not supported for signatures requested when adding an exception or exception comment in the Production Execution Client and the Production Response Client, respectively.

■ **Comment Header Length**

In case a pre-defined comment list is selected, the comment header length is a mandatory property with **40** as default setting.

Enter a value within the range of [2..40] to define the maximum text length of the search range for the separator character (from the beginning through the first occurrence of the separator character).

If the separator character cannot be found, the complete text is used as the pre-defined header.

Otherwise the **Comment Header Length** is read-only and cannot be changed.

■ **Separator Character**

In case a pre-defined comment list is selected, the separator character is a mandatory property with - (hyphen) as default setting.

Enter one character whose first occurrence is used as a separator to define the pre-defined header for signature comments.

Otherwise the **Separator Character** is read-only and cannot be changed.

5. When you have completed your data entry, you can

- either click [Save] to close the dialog after adding your signature
- or click [Cancel] to close the dialog without saving the entered data.

DELETE SIGNATURES

Perform the following steps to delete signatures from a **Signature** access privilege. To do so, the logged-in user must have the *PSAC_deleteSignature* privilege.

To delete a signature, proceed as follows:

1. From the list of access privileges, select the **Signature** access privilege whose signature you want to delete.
2. From the list of assigned user groups below the list of access privileges, select the user group type (performer, verifier) from which you want to delete the signature.

TIP

All user groups of a type (performer, verifier) are selected automatically.

3. In the button bar below the list of access privileges, click [Delete signature]. The system will ask you to confirm the deletion.
4. Click [OK] to delete the signature.

CREATE ACCESS RIGHTS FOR CONFIDENTIAL OBJECTS

The concept of confidential objects protects the intellectual property of recipes, workflows, custom building blocks, orders, ERP BOMs, and related data from unauthorized access. The system provides a specific access rights type to define access privileges that allow users to maintain protected recipes, workflows, and orders.

To set up your PharmaSuite installation for the maintenance of protected objects, proceed as follows:

- Create access rights of the **Confidential Object** access rights type.
- Assign the users/user groups who are allowed to maintain confidential objects to the access rights of the **Confidential Object** access rights type.

The users (users of the user groups) can maintain confidential master recipes and master workflow.

Consider also the setting of the

AccessPrivilege/ConfidentialObject.Modifiable.WhenCreatingRecipeStructure configuration key (see "*Configuration Keys of PharmaSuite*" in *PharmaSuite Technical Manual Configuration & Extension - Volume 4*, [06] (page 3)).

EXAMPLES OF ELECTRONIC SIGNATURES IN PHARMA SUITE

The following figures present examples of electronic signatures in PharmaSuite:

The 'Electronic Signature' dialog box contains the following fields and controls:

- Description:** Status change: Edit -> Verification
- Reason:** Authorship
- User Name:** dgerr
- Password:** (Yellowed out field)
- Comment:** (Empty text box)
- Buttons:** OK, Cancel
- Identifier:** Vers_Trans_Edit-Verification

Figure 28: Signature execution with a signature dialog box for a single signature

The 'Electronic Signature' dialog box contains the following fields and controls:

- Description:** Status change: Edit -> Verification
- Reason:** Authorship
- User Name:** dgerr
- Password:** (Yellowed out field)
- Comment:** (Empty text box)
- Predefined Comment:** (Dropdown menu with a downward arrow)
- Buttons:** OK, Cancel
- Identifier:** Vers_Trans_Edit-Verification

Figure 29: Signature execution with a signature dialog box for a single signature with a pre-defined comment

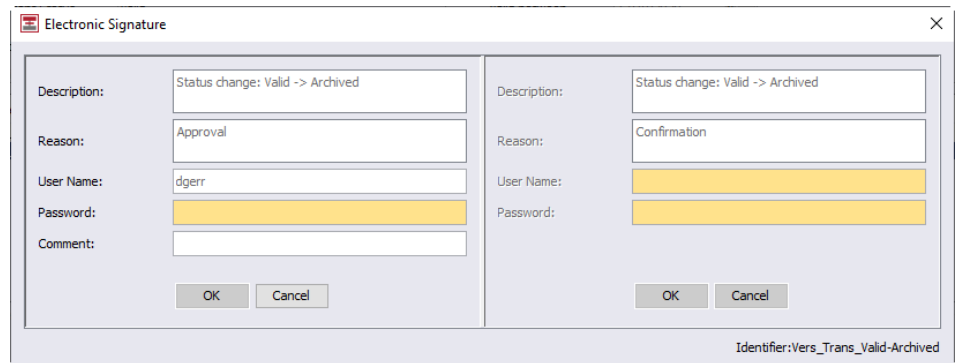


Figure 30: Signature execution with a signature dialog box for a double signature to support witness role

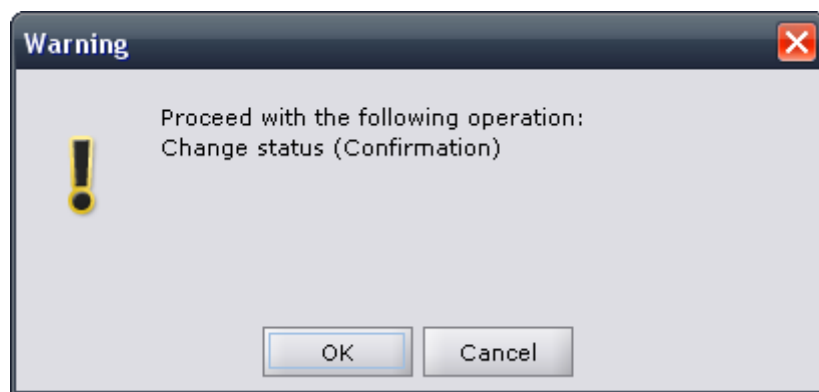


Figure 31: Signature execution with a warning dialog box

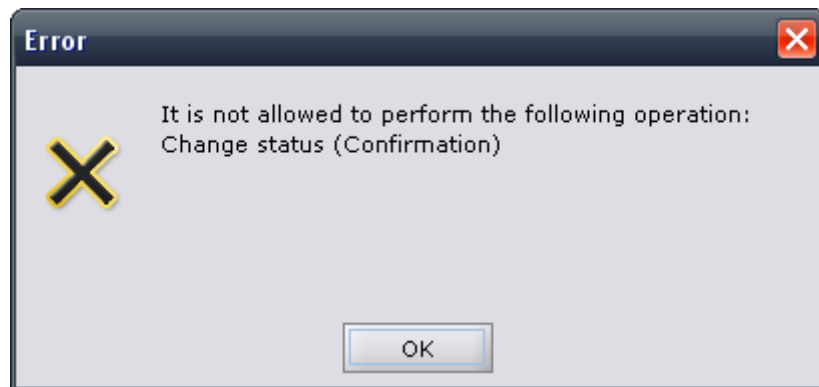


Figure 32: Signature execution with an error dialog box

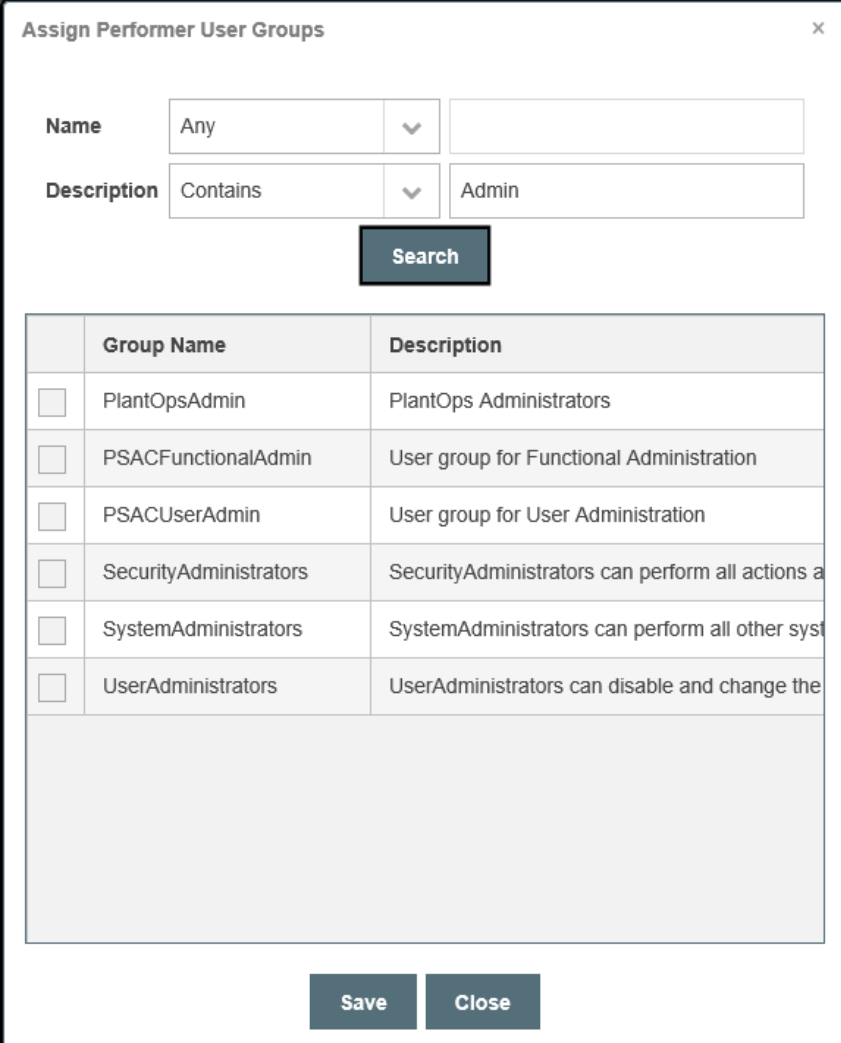
Assign User Groups to Access Privileges

Perform the following steps to assign performer user groups and verifier user groups to access privileges to define which user groups are allowed to perform the action protected by the access privilege. To do so, the logged-in user must have the *PSAC_assignUserGroupToAccessPrivilegePerformers* and *PSAC_assignUserGroupToAccessPrivilegeVerifiers* privileges, respectively.

To assign user groups to access privileges, proceed as follows:

1. From the list of access privileges, select the access privilege to which you want to assign a performer user group or a verifier user group.
2. Click [Assign Performer User Group] or [Assign Verifier User Group], respectively.

The system displays the **Assign Performer User Groups** or the **Assign Verifier User Groups** dialogs, respectively.



The dialog box titled "Assign Performer User Groups" contains search filters and a table of user groups.

Name: Any (dropdown) []

Description: Contains (dropdown) Admin []

Search [button]

	Group Name	Description
<input type="checkbox"/>	PlantOpsAdmin	PlantOps Administrators
<input type="checkbox"/>	PSACFunctionalAdmin	User group for Functional Administration
<input type="checkbox"/>	PSACUserAdmin	User group for User Administration
<input type="checkbox"/>	SecurityAdministrators	SecurityAdministrators can perform all actions a
<input type="checkbox"/>	SystemAdministrators	SystemAdministrators can perform all other syst
<input type="checkbox"/>	UserAdministrators	UserAdministrators can disable and change the

Save [button] **Close** [button]

Figure 33: Assign Performer User Groups dialog

3. To add assignments, in the first column, select the checkbox of each user group you want to assign to the access privilege. To remove assignments, in the first column, unselect the checkbox of each user group you want to remove from the access privilege.
Use the filter to narrow down the list of user groups displayed.
4. Make your changes and
 - either click [Save] to close the dialog and apply the assignments
 - or click [Close] to retain the old assignments without changes.

Delete Access Privileges

Perform the following steps to delete access privileges. To do so, the logged-in user must have the *PSAC_deleteAccessPrivilege* privilege.

To delete an access privilege, proceed as follows:

1. From the list of access privileges, select the access privilege you want to delete.
2. Click [Delete].
The system will ask you to confirm the deletion.
3. Click [OK] to delete the access privilege.

Manage Applications

Click [Applications] to display a list of available application objects. To view the **Applications** editor, the logged-in user must have the *PSAC_viewApplication* privilege. Click [Refresh] to refresh the list of application objects.

The **Applications** editor lists the number of assigned resources for each application object. Clicking an application object with assigned resources will display information for those resources in the **Assignments** box located between the list of applications and the list of properties.

You can import and export the data and configurations of applications via .xlsx spreadsheet. To do so, click [Import] or [Export], respectively. The logged-in user must have the *PSAC_importApplication* and *PSAC_exportApplication* privileges, respectively. For details on importing and exporting configurations, please refer to "Import/Export Configurations" in the *FTPC Modular Framework WebSDK User's Guide*, [03] (page 3).

TIP

To import an application object, the following prerequisites must be fulfilled:

- A name must be defined.
- The name value must not exceed the maximum length of 64 characters.
- The description value must not exceed the maximum length of 255 characters.
- The name of a property must not exceed the maximum length of 256 characters.
- The decimal value of a property must not exceed the maximum precision of 14 digits.
- The long value of a property must not exceed the maximum precision.
- The string value of a property must not exceed the maximum length of 1024 characters.

Add
Edit
Refresh
Delete
Assign

Import
Export

Name	Description	Category	Based on	Assignments
000207APP01			DefaultConfiguration	1
000675APP01			DefaultConfiguration	1
000689APP01			DefaultConfiguration	1
000711APP01			DefaultConfiguration	1
001062APP01			DefaultConfiguration	1
001093APP01			DefaultConfiguration	2
001098APP01			DefaultConfiguration	1
001120APP01			DefaultConfiguration	1
001120APP02			DefaultConfiguration	1

Assignments
Users: 000711U01

Add Property
Edit
Delete

Name	Value	Type	Object Type
UoMeOffPotency	000711UoMeOffPotency	Object	List

Figure 34: Applications editor

Add/Edit Applications

Perform the following steps to add or edit application objects. To do so, the logged-in user must have the *PSAC_addApplication* and *PSAC_editApplication* privileges, respectively.

To create a new application object, proceed as follows:

1. Click [Add].
Click [Add] and [Applications].

TIP

Make sure that no application object is selected.

The system displays the **Add Application** dialog.

Figure 35: Add Application dialog

2. Define the following properties:
 - **Name**
Enter the name of the application object. The name is a mandatory property.
 - **Description**
Enter the description of the application object, if required.
 - **Category**
Select a category from the drop-down menu, if required. The following options are available:
 - PS Administration-specific: **PSAdminClient**.
 - PharmaSuite-specific: **S88_eqm**, **S88_recipe**, **S88_OperatorExceptionTexts**, **S88_ReviewerExceptionTexts**, and **S88_SignatureComments**.

TIP

The **Admin**, **Report**, and **Setup** categories are system-defined categories and not available for selection.

■ **Base Application**

Click [...] to open the **Select Application** dialog. Select the application object and click [OK].

To clear the box, click the eraser button.

TIP

The settings of the referenced application object are inherited as default settings.

3. When you have completed your data entry, you can
 - either click [Save] if you are going to add more application objects.
The system saves the data and keeps the dialog open for adding another application object.
 - or click [Save and Close] to close the dialog.
 - or click [Cancel] to close the dialog without saving the entered data.

To edit an existing application object, proceed as follows:

1. From the list of application objects, select the application object you want to edit.
2. Click [Edit].
The system displays the **Edit Application** dialog.
The **Name** of the application object is read-only and cannot be changed.
3. Change the data as required.
4. When you have completed your data entry, you can
 - click [Save] to close the dialog after changing the data of your application object
 - or click [Cancel] to close the dialog without saving the entered data.

Once you have saved an application object, you can proceed with adding sub-groups (page 63), adding configuration properties (page 66), and assigning resources (page 68), if applicable.

ADD SUB-GROUPS TO APPLICATIONS

Perform the following steps to add sub-groups to an application object. To do so, the logged-in user must have the *PSAC_addApplication* privilege.

To add a sub-group, proceed as follows:

1. From the list of application objects, select the application object to which you want to add sub-groups.
2. Click [Add] and select the appropriate sub-group button. The following sub-groups are available: **Access Privileges, Activity Sets, Equipment, Forms, Label Designs, Libraries, Report Designs, Stations.**

TIP

Each sub-group can only be added once.
The added sub-groups are displayed as subordinate objects related to the application.

Once you have added a sub-group, you can proceed with adding configuration properties (page 66), if applicable.

ADD SUB-GROUP OBJECTS TO SUB-GROUPS

Perform the following steps to add objects to a sub-group of an application object. To do so, the logged-in user must have the *PSAC_addApplication* privilege.

TIP

Please note that you can only add sub-group objects to stations sub-groups.

To add station objects to a stations sub-group, proceed as follows:

1. In the list of application objects, navigate to the stations sub-group to which you wish to add station objects.
2. Click [Add] and then click [Station Objects].
The system displays the **Assign Station Objects** dialog.

3. To add assignments, in the first column, select the checkbox of each station you want to assign to the stations sub-group. To remove assignments, in the first column, unselect the checkbox of each station you want to remove from the stations sub-group.

Use the filter to narrow down the list of stations displayed.

Assign Stations

Name

Any

▼

Description

Any

▼

Search

	Name	Description
<input type="checkbox"/>	000178ST01	000178 Station 01
<input type="checkbox"/>	000184ST01	000184 Station 01
<input type="checkbox"/>	000207ST01	000207 Station 01
<input type="checkbox"/>	000233ST01	000233 Station 01
<input type="checkbox"/>	000233ST02	000233 Station 02
<input type="checkbox"/>	000406ST01	000406 Station 01
<input type="checkbox"/>	000407ST01	000407 Station 01
<input type="checkbox"/>	000408ST01	000408 Station 01
<input type="checkbox"/>	000418ST01	000418 Station 01
<input type="checkbox"/>	000419ST01	000419 Station 01

Save

Close

Figure 36: Assign Stations dialog

4. Make your changes and
 - either click [Save] to close the dialog and apply the assignments
 - or click [Close] to retain the old assignments without changes.

Once you have added a sub-group object, you can proceed with adding configuration properties (page 66), if applicable.

DELETE SUB-GROUP OBJECTS FROM SUB-GROUPS

Perform the following steps to delete sub-group objects from a sub-group of an application object. To do so, the logged-in user must have the *PSAC_deleteApplication* privilege.

TIP

Please note that only stations sub-groups can have sub-group objects.

To delete a station object from a stations sub-group, proceed as follows:

1. In the list of application objects, navigate to the stations sub-group from which you wish to delete a station object.
2. From the list of station objects, select the object you want to delete.
3. Click [Delete].
The system will ask you to confirm the deletion.
4. Click [OK] to delete the station object.

DELETE SUB-GROUPS FROM APPLICATIONS

Perform the following steps to delete sub-groups from an application object. To do so, the logged-in user must have the *PSAC_deleteApplication* privilege.

To delete a sub-group, proceed as follows:

1. From the list of application objects, select the application object whose sub-group you want to delete.
2. From the list of sub-groups, select the sub-group you want to delete.
3. Click [Delete].
The system will ask you to confirm the deletion.
4. Click [OK] to delete the sub-group.

ADD/EDIT CONFIGURATION PROPERTIES

Perform the following steps to add configuration properties to an application object or an application's sub-group. To do so, the logged-in user must have the *PSAC_addApplicationProperty* and *PSAC_editApplicationProperty* privileges, respectively.

To create a new configuration property, proceed as follows:

1. From the list of application objects or sub-groups, select the application object or sub-group for which you want to create configuration properties.
2. In the button bar below the list of application objects, click [Add property] and select the appropriate property type button. The following types are available: **String, Long, Decimal, Boolean, Object**.

The system displays the **Add <Property Type> Property** dialog.

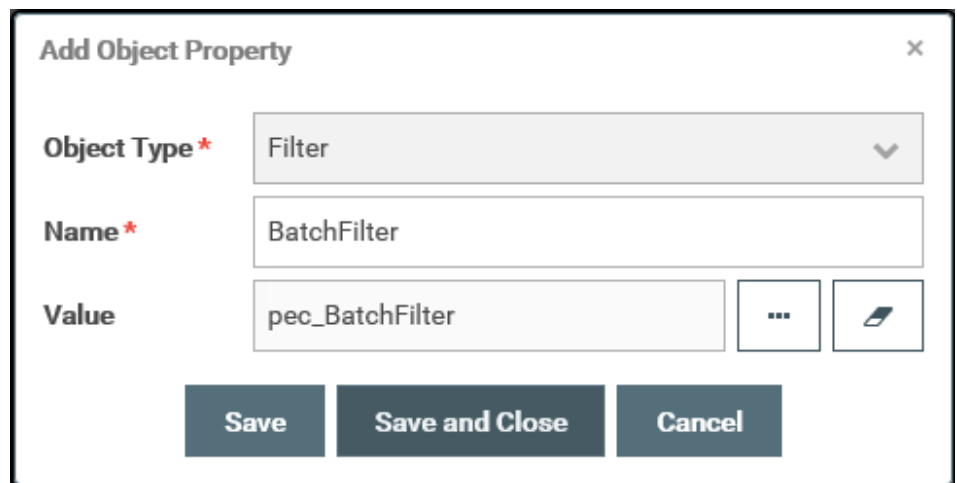


Figure 37: Add Object Property dialog

3. Define the following properties:

■ Object Type

TIP

This property is only available for configuration properties of the **Object** property type.

Select an object type from the drop-down menu. The following options are available: **Filter, List, Location, Report Designs, Subroutine**. The type is a mandatory property.

■ Name

Enter the name of the configuration property. The name is a mandatory property.

■ Value

The value depends on the property type.

■ **String, Long, Decimal**

Enter the value of the configuration property.

TIP

In case a **Long** property is saved without providing a value, the system displays -1.

■ **Boolean**

Select one of the following options: **Yes** (default) or **No**.

■ **Object**

Click [...] to open the **Select Object** dialog. Select the object and click [OK].

To clear the box, click the eraser button.

4. When you have completed your data entry, you can

- either click [Save] if you are going to add more configuration properties of the current type.

The system saves the data and keeps the dialog open for adding another configuration property.

- or click [Save and Close] to close the dialog.

- or click [Cancel] to close the dialog without saving the entered data.

To edit an existing configuration property, select the configuration property you want to edit.

1. Click [Edit]

The system displays the **Edit <Property Type> Property** dialog.

Figure 38: Edit Object Property dialog

2. Change the data as required.

TIP

Please note that when **Station Class** values are edited, they are inherited by the **Station Objects** assigned to the class.

3. When you have completed your data entry, you can
 - click [Save] to close the dialog after changing the data of your configuration property
 - or click [Cancel] to close the dialog without saving the entered data.

DELETE CONFIGURATION PROPERTIES

Perform the following steps to delete configuration properties from an application object or an application's sub-group. To do so, the logged-in user must have the *PSAC_deleteApplicationProperty* privilege.

To delete a configuration property, proceed as follows:

1. From the list of application objects or sub-groups, select the application object or sub-group whose configuration property you want to delete.
2. From the list of configuration properties below the list of application objects, select the configuration property you want to delete.
3. In the button bar below the list of application objects, click [Delete].
The system will ask you to confirm the deletion.
4. Click [OK] to delete the configuration property.

Assign Resources to Applications

Perform the following steps to assign users, user groups, and stations to application objects to define to which users, user groups, and stations the application object applies. To do so, the logged-in user must have the *PSAC_assignApplication* privilege and the privilege that corresponds to the object type to be assigned (*PSAC_assignUserForApplication*, *PSAC_assignUserGroupForApplication*, *PSAC_assignStationForApplication*).

To assign users, user groups, or stations to application objects, proceed as follows:

1. From the list of application objects, select the application object to which you want to assign resources.
2. Click [Assign] and select the appropriate resource button.

3. To add assignments, in the first column, select the checkbox of each resource you want to assign to the application object. To remove assignments, in the first column, unselect the checkbox of each resource you want to remove from the application object.

Use the filter to narrow down the list of resources displayed.

The dialog box titled "Assign User Groups" contains a search section with two filters: "Name" (set to "Starts With" and "P") and "Description" (set to "Any"). A "Search" button is located below the filters. Below the search section is a table with two columns: "Name" and "Description". The table lists ten user groups, each with a checkbox in the first column. At the bottom of the dialog are "Save" and "Close" buttons.

	Name	Description
<input type="checkbox"/>	PlantOpsAdmin	PlantOps Administrators
<input type="checkbox"/>	PlantOpsDesign	PlantOps Designers
<input type="checkbox"/>	PlantOpsGuest	PlantOps Guests
<input type="checkbox"/>	PlantOpsOpera	PlantOps Operators
<input type="checkbox"/>	PlantOpsSuper	PlantOps Supervisors
<input type="checkbox"/>	PMOperators	PMOperators have the ability to work with jobs and runtime ev
<input type="checkbox"/>	PMSupervisors	PMSupervisors can add job privileges and use the summary c
<input type="checkbox"/>	PSACFunctiona	User group for Functional Administration
<input type="checkbox"/>	PSACUserAdm	User group for User Administration

Figure 39: Assign User Groups dialog

4. Make your changes and
- either click [Save] to close the dialog and apply the assignments
 - or click [Close] to retain the old assignments without changes.

TIP

The assigned resources are displayed in the **Assignment** box.

Delete Applications

Perform the following steps to delete application objects. To do so, the logged-in user must have the *PSAC_deleteApplication* privilege.

To delete an application object, proceed as follows:

1. From the list of application objects, select the application object you want to delete.
2. Click [Delete].
The system will ask you to confirm the deletion.
3. Click [OK] to delete the application object.

TIP

An application object that is a base application of another application object or is assigned to any resource e.g. users, user groups or stations, cannot be deleted.

Appendix - Default Privileges and User Groups (PS Administration)

This appendix lists the privileges and user groups that are provided by default with PS Administration.

Privileges (PS Administration)

These tables list the default privileges available for PS Administration, separated by areas.

Access Privileges

Privilege	Description
PSAC_addAccessPrivilege	Allows creation of access privileges.
PSAC_assignUserGroupToAccessPrivilegePerformers	Allows assignment of user groups to access privileges. For access privileges of the Signature privilege type, allows assignment of performer user groups.
PSAC_assignUserGroupToAccessPrivilegeVerifiers	For access privileges of the Signature privilege type, allows assignment of verifier user groups.
PSAC_deleteAccessPrivilege	Allows deletion of access privileges.
PSAC_deleteSignature	Allows deletion of signatures from an access privilege of the Signature privilege type.
PSAC_editAccessPrivilege	Allows modification of access privileges.
PSAC_editSignature	Allows creation and modification of signatures for an access privilege of the Signature privilege type.
PSAC_exportAccessPrivilege	Allows the export of access privileges.
PSAC_importAccessPrivilege	Allows the import of access privileges.
PSAC_viewAccessPrivilege	Allows access to the Access Privileges editor.

Applications

Privilege	Description
PSAC_addApplication	Allows creation of applications.
PSAC_addApplicationProperty	Allows creation of properties of an application.
PSAC_assignApplication	Allows assignment of resources to applications.
PSAC_assignStationForApplication	Allows assignment of stations to applications.
PSAC_assignUserForApplication	Allows assignment of users to applications.
PSAC_assignUserGroupForApplication	Allows assignment of user groups to applications.
PSAC_deleteApplication	Allows deletion of applications.
PSAC_deleteApplicationProperty	Allows deletion of properties from an application.
PSAC_editApplication	Allows modification of applications.
PSAC_editApplicationProperty	Allows modification of properties of an application.
PSAC_exportApplication	Allows the export of applications.
PSAC_importApplication	Allows the import of applications.
PSAC_viewApplication	Allows access to the Applications editor.

Users

Privilege	Description
PSAC_addUser	Allows creation of users.
PSAC_assignUserGroupToUser	Allows assignment of user groups to users.
PSAC_changeUserPassword	Allows access to the Change Password dialog.
PSAC_disableUser	Allows disabling another user.
PSAC_editUser	Allows modification of users.
PSAC_exportUser	Allows the export of users.
PSAC_importUser	Allows the import of users.
PSAC_viewUser	Allows access into the User editor.

User groups

Privilege	Description
PSAC_editUserGroup	Allows the following: <ul style="list-style-type: none">■ Add and remove users from user groups.■ Change the user group-to-privilege mapping.
PSAC_addUserGroup	Allows creation of users group.
PSAC_assignUserGroupToUser	Allows assignment of user groups to users.
PSAC_deleteUserGroup	Allows deletion of user groups.
PSAC_exportUserGroup	Allows the export of user groups.
PSAC_importUserGroup	Allows the import of user groups.
PSAC_viewUserGroup	Allows access to the User Group editor.

Lists

Privilege	Description
deleteList	Allows deletion of lists.
editList	Allows creation, modification, import, and export of lists.
viewList	Allows access to the List editor.

User Groups (PS Administration)

The following tables list the user groups that are provided by default and the PS Administration-specific privileges that are assigned to them.

Authors

Authors can edit all of the configuration information in the system, but they do not have the ability to perform deletions.

Privileges	
editList	viewList

PSACFunctionalAdmin

PSACFunctionalAdmin administrators can perform all of the actions associated with lists, access privileges, and applications.

Privileges	
deleteList	PSAC_deleteApplicationProperty
editList	PSAC_deleteSignature
PSAC_addAccessPrivilege	PSAC_editAccessPrivilege
PSAC_addApplication	PSAC_editApplication
PSAC_addApplicationProperty	PSAC_editApplicationProperty
PSAC_assignApplication	PSAC_editSignature
PSAC_assignStationForApplication	PSAC_exportAccessPrivilege
PSAC_assignUserForApplication	PSAC_exportApplication
PSAC_assignUserGroupForApplication	PSAC_importAccessPrivilege
PSAC_assignUserGroupToAccessPrivilegePer formers	PSAC_importApplication
PSAC_assignUserGroupToAccessPrivilegeVer ifiers	PSAC_viewAccessPrivilege
PSAC_deleteAccessPrivilege	PSAC_viewApplication
PSAC_deleteApplication	viewList

PSACUserAdmin

PSACUserAdmin administrators can perform all of the actions associated with users and user groups.

Privileges	
PSAC_addUser	PSAC_editUserGroup
PSAC_addUserGroup	PSAC_exportUser
PSAC_assignUserGroupToUser	PSAC_exportUserGroup
PSAC_changeUserPassword	PSAC_importUser
PSAC_deleteUserGroup	PSAC_importUserGroup
PSAC_disableUser	PSAC_viewUser
PSAC_editUser	PSAC_viewUserGroup

SuperAuthors

SuperAuthors have the ability to manipulate all system configurations.

Privileges	
deleteList	viewList
editList	

Viewers

Viewers are the read-only users of the system. They cannot make any changes.

Privileges
viewList

-
-
- PS Administration - Implementation Guide
-
-

A

Access privileges • 36

Adding • 42

Confidential object • 52

Deleting • 57

Editing • 42

Exporting • 36

Filters • 39

Importing • 36

Privileges • 69

Adding

Access privileges • 42

Applications • 58

Changing • 27

Properties • 62

Station objects • 60

Sub-group objects • 60

Sub-groups • 60

User groups • 33

Users • 22

Administration user • 3

Applications • 57

Adding • 58

Deleting • 67

Editing • 58

Exporting • 57

Importing • 57

Privileges • 69

Assigning

Access privileges to user groups • 34

Start forms to users • 25

Stations to applications • 65

User groups to access privileges • 55

User groups to applications • 65

User groups to users • 26

Users to applications • 65

Users to user groups • 35

Audience • 1

C

Conventions (typographical) • 1

D

Defining

Signatures • 49

Deleting

Access privileges • 57

Applications • 67

Properties • 65

Signatures • 52

Station objects • 62

Sub-group objects • 62

Sub-groups • 62

User Groups • 36

Disabling

Users • 29

E

Editing

Access privileges • 42

Applications • 58

Properties • 62

User groups • 33

Users • 22

Enabling

Users • 29

Expectations • 1

Exporting

Access privileges • 36

Applications • 57

User groups • 30

Users • 17

F

Filters

- Access privileges • 39
- User groups • 31
- Users • 18

I

- Importing
 - Access privileges • 36
 - Applications • 57
 - User groups • 30
 - Users • 17

L

- Lists
 - Privileges • 71

P

- Privileges • 69
- Properties
 - Adding • 62
 - Deleting • 65
 - Editing • 62
- PS Administration • 5
 - Installing • 10
 - Uninstalling • 16

S

- Signatures
 - Defining • 49
 - Deleting • 52
- Stations
 - Adding objects • 60
 - Assigning to applications • 65
 - Deleting objects • 62
- Sub-groups
 - Adding • 60
 - Adding objects • 60
 - Deleting • 62
 - Deleting objects • 62

T

- Technical support • 3
- Typographical conventions • 1

U

- User groups • 30
 - Adding • 33
 - Assigning access privileges • 34
 - Assigning to access privileges • 55
 - Assigning to applications • 65
 - Assigning users • 35
 - Authors • 71
 - Available user groups (PharmaSuite) • 6
 - Deleting • 36
 - Editing • 33
 - Exporting • 30
 - Filters • 31
 - Importing • 30
 - Privileges • 70
 - PSACFunctionalAdmin • 71
 - PSACUserAdmin • 72
 - SuperAuthors • 72
 - Viewers • 72
- Users • 17
 - Adding • 22
 - Assigning start forms • 25
 - Assigning to applications • 65
 - Assigning user groups • 26
 - Available users (PharmaSuite) • 6
 - Changing password • 27
 - Disabling • 29
 - Editing • 22
 - Enabling • 29
 - Exporting • 17
 - Filters • 18
 - Importing • 17
 - Privileges • 70