PLA 3.0

Administration Guide

PLA

Version: 3.0.4

April 2021

STEGMANN SYSTEMS GmbH | Raiffeisenstr. 2 | 63110 Rodgau, Germany
Fon: +49 6106 77010-0 | Fax: +49 6106 77010-190 | info@stegmannsystems.com
www.stegmannsystems.com | www.bioassay.de | www.aps-info.de

STEGMANN SYSTEMS

Contents

1 Introduction to the Administration Guide

PLA 3.0 is your software for biostatistical analysis in R&D and regulated environments. This guide is intended for both system and functional administrators.

Purpose and structure of this document

PLA 3.0 consists of the PLA 3.0 Framework and PLA 3.0 add-ons. The PLA 3.0 Framework provides the features you need to achieve regulatory compliance. It handles data as electronic documents and supports access control, data integrity, security, validation, and traceability. PLA 3.0 add-ons, such as the Biological Assays Package for the pharmaceutical industry or the Dose-Response Analysis Package, extend the functionality of PLA to include the analytical methods your users require.

This guide is organized into four parts:

1. Introduction to the Administration Guide
2. Databases in PLA 3.0
3. Extensibility with PLA 3.0
4. Rights and permissions in PLA 3.0

In PLA 3.0, databases are not just used to store data. Each PLA 3.0 database also defines a work environment. This includes a range of information from structured documents that hold your data to user accounts, security contexts, signatures, and audit trails. The first part of this guide has the information you need to set up, monitor, and maintain PLA 3.0 databases in a compliant manner.

PLA 3.0 add-ons provide the analytical methods your users require and enable them to visualize, document, and report results. They also support a range of additional tasks from data acquisition to data aggregation and process monitoring using control charts. The second part of this guide has the information you need to install add-ons and make their functionality available to the users of particular PLA 3.0 databases.

PLA 3.0 provides the features you need to control access to your data in a sophisticated and compliant manner. It combines role-based user rights with resource-based permissions, which enable you to exercise very fine-grained control over who is allowed to perform particular tasks in a given context and which tasks are allowed with particular data. The third part of this guide has the information you need to set up users, groups, security contexts, and more.

Typographic conventions

This guide consists of concept and reference sections. Concept sections provide brief introductions to a feature or dialog. Reference sections describe the UI controls of a feature or dialog in detail. Each reference section has a "menu cascade" that indicates how you access the feature or dialog it describes.

The following menu cascade, for example, indicates how you access the Security tab of the Database policies dialog:

System menu **>** Database policies **>** Security tab

Throughout this guide, names of UI controls are indicated by upper case initials such as in "System menu", "Database policies", and "Security tab".

2 Databases in PLA 3.0

In PLA 3.0, databases are not just used to store data. Each PLA 3.0 database also defines a work environment. This includes a range of information from structured documents that hold your data to user accounts, security contexts, signatures, and audit trails. We therefore recommend to use separate databases for tasks that require different work environments. For example, use one database to test setups for databases and documents and a second database for production.

Current regulations, such as 21 CFR 11.10 in the pharmaceutical industry, require you to ensure that only authorized individuals can access your systems, perform operations, and sign records. The database-driven approach of PLA 3.0 enables you to take major steps toward meeting these requirements. Since most settings in PLA apply to individual databases, they allow you to differentiate, for example, between production and test databases. To enable you to create new databases more efficiently, PLA provides a database template feature. You use existing databases as templates for creating new databases.

Note: PLA supports two database types, that is, file-based SQLite databases and Microsoft SQL Server databases. We recommend Microsoft SQL Server databases for production purposes and for simultaneous access in multi-user environments.

The following three sections provide information on administering PLA 3.0 databases:

- Database settings
  - Database policies: System-idle lock, password policies, compliant signatures, traceability of changes to documents and protected values, database templates
  - Database info (PLA 3.0.5)/ Database properties (PLA 3.0.4): Description of database, dashboard for database
  - Configuration report: Report on database configuration
- Database monitoring
  - Audit trail
  - Session management
- Database maintenance

2.1 Database settings

Establish consistent policies for a range of features, such as passwords, signatures, and traceability, that control and document user access to individual databases.

The following three dialogs allow you to tailor database settings to your needs:

- Database policies: System-idle lock, password policies, compliant signatures, traceability of changes to documents and protected values, database templates
- Database info (PLA 3.0.5)/ Database properties (PLA 3.0.4): Description of database, dashboard for database
- Configuration report: Report on database configuration

2.1.1 Database policies

Control and document aspects of how users access individual databases.

System menu > Database policies

The Database policies dialog allows you to set password policies and the system-idle lock, enable compliant electronic signatures, require users to specify why they change data, enable database templates, and more.

2.1.1.1 Security

Set the system-idle lock and password policies for individual databases to ensure that passwords of authorized users are sufficiently strong and that users change their passwords as often as deemed necessary by your organization.

System menu > Database policies > Security tab

Note: The PLA password policy settings available in this dialog are primarily intended for file-based SQLite databases that do not provide their own access control beyond the file system permissions of the database files. We recommend Microsoft SQL Server databases for production purposes and for simultaneous access in multi-user environments.

Tip: PLA allows you to use directory services based on LDAPS, such as Microsoft Active Directory Domain Services, to handle user authentication. Active Directory allows you to enforce greater password complexity and to prevent user names from being employed as passwords. Please consult the Directory service configuration section of the Administration Guide for additional information.

Section	Item	Description
System	Idle lock interval [min]	The system automatically locks for users who have stopped interacting with it for the number of minutes specified here. Users who are locked out have to re-enter their password. Enter "0" to disable this option.
Password	Minimum length	The system accepts passwords that do not have fewer characters than the number specified here. **Note:** The number you enter for Minimum length cannot be greater than Maximum length.

Minimum number of special characters	The system accepts passwords that do not have fewer special characters than the number specified here. Special characters are characters that are neither letters nor numbers such as @, #, !, ", %, &, (,), *, +. **Note:** The number you enter for Minimum number of special characters cannot be greater than Maximum length.
Maximum length	The system accepts passwords that do not have more characters than the number specified here. **Note:** The number you enter for Maximum length cannot be less than Minimum length.
Maximum age [d]	The system accepts passwords that are not older than the number of days specified here. Users have to change their password when it has reached Maximum age. Enter "0" to disable this option. **Note:** The number you enter for Maximum age cannot be less than Minimum age. **Tip:** Current regulations, such as 21 CFR 11.300(b) in the pharmaceutical industry, require you to implement policies with regard to password aging.
Warning age [d]	Prompts users to change passwords that are older than the number of days specified here. Enter "0" to disable this option.
Minimum age [d]	Allows users to change passwords that are at least as old as the number of days specified here. Enter "0" to disable this option. **Note:** The number you enter for Minimum age cannot be greater than Maximum age. **Tip:** Enable this option in conjunction with a password history policy (see History length option below) to effectively discourage users from reusing old passwords.

Maximum age blocks account	Locks user accounts whose password has reached Maximum age. An administrator has to access PLA and unlock user accounts whose password has reached Maximum age. **Warning:** If you enable this option and the password of the Administrator account reaches Maximum age, the administrator is locked out of the system. **Note:** If you disable this option, users still have to change their password when it has reached Maximum age. Yet no Unlock action by an administrator is required (see: System menu > Account management > Users section > Unlock now).
Maximum failures	Locks user accounts that have the number of failed consecutive logins specified here.
Failure grace interval [min]	Locks user accounts for the number of minutes specified here when they have reached Maximum failures. Enter "0" to keep accounts locked until an administrator unlocks them manually.
History length	Specifies the number of consecutive unique passwords saved for individual user accounts. Determines how often users have to change their password before they can reuse previous passwords of the same account. Enter "0" to keep all previous passwords and prevent passwords from being used ever again for the same account. **Tip:** Enable this option in conjunction with a password minimum age (see Minimum age option above) to effectively discourage users from reusing old passwords.
List of invalid passwords	Prevents the character strings listed from being used as passwords. Click the Edit button to open the Manage invalid passwords dialog, which allows you to edit the Invalid passwords list. **Note:** This feature is case-sensitive. If you add the character string "password" to the list, you do not prevent users from using "Password".

Example: Password policies
The following table provides an example of valid entries for all password policy options.

Item	Example of valid setting
Minimum lenth	8
Minimum number of special characters	1

Maximum length	16
Maximum age [d]	90
Warning age [d]	14
Minimum age [d]	3
Maximum age blocks account	enabled
Maximum failures	2
Failure grace interval [min]	0
History length	5
List of invalid passwords	password Password

2.1.1.2 Signatures and regulatory compliance

Enable elecronic signatures. Specify how signatures are created and how signed documents are handled to make signatures compliant with current regulations such as 21 CFR 11.100 and 11.200 in the pharmaceutical industry.

System menu **>** Database policies **>** Signatures tab

Section	**Item**	**Description**
General	Requires user name	Requires users to enter their user name every time they want to sign documents or remove signatures. The system only accepts the user name of the user who is currently logged in. **Note:** If you disable this option, the user name of the current user is recorded automatically.
Document signatures	Templates for electronic signatures	Provides users with a list of valid reasons for signing documents and removing signatures. **Note:** When users sign a document or remove a signature and are prompted to provide a reason for their actions, they can either type the reason into a text box or select an option provided by the Template list. **Tip:** Click the Edit button to open the Manage templates dialog, which allows you to edit the Template list.

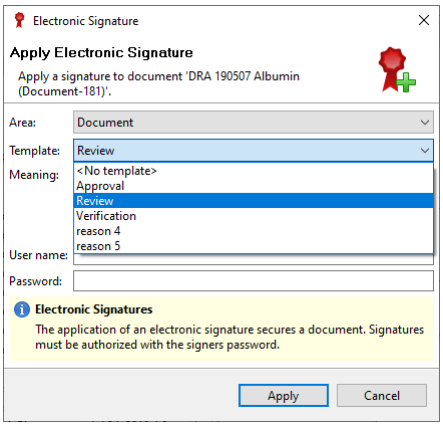
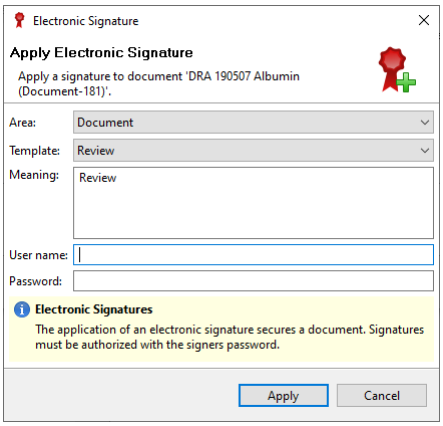
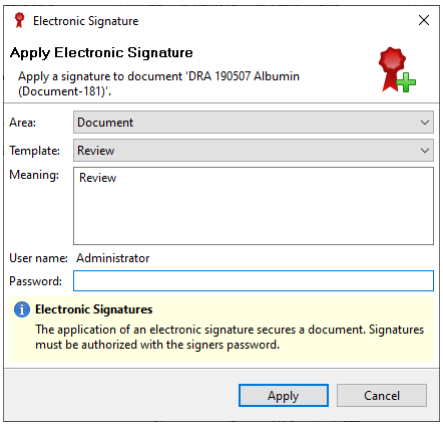
	Deny signature removal	Prevents the removal of signatures even by users who have the permissions required to remove signatures.
	Deny deletion of signed documents	Prevents the deletion of signed documents even by users who have the permissions required to delete signed documents.
	Deny deletion of documents containing signatures	Prevents the deletion of documents that contain signed sections or "scopes" even by users who have the permissions required to delete signed sections or "scopes".

Example: Signature compliance with 21 CFR Part 11
Select the following options to make your signatures compliant with 21 CFR Part 11.

Item	Required setting
Requires user name	enabled
Deny signature removal	enabled
Deny deletion of signed documents	enabled
Deny deletion of documents containing signatures	enabled

Example: Requires user name
The following table shows the Apply electronic signature dialog, which prompts users to enter information when they sign documents or remove signatures. The screenshots and descriptions indicate how the two settings "Templates for electronic signatures" and "Require user name" affect the dialog.

Item	Description

	Figure 1 shows the dialog with the Template drop-down list displayed: The list consists of all entries provided in the Manage templates dialog, which you access from the Signatures tab of the Database policies dialog. **Tip:** If your organization provides standardized reasons for signing documents and removing signatures, users can select one from the Template drop-down list, which is then inserted in the Meaning text box. Users can still type additional information into the text box.
	Figure 2 shows the dialog with the "Requires user name" option enabled on the Signatures tab: It displays three text boxes where users enter the reason for signing, their user name, and their password. **Note:** Some regulations, such as 21 CFR 11.200 in the pharmaceutical industry, require signatures to "employ at least two distinct identification components". Your organization is on the safe side if you require users to manually enter both user name and password provided that user name and password are not identical strings.
	Figure 3 shows the dialog with the "Requires user name" option disabled on the Signatures tab: It displays two text boxes where users enter the reason for signing and their password. **Note:** PLA automatically inserts the user name of the current user, which is "Administrator" in this example.

2.1.1.3 Traceability

Adjust how PLA traces changes to documents and protected values. Require users to specify why they modify documents and protected values to improve traceability and protect data from intentional and unintentional changes.

System menu > Database policies > Traceability tab

Section	Item	Description
Changes to documents	Templates for reasons to change	Provides users with a list of valid reasons for making changes to documents. **Note:** When users save a document and are prompted to provide a reason for their changes, they can either type the reason into a text box or select an option provided by the Template list. **Tip:** Click the Edit button to open the Manage templates dialog, which allows you to edit the Template list.
	Request reasons for change	Specifies whether users who save a document are prompted to explain why they made changes to the document. Available options • Never: When users save a document after making changes, they do not have the opportunity to provide a reason for their changes. • Optional: Displays the Reason for change dialog when users save a document. The dialog gives them the opportunity to enter a reason for their changes. **Note:** Users can leave the Reason for change dialog empty and still save the document. • Always: Displays the Reason for change dialog when users save a document. They cannot save the document without entering a reason for their changes. • Always after initial saving: Displays the Reason for change dialog when users save a document. The dialog does not get displayed when users save a new document for the first time. In all other cases, users cannot save the document without entering a reason for their changes.
Changes to protected values	Templates for reasons for change	Provides users with a list of valid reasons for making changes to protected values. **Note:** When users change a protected value and are prompted to provide a reason for their changes, they can either type the reason into a text box or select an option provided by the Template list. **Tip:** Click the Edit button to open the Manage templates dialog, which allows you to edit the Template list.

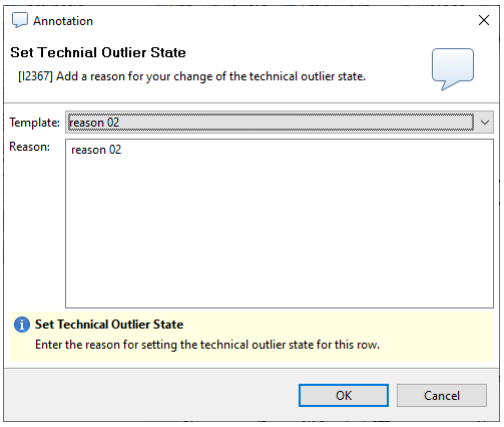
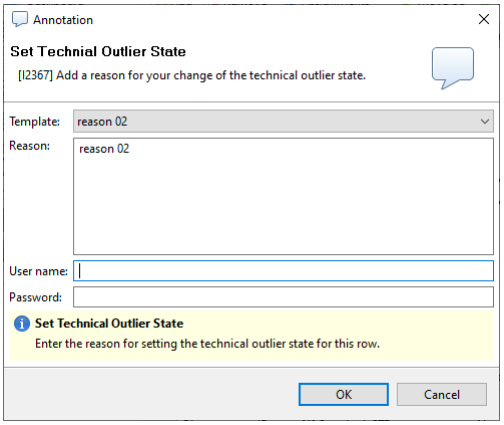
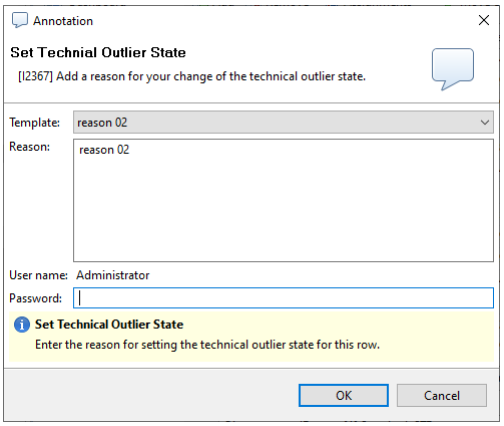
Manual change	Specifies whether users are permitted to change protected values and, if they are permitted, whether users are prompted to explain why they made changes and whether they have to provide their user name and password. Available options • Forbidden: No changes are permitted. In the Observations table and related data views accessible to users, protected values are grayed out and not available for editing. • Permitted with reason and signature: Changes are permitted, but users are prompted to provide a reason for their changes and to enter their user name and password. **Note:** With this setting, the dialog displayed to prompt users depends on how signatures are set up. Users are always prompted to enter a reason for their changes and their password. In addition, users are prompted to enter their user name if the "Requires user name" option is enabled on the Signatures tab. • Permitted with reason: Changes are permitted, but users are prompted to provide a reason for their changes. • Permitted: Changes are permitted. **Note:** Irrespective of the option you select, PLA adds an annotation to protected values that have been modified. To display the annotation, right-click the value in the Observations table and select the Show annotations option from the context menu.
Change by import	Specifies whether data acquisition processes are permitted to change protected values. Available options • Forbidden: No changes are permitted. In the Observations table and related data views accessible to users, protected values are grayed out and cannot be modified by another import or data acquisition. • Permitted: Changes are permitted. **Note:** Irrespective of the option you select, PLA adds an annotation to protected values that have been modified. To display the annotation, right-click the value in the Observations table and select the Show annotations option from the context menu.

	Change technical outlier state	Specifies whether users are permitted to change the technical outlier state (true or false) of observed values and, if they are permitted, whether users are prompted to explain why they made changes and whether they have to provide their user name and password. Available options • Forbidden: No changes are permitted. In the Observations table, technical outlier states are grayed out and not available for editing. • Permitted with reason and signature: Changes are permitted, but users are prompted to provide a reason for their changes and to enter their user name and password. **Note:** With this setting, the dialog displayed to prompt users depends on how signatures are set up. Users are always prompted to enter a reason for their changes and their password. In addition, users are prompted to enter their user name if the "Requires user name" option is enabled on the Signatures tab. • Permitted with reason: Changes are permitted, but users are prompted to provide a reason for their changes. • Permitted: Changes are permitted. **Note:** Irrespective of the option you select, PLA adds an annotation to technical outlier states that have been modified. To display the annotation, right-click the value in the Observations table and select the Show annotations option from the context menu.

Example: Change technical outlier state settings
The following table shows the Set technical outlier state dialog, which prompts users to enter information when they change the technical outlier state (true or false) of observed values. The screenshots and descriptions indicate how the two settings "Permitted with reason" and "Permitted with reason and signature" affect the dialog. They also indicate how the "Requires user name" option of the Signatures tab affects the dialog when the setting "Permitted with rason and signature" is enabled.

Tip: Apply these settings under "Manual change" rather than "Change technical outlier state" to define the dialog that prompts users when they manually change protected values.

Item	Description

	Figure 1 shows the dialog for the setting "Permitted with reason": It displays one text box where users enter the reason for changing the technical outlier state of an observed value. **Tip:** If your organization provides standardized reasons, users can select one from the Template drop-down list, which is then inserted in the Reason text box. Users can still type additional information into the text box.
	Figure 2 shows the dialog for the setting "Permitted with reason and signature" with the "Requires user name" option enabled on the Signatures tab: It displays three text boxes where users enter the reason for making changes, their user name, and their password.
	Figure 3 shows the dialog for the setting "Permitted with reason and signature" with the "Requires user name" option disabled on the Signatures tab: It displays two text boxes where users enter the reason for making changes and their password. **Note:** PLA automatically inserts the user name of the current user, which is "Administrator" in this example.

2.1.1.4 Advanced

Enable draft components, use of databases as templates, automatic check of component package versions, changes to document and folder keys, and automatic saving of new, unedited documents.

System menu > Database policies > Advanced tab

Section	Item	Description

Development	Activate draft components	Enables users to preview and test custom components, such as custom reports, in draft mode prior to their release. **Note:** You do not need this feature if users only work with components that have been released.
Behavior	Allow usage as database template	Enables users who create new databases to employ this database as a template.
	Activate check for updateable component packages	Compares the versions of installed components with the versions evident in databases. This is automatically done when users connect to the database. PLA informs users if components installed on their computers are newer than the versions evident in the database. **Note:** We recommend to always use the most recently released versions of components.
Documents and folders	Deny change document or folder keys	Prevents changes to document keys and folder keys even by users who have the permissions required to change these keys.
	Save new documents before editing the first time	Causes new, unedited documents to be saved automatically. Available options • Always: Induces automatic saving of all new documents. • Only at creation from templates: Only induces automatic saving when users create new documents from templates. • Never: Disables automatic saving of new documents. **Note:** With this feature enabled, PLA creates empty documents in the database and then opens them for editing. With this feature disabled, PLA opens empty documents in the editor and only adds them to the database when users manually save them for the first time. **Tip:** Enable this feature to ensure that PLA logs all changes to documents from their creation. If users create documents from templates, this allows you to track all changes that cause discrepancies between documents and templates.
Database	UUID	Displays the universally unique identifier of databases.

2.1.2 Database info

Provide information on databases to improve navigation and to support users who work with them.

System menu > Database info (PLA 3.0.5)/ Database properties (PLA 3.0.4)

Section	Item	Description
Summary tab (PLA 3.0.5)/ General tab (PLA 3.0.4)	Database name text box (PLA 3.0.5)/ Label text box (PLA 3.0.4)	PLA displays the information you enter here in the PLA database management dialog when users employ this database as a template to create new databases. **Note:** Users can employ this database as a template if the Allow usage as database template option is enabled on the Advanced tab of the Database policies dialog.
	Brief description text box (PLA 3.0.5)/ Description text box (PLA 3.0.4)	
Detailed information tab (PLA 3.0.5)/ Dashboard tab (PLA 3.0.4)	text box	PLA displays the information you enter here on the database dashboard when users open the database. **Tip:** This feature allows you to provide pertinent, HTML-formatted information to all users of the database.

2.1.3 Database configuration report

Enable authorized users to generate customized PDF reports that document and communicate pertinent information on database configurations.

System menu > Configuration report

Section	Item	Description
Settings tab	Target folder	Specifies the folder where database configuration reports are to be stored.
	Report configuration	Specifies the items to be included in database configuration reports. **Tip:** Please consult the Configuration report section of the User Guide for additional information that details the permissions users require to access specific database configuration items.

Tasks tab	Table field	Displays progress when you generate configuration reports. • Task column: Lists all configuration items that have already been processed. • Message column: Indicates the status of each item that has been processed.

2.2 Database monitoring

Monitor user sessions and document locks. Maintain a permanent record of all relevant events related to user access, changes in work environments, and changes to data for each individual PLA database and document.

The following three dialogs provide access to database monitoring features:

- Session management
- Audit trail (system context)
- Audit trail (document context)

2.2.1 Session management

View and manage the sessions of all users who are currently connected to the database. The upper table of the Session management dialog lists all sessions. Select a session to display all its document locks in the lower table.

System menu **>** Session management

When users log into PLA databases, PLA assigns separate sessions to individual users. Each session is valid for one particular user and database and has a unique ID, which PLA saves to the database. When users open PLA documents, their session IDs lock the documents for other users. PLA unlocks documents when users close them. When users log out of databases, PLA unlocks all documents locked by their session IDs and deletes their session IDs from the databases.

Note: PLA checks every five minutes if sessions are obsolete. When users get disconnected from databases, PLA deletes their sessions.

Item	Description
Auto-refresh rate	Specifies whether the session and lock tables displayed in the dialog are to be automatically refreshed. The drop-down list provides time interval options in seconds (s) and minutes (m).
Refresh	Refreshes the session and lock tables displayed in the dialog.

Kill session	Terminates the session currently selected in the dialog, and unlocks all its documents and folders. **Note:** We do not recommend to use this command unless obsolete sessions remain after users failed to properly close PLA.
Remove all locks	Unlocks all documents that belong to the session currently selected in the dialog. **Note:** We do not recommend to use this command unless documents remain locked by obsolete sessions after users failed to properly close PLA.
Remove lock	Unlocks the document currently selected in the dialog. **Note:** We do not recommend to use this command unless documents remain locked by obsolete sessions after users failed to properly close PLA.

2.2.2 Audit trail

Interpret the audit trail. Track and communicate events related to user access, changes in work environments, and changes to data for each individual PLA database and document. The upper table of the Audit trail dialog lists all recorded "actions". Select an action to display all affected elements and their values in the lower table.

PLA provides both system and document audit trails:

System menu > Audit trail

Open document > Editor bar > Audit trail button

Audit trails and regulatory compliance
Current regulations, such as 21 CFR 11.10 in the pharmaceutical industry, require you to document user access to the system and all actions that create, modify, or delete records. PLA audit trails enable you to take major steps toward meeting these requirements. PLA provides a seperate secure audit trail for each individual PLA database and document.

Audit trails record all user login and logout events of individual databases, all changes to the database settings, and all changes to the documents saved in individual databases. For every recorded event, audit trails provide a time stamp and all modified values.

System and document audit trails provide the following information:

- System audit trail: Contains all recorded events of an individual database.
- Document audit trail: Contains all recorded events that relate to an individual document. The events provided by a document audit trail are a subset of those recorded in the system audit trail of the document's database.

Note: Some system events are not included in the document audit trails.

Note: Users require permissions to access system and document audit trails. Please consult the Global permissions section of the Administration Guide for additional information.

Tip: PLA provides advanced features to enhance the experience of users who work with audit trails:

- Filter dialog: Enables users to filter the entries of individual audit trails by user, date, action, and object.
- Export dialog: Allows users to export entire audit trails or the entries provided by previously defined filters.

Please consult the Audit trail section of the User Guide for additional information.

Information recorded in audit trails
Each audit trail entry provides the following information on an individual action.

Section	Item	Description
Audit trail table (upper table)	#	Consecutive number of the audit trail entry provided in this table row: These numbers are unique within the audit trails of individual databases.
	Time stamp	Time of entry: PLA provides time stamps with millisecond precision. Time stamps are not necessarily unique within audit trails.
	Action	Action type key: PLA provides uniform keys to indicate what type of action has been recorded.
	Object	Object name: The action recorded in this table row was performed on this object.
	Operator	User name of the operator: This PLA user performed the action recorded in this table row.
	Host name	NetBIOS name of the computer: The PLA instance used to perform the action was started on this computer.
	Serial	PLA license used: Depending on the type of license used, this may be a ProtectionKey ID, a serial number or hardware ID, or a test version ID.
Object table (lower table)	Key	Object property: The object properties listed in this column were affected by the action selected in the upper table.
	Operation	Operation type: This type of operation was performed on the object property listed in this table row.

	Old value	Value of the element prior to the operation: If the operation created the element, no value is displayed. The values of passwords are never displayed.
	New value	Value of the element after the operation: If the operation deleted the element, no value is displayed. The values of passwords are never displayed.

Actions and their keys recorded in audit trails

The following table provides the "actions" recorded in audit trails and the keys used to represent them.

Section	Item	Description
Schemas	SCHEMA_INIT	The database schema was initialized.
	SCHEMA_UPDATE	The database schema was updated.
Information packages	INFORMATIONPACKAGE_INITIAL	An information package was imported for the first time for this serial number.
	INFORMATIONPACKAGE_SAVED	An information package was updated for this serial number.
Add-ons, components, OQ packages, OSGI bundles, document packages	COMPONENT_INITIAL	A component was created.
	COMPONENT_SAVED	A component was saved.
	COMPONENT_UPDATED	A component was updated.
	COMPONENT_IMPORTED	A component was imported because a package was installed.
	COMPONENT_DELETE (to PLA 3.0.4), COMPONENT_DELETED (from PLA 3.0.5)	A component was deleted.
	ADDON_ACTIVATED (from PLA 3.0.5)	An add-on was activated in the database.
	ADDON_DEACTIVATED (from PLA 3.0.5)	An add-on was deactivated in the database.
	ADDON_CATALOG_IMPORTED (from PLA 3.0.5)	An add-on catalog file was imported.

	OQPACKAGE_INITIAL (from PLA 3.0.5)	An OQ package was created.
	OQPACKAGE_DELETED (from PLA 3.0.5)	An OQ package was deleted.
	OSGIBUNDLE_INITIAL (from PLA 3.0.5)	An OSGI bundle was created.
	OSGIBUNDLE_DELETED (from PLA 3.0.5)	An OSGI bundle was deleted.
IQ, OQ, PQ	IQ_EXECUTED	An installation qualification was executed.
	OQ_IMPORTED	An operational-qualification package was imported.
	OQ_EXECUTED	An operational qualification was executed.
	OQ_EXPORTED	An operational-qualification package was exported.
	PQ_IMPORTED	A performance qualification package was imported.
	PQ_EXECUTED	A performance qualification was executed.
	PQ_EXPORTED	A performance qualification package was exported.
Users, sessions	USER_INITIAL	A user was created.
	USER_SAVED	Changes to a user were saved.
	USER_DELETE (to PLA 3.0.4), USER_DELETED (from PLA 3.0.5)	A user was deleted.
	USER_LOGIN (to PLA 3.0.4), DB_ADD_SESSION (to PLA 3.0.4), USER_SESSION_OPENED (from PLA 3.0.5)	A user logged into the database, and a session was created for the user.
	USER_LOGINREJECTED (to PLA 3.0.4), USER_SESSION_DENIED (from PLA 3.0.5)	A user tried to log into the database, but the login failed.
	USER_LOGOUT (to PLA 3.0.4), DB_DELETE_SESSION (to PLA 3.0.4), USER_SESSION_CLOSED (from PLA 3.0.5)	A user logged out of the database, and the session of the user was deleted.

	DB_DELETE_SESSION (to PLA 3.0.4), USER_SESSION_DELETED (from PLA 3.0.5)	A user session was deleted in the database.
	DB_KILL_SESSION (to PLA 3.0.4), USER_SESSION_DELETED (from PLA 3.0.5)	A user session was deleted from the Session management dialog.
	USER_PWCHANGE (to PLA 3.0.4), USER_PASSWORD_CHANGED (from PLA 3.0.5)	A user account password was changed.
	USER_RESETPW (to PLA 3.0.4), USER_PASSWORD_CHANGED (from PLA 3.0.5)	A user account password was reset.
User groups	GROUP_INITIAL	A user group was created.
	GROUP_SAVED	Changes to a user group were saved.
	GROUP_DELETE (to PLA 3.0.4), GROUP_DELETED (from PLA 3.0.5)	A user group was deleted.
User roles	ROLE_INITIAL	A user role was created.
	ROLE_SAVED	Changes to a user role were saved.
	ROLE_DELETE (to PLA 3.0.4), ROLE_DELETED (from PLA 3.0.5)	A user role was deleted.
Folder properties, folder restrictions, security contexts	CONFIGURATIONCONTEXT_INITIAL	A configuration for the document key format was created.
	CONFIGURATIONCONTEXT_SAVED	Changes to a configuration for the document key format were saved.
	CONFIGURATIONCONTEXT_DELETED	A configuration for the document key format was deleted.
	RESTRICTIONCONTEXT_INITIAL	A configuration for document restrictions was created.
	RESTRICTIONCONTEXT_SAVED	Changes to a configuration for document restrictions were saved.

	RESTRICTIONCONTEXT_DELETED	A configuration for document restrictions was deleted.
	SECURITYCONTEXT_INITIAL	A security context was created.
	SECURITYCONTEXT_SAVED	Changes to a security context were saved.
	SECURITYCONTEXT_DELETE (to PLA 3.0.4), SECURITYCONTEXT_DELETED (from PLA 3.0.5)	A security context was deleted.
	FOLDER_PROPERTIES_SAVED	Changes to folder properties were saved.
Database policies, database properties	HTMLFRAGMENT_INITIAL	The HTML fragment for the database dashboard was created.
	HTMLFRAGMENT_SAVED	Changes to the HTML fragment for the database dashboard were saved.
	HTMLFRAGMENT_DELETED	The HTML fragment for the database dashboard was deleted.
	OPTION_MODIFIED (to PLA 3.0.4), DB_POLICIES_SAVED (from PLA 3.0.5)	Changes to the database policies were saved.
	DATABASE_PROPERTIES_SAVED	Changes to the database properties were saved.
	LDAP_PROPERTIES_SAVED	Changes to the LDAP properties were saved.
Database locks, system locks	DB_ADMINACCESS_ON	The database was locked for exclusive access.
	DB_ADMINACCESS_OFF	A lock for exclusive database access was removed.
	SYSTEM_LOCKED	PLA was locked.
	SYSTEM_UNLOCKED	PLA was unlocked.
	SYSTEM_UNLOCKREJECTED	An attempt to unlock PLA was rejected.

	ACCOUNT_MANAGEMENT_LOCKED	The account management of the database was locked.
	ACCOUNT_MANAGEMENT_UNLOCKED	The account management of the database was unlocked.
	ARTIFACT_MANAGEMENT_LOCKED (from PLA 3.0.5)	Artifact management was locked, that is, component, package, and add-on management.
	ARTIFACT_MANAGEMENT_UNLOCKED (from PLA 3.0.5)	Artifact management was unlocked, that is, component, package, and add-on management.
	DB_POLICIES_LOCKED	The database policies were locked.
	DB_POLICIES_UNLOCKED	The database policies were unlocked.
	DB_PROPERTIES_LOCKED	The database properties were locked.
	DB_PROPERTIES_UNLOCKED	The database properties were unlocked.
	DB_KILL_LOCK (to PLA 3.0.4), OBJECT_LOCK_DELETED (from PLA 3.0.5)	An object was unlocked from the Session management dialog.
	DB_KILL_ALL_LOCKS (to PLA 3.0.4), OBJECT_LOCKS_DELETED (from PLA 3.0.5)	All objects were unlocked from the Session management dialog.
	SESSION_MANAGEMENT_LOCKED	Session management was locked.
	SESSION_MANAGEMENT_UNLOCKED	Session management was unlocked.
Database maintenance	DB_MAINTENANCE_START	A new database maintenance was started.
	DB_MAINTENANCE_COMPLETE	Database maintenance was completed.

	DB_MAINTENANCE_INCOMPLETE	Database maintenance remained incomplete because it was canceled by a user or because locked documents were skipped.
	DB_MAINTENANCE_CONTINUE	Incomplete database maintenance was resumed.
	DB_MAINTENANCE_REGISTRYUPDATED	Database maintenance caused the list of document properties to be reinitialized.
Object, data, document	DATA_ACQUIRED	Data were successfully acquired for a document.
	DATA_ACQUIRED_CANCELED	Data acquisition was canceled.
	DATA_ACQUIRED_FAILED	Data acquisition failed.
	DOC_KEY_CHANGED	A document key was changed.
	OBJECT_INITIAL	An object was created.
	OBJECT_IMPORTED	An object was imported.
	OBJECT_UPGRADE	The document type version of a document was upgraded.
	OBJECT_SAVED	Changes to an object were saved.
	OBJECT_MOVED	An object was moved.
	OBJECT_SIGN	A signature was applied to a document.
	OBJECT_REMOVESIGNATURE	A signature was removed from a document.
	OBJECT_COPIED_FROM	This object is a copy of another object.
	OBJECT_COPIED_TO	A copy of this object was created.
	OBJECT_EXECUTE_TASK	An action was executed on this object.
	OBJECT_EXPORTED	An object was exported.

	OBJECT_DELETE	An object was deleted.

2.3 Database maintenance

Perform database maintenance.

System menu > Database maintenance

Note: By default, only system administrators have the permissions required to perform database maintenance.

Note: Depending on the database, maintenance may take considerable time.

Section	Item	Description
Settings tab	Start new maintenance	Starts a new database maintenance. **Note:** This causes a DB_MAINTENANCE_STARTED entry to be written to the audit trail.
	Start new maintenance with reinitialization of the list of document properties	Starts a new database maintenance that also reinitializes the list of document properties. **Note:** This operation temporarily locks the database. **Tip:** Use this option if: • your Bioassay Package is older than Bioassay Package 24 and • you upgrade to Bioassay Package 24 or newer.
	Resume incomplete maintenance	Resumes the most recent database maintenance. **Tip:** This option only becomes available when maintenance has not been completed, which occurs when: • users cancel maintenance or • maintenance skips documents because they are locked.

Tasks tab	Table field	Displays progress when you perform database maintenance. • Task column: Lists all maintenance steps that have already been processed. • Message column: Indicates the status of each maintenance step that has been processed. **Note:** The Task column lists the Rebuilding digest task when structural changes occur in the document digest. This may require an update of existing documents.
	Message field	Displays result and supporting information. • Database maintenance complete: Confirms that all maintenance tasks have been completed successfully. • Database maintenance incomplete: Indicates that either a user cancelled maintenance or documents were skipped because they were locked. **Note:** This causes a DB_MAINTENANCE_INCOMPLETE entry to be written to the audit trail. **Tip:** When maintenance is incomplete, the Resume incomplete maintenance option becomes available in the Database maintenance dialog. • Database maintenance failed: Results from an internal error. Database maintenance was not executed.

	Log button	Generates and displays a PDF document that contains the information displayed on the Tasks tab and the following additional information on how the PDF document was generated: • Database: Name of the database • PLA version • S/N: Serial number of PLA license • User: User name • Workstation: Name of the computer • Timestamp: Date and time of PDF document generation

3 Extensibility with PLA 3.0

The PLA 3.0 Framework provides the features you need to achieve regulatory compliance. PLA 3.0 add-ons, such as the Biological Assays Package for the pharmaceutical industry or the Dose-Response Analysis Package, extend the functionality of PLA 3.0 to include the analytical methods your users require and enable them to visualize, document, and report results. They also support a range of additional tasks from data acquisition to data aggregation and process monitoring using control charts.

If some of your users need to work with a new analytical method, for example, or need to acquire data from a new instrument, you first install the add-ons required for the task. Once you have installed new add-ons to extend the functionality of PLA 3.0 or to update existing functionality, you activate these add-ons for the particular PLA databases whose users need the new functionality.

Note: The users of a PLA database can only work with the add-ons and add-on versions that are currently activated for this particular database. This approach guarantees that all users of the database work with the same add-ons and with the same add-on versions.

Tip: When users work with updated add-ons and try to access PLA documents created and edited with previous add-on versions, these documents open in read-only mode. Users can still edit such documents or use the analytical setups of such documents if they upgrade the structure of the documents. Since the Upgrade structure process is irreversible and discards all results and signatures contained in documents, the process provides the option "Ugrade copies of documents", which leaves the original documents untouched. Please consult the Document structure upgrade section of the Administration Guide for additional information.

The following two sections provide information on installing and using add-ons to extend and update the functionality of PLA 3.0:

- Add-on installation and activation
- Document structure upgrade

3.1 Add-on installation and activation

Install new PLA 3.0 add-ons to extend the functionality of PLA 3.0 or to update existing functionality. Activate add-ons to make the new functionality available to users of particular PLA databases.

The following steps are required to make the functionality of a new add-on available to users:

1. Run the add-on's setup program to install the add-on on the system.
2. Activate the add-on for the PLA databases whose users require the extended or updated functionality.

Tip: To install add-ons on the system, you require administrative rights.

Tip: To activate add-ons for PLA databases, you require a global role that allows you to perform the database task "Manage component packages" (System menu > Account management > Global roles > General tab).

The following dialog allows you to activate add-ons for PLA databases:

- Package management

3.1.1 Add-on management

Make the functionality of new PLA 3.0 add-ons available to the users of PLA databases.

System menu **>** Package management

The Package management dialog lists all available and activated add-ons, and it provides controls to activate and deactivate these add-ons. This feature is only accessible to users whose global role allows them to perform the database tasks "Manage component packages" and "See component packages" (System menu > Account management > Global roles > General tab).

Note: When you make updated add-ons available to users and they try to access PLA documents created with previous add-on versions, these documents open in read-only mode. Please consult the Document structure upgrade section of the Administration Guide for additional information.

Tip: Users whose global role includes the "See component packages" database task can open the Package management dialog and view the lists of available and activated add-ons, but they cannot execute the Activate and the Deactivate command in the dialog.

Package management dialog
The following table explains the features and controls available in the dialog.

Section	Item	Description
Header	Manage packages of database <database name>.	Displays the name of the current database. The controls of this dialog (Activate and Deactivate) apply to this particular database.
Available packages	Activate	Activates the package currently selected in the Available packages list, and makes the functionality of this package available for the current database.

	Available packages list	Lists the packages installed on the System: The Setup programs of PLA and of individual packages install packages in the following two locations: • Standard packages: C:\Program Files (x86)\Stegmann Systems\PLA 3.0\packages • Additional packages: C:\Program Files (x86)\Common Files \Stegmann Systems\PLA 3.0\packages
Activated packages	Deactivate	Deactivates the package currently selected in the Activated packages list, and makes the functionality of this package unavailable for the current database.
	Activated packages list	Lists the packages activated for the current database.

3.2 Document structure upgrade

Upgrade the structure of existing PLA documents, or upgrade the structure of copies of existing PLA documents.

File menu **>** Advanced **>** Upgrade structure, Upgrade structures in folder

When users work with updated add-ons and try to access PLA documents created and edited with previous add-on versions, these documents open in read-only mode. Users can still edit such documents or use the analytical setups of such documents if they upgrade either the structure of the documents themselves or the structure of copies of the documents.

Note: This feature is accessible if the security context of the current folder allows users to perform the document task "Edit documents" (System menu > Account management > Document roles > General tab).

Tip: Since the Upgrade structure process is irreversible and discards all results and signatures contained in documents, the process provides the option "Upgrade copies of documents", which leaves the original documents untouched.

When you make new add-on versions available and activate them for PLA databases that contain documents created and edited with previous add-on versions, the following options become available in the File menu and in the context menus of the Navigator.

- Upgrade structure: Becomes available if you select documents in the Navigator that were created and edited with previous add-on versions.
- Upgrade structures in folder: Becomes available if you select a folder in the Navigator, irrespective of whether this particular folder contains or does not contain documents created and edited with previous add-on versions.

Both menu options open the Upgrade document structures dialog. But the dialog has two variants, which differ with regard to the dialog's document selection section.

Tip: Users who open documents that do not contain any signatures except their own can access the upgrade document structure command directly by clicking the Upgrade structure button inside the document rather than opening the Upgrade document structures dialog.

Upgrade document structures dialog
The following table explains the features and controls available in the dialog.

Section	Item	Description
document selection: variant 1	entire section	The dialog displays this variant of the document selection section when users select one or several documents to be upgraded in the Navigator and use the "Upgrade structure" option to open the dialog.
	document list	Lists the documents currently selected in the Navigator. The commands of the dialog apply to these documents.
document selection: vaiant 2	entire section	The dialog displays this variant of the document selection section when users select a folder in the Navigator and use the "Upgrade structures in folder" option to open the dialog.
	document mode list	Specifies the document "modes" whose structures are to be upgraded. The commands of the dialog only apply to documents that belong to the "modes" you select here. The following options are available: • Documents • Templates • PQ definitions
	Source folder: <folder name (key)>	Displays both the Name and the unique Key of the currently selected folder. The commands of the dialog only apply to documents contained in this folder and its subfolders.
	select folder button	Sets the Source folder. Use this control if the folder currently set as Source folder does not contain the documents whose structure you want to upgrade. The button opens a dialog that allows you to navigate to and select the correct folder.

upgrade method	Upgrade copies of documents	With this option selected, the Upgrade structure process does the following: • Creates copies of the documents whose structure is to be upgraded. • Deletes all results and signatures in these copies. • Upgrades the document structure of these copies. • Leaves the original documents untouched, and therefore preserves the results and signatures in the original documents. **Tip:** Select this option if you want to preserve the original documents.
	Upgrade document structures directly	With this option selected, the Upgrade structure process does the following: • Deletes all results and signatures in the documents whose structure is to be upgraded. • Upgrades the document structure of these documents. **Warning:** The Upgrade structure process is irreversible and discards all results and signatures. Select this option if you no longer need the results and signatures contained in the original documents. **Tip:** Select this option and disable the "Upgrade signed documents" option below if you want to preserve all signed documents including the results and signatures contained in these documents, but no longer need the results contained in unsigned documents.
	Upgrade signed documents	Specifies whether the structure of signed documents is to be upgraded. This option requires user authentication since it discards all results and signatures. **Note:** With this option enabled, you have to enter your password below to complete the dialog.
user authentication	User: <login name>	Displays the Login name of the current user.

	Password text box	Requires the password of the current user. **Note:** The Password text box is only enabled and user authentication required when you select the "Upgrade signed documents" option above.

4 Rights and permissions in PLA 3.0

PLA 3.0 provides the features you need to control access to your data in a sophisticated and compliant manner. It combines role-based user rights with resource-based permissions, which enable you to exercise very fine-grained control over who is allowed to perform particular tasks in a given context and which tasks are allowed with particular data.

The Account management features of PLA 3.0 combine a role-based approach with Security contexts. For this purpose, PLA 3.0 distinguishes between two types of roles, Global and Document roles. You set up Global roles for database tasks such as setting up database policies or managing user sessions. The Global roles you assign to users and groups are valid for the entire database. You set up Document roles for document tasks such as editing documents or applying electronic signatures. Assignments of Document roles to users and groups define Security contexts. You can then apply these Security contexts to folders or folder trees. Every user and group can be part of more than one Security context. So, the Document roles of a particular user or group can vary from folder to folder or from folder tree to folder tree.

Note: The Account management features of PLA 3.0 allow you to set up users and groups directly in PLA. But you can also use directory services based on secure LDAP (LDAPS: Lightweight Directory Access Protocol over SSL/ TLS) to map PLA groups and their roles to user groups defined elsewhere on your network.

In addition to the features provided by Account management, Folder properties allow you to restrict the content of particular folders to documents generated from particular document templates. And each document template allows you to define permissions that apply to entire documents generated from it or just to specific sections whithin generated documents. The granularity of permissions you define in document templates even reaches down to the level of individual data elements such as—in biological assays, for example—the preparation scheme associated with a test sample or the number of replicates defined in a preparation scheme.

The following three sections provide information on administering rights and permissions in PLA 3.0:

- Users, groups, and Global roles
  - Global roles: Combine database tasks into Global roles to be assigned to users and groups.
  - User groups in PLA 3.0: Create PLA user groups and give them Global roles.
  - Directory service configuration: Use secure LDAP (LDAPS) directory services, such as Active Directory Domain Services, to map your PLA 3.0 groups to user groups defined elsewhere on your network.
  - Users in PLA 3.0: Define users directly in PLA.
- Security contexts and Document roles
  - Document roles: Combine document tasks into Document roles to be used for Security contexts.
  - Security contexts: Assign Document roles to PLA 3.0 users and groups to define Security contexts.

- Permissions of folders, documents, and data elements
  - Change security context: Control what actions particular users and groups can perform in particular folders and folder trees.
  - Folder properties: Control what content users can create and store in particular folders and folder trees.
  - Document templates: Control what actions users can perform on particular documents, document sections, and individual data elements within documents.

4.1 Users, groups, and Global roles

Set up users, groups, and Global roles. Assign Global roles to users and groups to control who can perform particular database tasks such as setting up database policies or managing user sessions.

The following four dialogs allow you to set up Global roles and assign them to users and groups:

- Global roles: Combine database tasks into Global roles to be assigned to users and groups.
- User groups in PLA 3.0: Create PLA user groups and give them Global roles.
- Directory service configuration: Use secure LDAP (LDAPS) directory services, such as Active Directory Domain Services, to map your PLA 3.0 groups to user groups defined elsewhere on your network.
- Users in PLA 3.0: Define users directly in PLA.

4.1.1 Global roles

Set up Global roles and assign them to users and groups to control who can perform particular database tasks.

System menu **>** Account management **>** Global roles

Select the Global roles entry in the Account management dialog to display the Roles tab where you create, modify, and delete global roles for the database. Expand the Global roles node and select one of the global roles listed to display the General tab, which allows you to assign and unassign Task permissions to this particular global role.

Tip: When you create a new database in PLA, predefined global roles are included and accessible from the Account management dialog. In the default setup, one of these global roles —the System administrator global role—is needed for the Administrator account. It is assigned to the Administrator through membership in the System administrators group and has the required Manage accounts task permission. All other global roles are intended as examples to help you set up the global roles you require.

Global roles dialog
The following table explains the features and controls available in the Global roles dialog.

Section	Item	Description

Roles tab	Add button	Opens the Add global role dialog, which allows you to create a new global role in the database. The dialog provides the following two text boxes: • Name: Enter a name for the new global role. **Note:** The names of Global roles and Document roles have to be unique within the database. • Description: Provide a brief description of the new global role.
	Edit button	Opens the General tab for the global role currently selected in the role table, which allows you to modify this global role. Please consult the General tab section below for additional information.
	Remove button	Opens a dialog that allows you to delete the currently selected global role from the database.
	Filter text box	Modifies the role table displayed to only include the global roles whose name contains the character sequence you enter in the text box.
	Name column	Lists the names of all global roles set up in the database or, if you set a filter, of the global roles that match the filter.
	Description column	Provides brief descriptions of the global roles listed in the Name column. **Tip:** To change the description of a global role, select it in the table and click Edit, which displays the General tab for this global role.
General tab, Details section	Name	Displays the name of the currently selected global role.
	Description text box	Allows you to edit the description of the currently selected global role.

	Translate button	Opens a dialog that allows you to provide translations of the description. **Tip:** If you provide translations in the preferred languages of your users, PLA displays the description in the language preferred by the current user according to the language settings of the operating systems. The dialog provides the following controls: • Add button: Opens the Add language dialog, which allows you to select a language or locale identifier from a drop-down list and add it to the language table. • Remove button: Opens a dialog that allows you to delete the currently selected language from the language table. • Usage column: Displays the default language and additional languages you have added to the table. Expand the node of a language to display items you can translate. • Value column: Displays the translations. Click a translation to edit the text.
General tab, Task permissions table	Add button	Opens the Add task permission dialog, which allows you to select a single task from a list and assign it to the currently selected global role. Please consult the Global tasks table below for additional information on particular tasks.
	Remove button	Unassigns the currently selected task from the global role.
	Task column	Lists the names of all tasks assigned to the global role.
	Description column	Provides brief descriptions of the tasks listed in the Task column.

Database tasks

The following table explains the tasks available for global roles.

Item	Description
Database maintenance	Run Database maintenance (System menu).
Edit database policies	Modify settings in the Database policies dialog (System menu).
Execute IQ	Execute the Installation qualification (IQ) command (Validation menu).

Execute OQ	Execute the Operational qualification (OQ) command (Validation menu). **Note:** This requires an active PLA 3.0 Validation Package license.
Execute PQ	Execute the Performance qualification (PQ) command (Validation menu). **Note:** This requires an active PLA 3.0 Validation Package license.
Lock database	Execute the Lock database command (System menu) to lock other users out and have exclusive access to the database.
Manage accounts	Modify settings in the Account management dialogs (System menu): Global roles, Document roles, Groups, Security contexts, and Users. **Note:** This task setting does not affect accessibility of tasks related to the Change security context feature (File menu > Advanced). **Note:** To maintain the database, at least one user needs to have the Manage accounts task. In the default setup of PLA databases, the Administrator has this task due to membership in the System administrators group, which has the System administrator global role assigned.
Manage add-ons (PLA 3.0.5)/ Manage component packages (PLA 3.0.4)	Execute commands in the Add-ons dialog (PLA 3.0.5)/ Package management dialog (PLA 3.0.4) (System menu). **Note:** To execute commands in the Package management dialog (PLA 3.0.4), users also need the See component packages task, which enables them to open the Package management dialog.
Manage database info (PLA 3.0.5)/ Manage database properties (PLA 3.0.4)	Modify settings in the Database info dialog (PLA 3.0.5)/ Database properties dialog (PLA 3.0.4) (System menu).
Manage own account	Edit Details associated with one's own user account such as the e-mail address or phone number (System menu > Account management > Users). **Tip:** This task setting only affects user accounts set up in PLA rather than an external directory.
Manage sessions	View Session management (System menu), and execute commands in the dialog.

See component packages (PLA 3.0.4)	View the Package management dialog (PLA 3.0.4) (System menu). **Tip:** To execute commands in this dialog, users also need the Manage component packages task.
Show audit trail	View the system audit trail (System menu > Audit trail). **Note:** This task setting only affects the system audit trail. The document audit trails are accessible to all users who can view related documents.

4.1.2 User groups in PLA 3.0

Set up PLA 3.0 groups to assign them Global roles and combine them with Document roles into Security contexts. PLA 3.0 allows you to use secure LDAP (LDAPS) directory services to map your PLA groups to user groups defined elsewhere on your network.

System menu **>** Account management **>** Groups

Select the Groups entry in the Account management dialog to display the Groups tab, where you create, modify, and delete groups. Expand the Groups node and select one of the groups listed to display the General tab and the Roles tab where you can modify the settings of this group and assign it global roles.

Tip: When you create a new database in PLA, predefined groups are included and accessible from the Account management dialog. In the default setup, one of these groups—the System administrators group—is needed for the Administrator account. It has the System administrator global role assigned, which includes the required Manage accounts task permission. All other groups are intended as examples to help you set up the groups you require.

Groups dialog
The following table explains the features and controls available in the Groups dialog.

Section	Item	Description
Groups tab	Add button	Opens the Add group dialog, which allows you to create a new group in the database. The dialog provides the following two text boxes: • Name: Enter a name for the new group. **Note:** Group and user names have to be unique within the database. • Description: Provide a brief description of the new group.

	Edit button	Opens the General tab for the group currently selected in the group table, which allows you to modify this group. Please consult the General tab section below for additional information.
	Remove button	Opens a dialog that allows you to delete the currently selected group from the database.
	Filter text box	Modifies the group table displayed to only include the groups whose name or description contains the character sequence you enter in the text box.
	Avatar column	Displays the avatars of the groups listed in the Group column. **Tip:** To change the avatar of a group, select it in the table and click Edit, which displays the General tab for this group.
	Group column	Lists the names of all groups set up in the database or, if you set a filter, of the groups that match the filter.
	Description column	Provides brief descriptions of the groups listed in the Group column. **Tip:** To change the description of a group, select it in the table and click Edit, which displays the General tab for this group.
General tab, Details section	Change button	Opens a dialog that allows you to select a JPEG or PNG image to be used as the avatar of the currently selected group.
	Name	Displays the name of the currently selected group.
	Description text box	Allows you to edit the description of the currently selected group.
	Expiry date	Sets an expiration date for the currently selected group.
	Group is disabled	Disables the currently selected group.

	Translate button	Opens a dialog that allows you to provide translations of the description. **Tip:** If you provide translations in the preferred languages of your users, PLA displays the description in the language preferred by the current user according to the language settings of the operating systems. The dialog provides the following controls: • Add button: Opens the Add language dialog, which allows you to select a language or locale identifier from a drop-down list and add it to the language table. • Remove button: Opens a dialog that allows you to delete the currently selected language from the language table. • Usage column: Displays the default language and additional languages you have added to the table. Expand the node of a language to display items you can translate. • Value column: Displays the translations. Click a translation to edit the text.
General tab, Members section	Add button	Opens the Add members dialog, which allows you to select one or several PLA users from a list and assign them to the currently selected group.
	Remove button	Unassigns the currently selected user from the group.
	Filter text box	Modifies the Members table displayed to only include the groups whose description contains the character sequence you enter in the text box.
	Avatar column	Displays the avatars of the users listed in the Name column.
	Name column	Lists the Login and Display names of all PLA users who are members of the group or, if you set a filter, of the members who match the filter.
	Description column	Provides brief descriptions of the members listed in the Name column.
Roles tab	Add button	Opens the Add global roles dialog, which allows you to select one or several global roles from a list and assign them to the currently selected group.
	Remove button	Unassigns the currently selected global role from the group.

	Role column	Lists the names of all global roles assigned to the group.
	Description column	Provides brief descriptions of the global roles listed in the Role column.

4.1.3 Directory service configuration

Use secure LDAP (LDAPS) directory services, such as Microsoft Active Directory Domain Services, to authenticate PLA users. You map your PLA groups, which have PLA roles assigned, to user groups set up on a directory server. You cannot directly assign directory users to PLA groups.

System menu **>** Directory service

Note: When you use directory services to authenticate users, PLA has read-only access to the directory server to read information on users and their assignments to groups. If users need to change their password, for example, this has to be done by other means.

The Directory service configuration wizard—a series of five dialogs—allows you to set up the connection to the directory server and map PLA groups to directory groups.

Dialog 1: Access directory server
This step of the Directory service configuration wizard allows you to enter the settings required to establish a connection to the directory server.

Section	Item	Description
General	Use directory service	Enables directory services. **Tip:** When you disable directory services, PLA still keeps the settings you make in this dialog.
Directory server	Host	Enter the name or IPv4 address of the directory server host. **Note:** PLA only supports encrypted connections (SSL) to directory servers. Please make sure the server uses appropriate encryption.
	Port	Enter the number of the port to be used.

	Directory type	Select the directory type from the drop-down list. The following options are available. • Active Directory • Generic **Tip:** Use the Active Directory option if you use Microsoft Active Directory or Active Directory Domain Services. In all other cases, use the Generic option.
Search account	User ID (Bind DN)	Enter the ID of the user to be employed for the search account. **Note:** PLA needs the Search account to access information required for user authentication. We recommend to employ a user account specifically designated for this purpose.
	Password	Enter the password of the Search account. **Tip:** For the Search account, we recommend to employ a user account whose password does not expire.

Example of valid entries for Dialog 1: Access directory server
The following table provides an example of valid entries.

Section	Item	Example of valid setting
Directory server	Host	192.168.1.210
	Port	636
	Directory type	Generic
Search account	User ID (Bind DN)	cn=ldapsearch,dc=openldap,dc=int

Dialog 2: Review and accept the SSL certificate
PLA only supports encrypted connections (SSL) to directory servers. This step of the Directory service configuration wizard allows you to review and accept the required SSL certificate.

Section	Item	Description
Certificate issued to	text displayed	Lists information on the entity to which the certificate has been issued.

status message	The certificate is trusted.	Displays the following command options. • Show certificate • Remove certificate
	The certificate will not be trusted.	Displays the following command options. • Technical details • Show certificate • Trust certificate
command buttons	Show certificate	Opens a dialog that displays information on the certificate. Please consult the Certificate viewer section below for additional information.
	Remove certificate	Deletes the certificate information, which the directory server provided, from the database.
	Technical details	Displays a pop-up window that provides detailed information on why the certificate is not trusted.
	Trust certificate	Allows you to affirm that you trust the certificate.
Certificate viewer	General tab	Provides the following information on the certificate. • Issued to • Issued by • Validity: Provides both the issue and expiration date of the certificate. • Fingerprints
	Details tab	Provides the following information on the certificate. • Certificate hierarchy • Certificate details • Field raw values

Dialog 3: Configure directory classes and attributes
Directory services require configuration of various directory classes and attributes. This step of the Directory service configuration wizard lists settings for review and allows you to confirm that they match the settings of your directory server.

Note: PLA only displays this dialog if you select the Generic directory type in Dialog 1. The Directory service configuration wizard for Active Directory skips this page.

Section	Item	Description
Class/ attribute table	Class/ attribute type column	Lists both class and attribute types.
	Class/ attribute value column	Displays the values of the class and attribute types listed.
	Reset to default values button	Resets all values displayed to their default.

Example of valid entries for Dialog 3: Configure directory classes and attributes
The following table provides an example of valid entries.

Section	Example types	Example values
Class type	Group class	groupOfNames
	User class	inetOrgPerson
Attribute type	Group membership attribute	member
	User icon attribute	jpegPhoto
	User ID attribute	uid
	User name attribute	sn
	User display name attribute	displayName
	User department attribute	departmentNumber

Dialog 4: Select the search base
This step of the Directory service configuration wizard allows you to select the directory subtree to be searched to authenticate PLA users.

Section	Item	Description
Settings	Search base:	ellipsis button: Opens a dialog that allows you to navigate to and select the directory tree or subtree that contains the configuration and is to be searched for users. **Note:** Please make sure the directory tree or subtree you select contains both the Groups and Users.

Dialog 5: Map PLA groups to your directory groups
This step of the Directory service configuration wizard allows you to map your PLA groups to user groups set up on the directory server.

Section	Item	Description
Group table	PLA group column	Lists the names of all PLA groups set up in this database. **Tip:** You do not have to map all PLA groups listed.
	Directory group column	Displays the names of the directory groups to which the PLA groups are mapped.
Command buttons	Assign	Opens a dialog that allows you to navigate to and select the directory group to which you want to map the PLA group currently selected in the group table.
	Unassign	Deletes the mapping currently selected in the group table.

Example of valid entries for Dialog 5: Map PLA groups to your directory groups
The following table provides an example of valid entries.

Example PLA groups	Example directory groups
Functional administrators	Group3
Inspectors	<not assigned>
Power users	Group2
System administrators	Group1
Users	<not assigned>

4.1.4 Users in PLA 3.0

If you do not have access to LDAP directory services on your network, you can set up user accounts directly in PLA 3.0.

System menu **>** Account management **>** Users

Select the Users entry in the Account management dialog to display the Users tab, where you create, modify, and delete users. Expand the Users node and select one of the users listed to display the General tab and the Roles and groups tab where you can modify the settings of this user, assign her global roles, and assign her to user groups.

Tip: When you create a new database in PLA, one predefined user—named "Administrator"—is included and accessible from the Account management dialog. In the

default setup, this user is needed to maintain the database. Due to its membership in the System administrators group, it has the System administrator global role assigned, which includes the required Manage accounts task permission.

Users dialog

The following table explains the features and controls available in the Users dialog.

Section	Item	Description
Users tab	Add button	Opens the Add a new user dialog, which allows you to create a new user in the database. The dialog provides the following four controls: • Login name: Enter a login name for the new user. **Note:** Group and user names have to be unique within the database. • New password, Confirm password: Enter a password for the new user. **Tip:** Please consult the Database policies section of the Administration Guide for additional information on passwords. • Password has to be changed at next login: Locks the user account for the current password. When the user tries to log in, a pop-up window prompts the user to change her password.
	Edit button	Opens the General tab for the user currently selected in the user table, which allows you to modify this user. Please consult the General tab section below for additional information.
	Remove button	Opens a dialog that allows you to delete the currently selected user from the database.
	Filter text box	Modifies the user table displayed to only include the users whose name or description contains the character sequence you enter in the text box.
	Avatar column	Displays the avatars of the users listed in the Name column. **Tip:** To change the avatar of a user, select it in the table and click Edit, which displays the General tab for this user.
	Name column	Lists the login names of all users set up in the database or, if you set a filter, of the users that match the filter.

	Description column	Provides brief descriptions of the users listed in the Name column. **Tip:** To change the description of a user, select it in the table and click Edit, which displays the General tab for this user.
General tab	Change button	Opens a dialog that allows you to select a JPEG or PNG image to be used as the avatar of the currently selected group.
	Login name	Displays the login name of the currently selected user.
	First name, Last name, Description, Department, Telephone number (text boxes)	Allow you to edit information on the currently selected user.
	Display name text box	Allows you to edit the display name of the currently selected user. In most contexts, PLA substitutes the display name for the login name. The default value of the display name is the login name of the user. **Note:** The display name does not have to be unique. The audit trail provides the login names rather than the display names of users to guarantee traceability of changes to a particular user account.
	E-mail text box	Allows you to edit the e-mail address of the currently selected user.
	Expiry date	Sets an expiration date for the currently selected user.
	Unlock now	Unlocks the currently selected user account. This button is only enabled if the user has been locked due to login failures. **Tip:** Please consult the Database policies section of the Administration Guide for additional information on passwords.
	Password has to be changed at next login	Locks the user account for the current password. When the user tries to log in, a pop-up window prompts the user to change her password. **Tip:** Do not use this feature to enforce new password policies. At every login, PLA automatically checks whether passwords are consistent with password policies.

Account is disabled	Disables the currently selected user account. When you disable an account, the user can no longer log into the database. And the user name is no longer listed in the Select user dialog of the login screen.
Set password	Opens a dialog that allows you to change the password of the currently selected user. **Tip:** Please consult the Database policies section of the Administration Guide for additional information on passwords.
Reset password	Opens a dialog that allows you to reset the password of the currently selected user. If you confirm the dialog, PLA opens your default e-mail application and creates an e-mail to the user that contains a new, randomly generated password. You have to send the e-mail manually. When the user tries to log in, a pop-up window prompts the user to change her password. This button is only enabled if you or the user has entered an e-mail address on this tab.
Translate button	Opens a dialog that allows you to provide translations of the description. **Tip:** If you provide translations in the preferred languages of your users, PLA displays the description in the language preferred by the current user according to the language settings of the operating systems. The dialog provides the following controls: • Add button: Opens the Add language dialog, which allows you to select a language or locale identifier from a drop-down list and add it to the language table. • Remove button: Opens a dialog that allows you to delete the currently selected language from the language table. • Usage column: Displays the default language and additional languages you have added to the table. Expand the node of a language to display items you can translate. • Value column: Displays the translations. Click a translation to edit the text.

Roles and groups tab, Global roles section	Add button	Opens the Add global roles dialog, which allows you to select one or several global roles from a list and assign them to the currently selected user.
	Remove button	Unassigns the currently selected global role from the user.
	Role column	Lists the names of all global roles assigned to the user.
	Description column	Provides brief descriptions of the global roles listed in the Role column.
Roles and groups tab, Groups section	Add button	Opens the Add groups dialog, which allows you to select one or several groups from a list and assign the user to these groups.
	Remove button	Unassigns the user from the currently selected group.
	Group column	Lists the names of all groups to which the user is currently assigned.
	Description column	Provides brief descriptions of the groups listed in the Group column.

4.2 Security contexts and Document roles

Set up Document roles and assign them to users and groups to define Security contexts. You then apply these Security contexts to folders to control who can perform particular document tasks, such as editing documents or applying electronic signatures, in these folders or folder trees.

The following two dialogs allow you to set up Document roles and define Security contexts:

- Document roles: Combine document tasks into Document roles to be used for Security contexts.
- Security contexts: Assign Document roles to PLA 3.0 users and groups to define Security contexts.

See also:

- Change security context: Control what actions particular users and groups can perform in particular folders and folder trees.

4.2.1 Document roles

Set up Document roles as a preliminary step in defining the security contexts you need for the database. They allow you to control who can perform which tasks on documents stored in particular folders or folder trees.

System menu **>** Account management **>** Document roles

Select the Document roles entry in the Account management dialog to display the Roles tab where you create, modify, and delete document roles for the database. Expand the Document roles node and select one of the document roles listed to display the General tab, which allows you to assign and unassign Task permissions to this particular document role.

Tip: PLA even allows you to customize the individual document Task permissions you assign to document roles. You can impose restrictions that limit the scope of individual document tasks to particular document types, document modes, and document signature statuses.

Tip: When you create a new database in PLA, predefined document roles are included and accessible from the Account management dialog. They are intended as examples to help you set up the document roles you require.

Document roles dialog

The following table explains the features and controls available in the Document roles dialog.

Section	Item	Description
Roles tab	Add button	Opens the Add document role dialog, which allows you to create a new document role in the database. The dialog provides the following two text boxes: • Name: Enter a name for the new document role. **Note:** The names of Global roles and Document roles have to be unique within the database. • Description: Provide a brief description of the new document role.
	Edit button	Opens the General tab for the document role currently selected in the role table, which allows you to modify this document role. Please consult the General tab section below for additional information.
	Remove button	Opens a dialog that allows you to delete the currently selected document role from the database.
	Filter text box	Modifies the role table displayed to only include the document roles whose name contains the character sequence you enter in the text box.
	Name column	Lists the names of all document roles set up in the database or, if you set a filter, of the document roles that match the filter.

	Description column	Provides brief descriptions of the document roles listed in the Name column. **Tip:** To change the description of a document role, select it in the table and click Edit, which displays the General tab for this document role.
General tab, Details section	Name	Displays the name of the currently selected document role.
	Description text box	Allows you to edit the description of the currently selected document role.
	Translate button	Opens a dialog that allows you to provide translations of the description. **Tip:** If you provide translations in the preferred languages of your users, PLA displays the description in the language preferred by the current user according to the language settings of the operating systems. The dialog provides the following controls: • Add button: Opens the Add language dialog, which allows you to select a language or locale identifier from a drop-down list and add it to the language table. • Remove button: Opens a dialog that allows you to delete the currently selected language from the language table. • Usage column: Displays the default language and additional languages you have added to the table. Expand the node of a language to display items you can translate. • Value column: Displays the translations. Click a translation to edit the text.
General tab, Task permissions table	Add button	Opens the Add task permission dialog, which allows you to select a single task from a list and assign it to the currently selected document role. Please consult the Document tasks table below for additional information on particular tasks.
	Remove button	Unassigns the currently selected task from the document role.
	Edit button	Opens the Restrict task permission dialog for the task currently selected in the Task permissions table. Please consult the Restrict task permission dialog entry below for additional information.
	Task column	Lists the names of all tasks assigned to the currently selected document role.

Description column	Provides brief descriptions of the tasks listed in the Task column.
Restrictions column	Advises of current restrictions imposed on individual task permissions. The column indicates the areas where restrictions apply: • Permitted document types • Permitted document modes • Permitted document signature states Please consult the Restrict task permission dialog entry below for additional information.
Restrict task permission dialog	This dialog allows you to impose restrictions that limit the scope of the currently selected document task permission. Select a task permission in the Task permissions table and click Edit to open the dialog for this task permission. **Tip:** When you change the settings of a task permission, your changes only apply to the currently selected document role rather than all document roles that have the task. The dialog has the following sections: • Task: Displays the name of the task to which the settings of the dialog apply. • Description: Displays the description of the task. • Permitted document types: Lists all document types activated for the database. Clear the checkboxes of the document types you want to exclude from this task permission. By default, all document types are included. • Permitted document modes: Lists all document modes available in PLA. Clear the checkboxes of the document modes you want to exclude from this task permission. By default, all document modes are included. • Permitted document signature states: Lists all document signature states available in PLA. Clear the checkboxes of the document signature states you want to exclude from this task permission. By default, all document signature states are included.

Document tasks

The following table explains the tasks available for document roles.

Item	Description

Create new documents	• Create new documents, templates, and folders in the database. • Import documents into the database. • Generate documents from templates available in the database. • Create new PQ definitions. • Execute OQ and PQ.
Read documents	• View the name and other properties of documents and folders that are available for display in the Navigator. • Open and view documents in the editor (read-only mode).
Edit documents	Open and modify documents in the editor.
Remove documents	Delete documents and folders from the database.
Move documents	Move documents to other locations within the database. **Note:** This task also requires permission to Create new documents in the target folder.
Copy documents	Copy documents and folders to other locations within the database. **Note:** This task also requires permission to Create new documents in the target folder.
Export documents	Export documents from the database. **Tip:** Exported PLA document packages have the ".edpdp" file extension.
Change document and folder key	Change the identification key of documents and folders. **Note:** The option "Deny change document or folder key" in the Database policies (System menu > Database policies > Advanced) overrides this permission for the entire database. **Tip:** The extent to which users are free to decide on the form of new keys depends on the Document key format settings in the Folder properties (File menu > Properties > Document key format).

Read folder properties	Open the Folder properties dialog on a folder to view its settings (File menu > Properties).
Edit folder properties	Open the Folder properties dialog on a folder to modify its settings (File menu > Properties).
Edit documents with elevated permissions (PLA 3.0.5)/ Edit field protections (PLA 3.0.4)	Open documents generated from a template in the mode required to edit the values and field protections set by the template (File menu > Open with elevated permissions).
Change security context	Open the Change security context dialog on a folder to select a different security context for this folder (File menu > Advanced > Change security context).
Confirm electronic signatures	Open the Signatures dialog to apply one or more electronic signatures to documents that have been signed already. **Note:** This task also requires permission to open the documents to be signed.
Apply electronic signatures	Open the Signatures dialog to apply one or more electronic signatures to documents irrespective of whether they have been signed already. **Note:** This task also requires permission to open the documents to be signed.
Remove own electronic signatures	Open the Signatures dialog to delete signatures that have been applied by the current user. **Note:** This task also requires permission to open the documents whose signatures are to be deleted. **Note:** The option "Deny signature removal" in the Database policies (System menu > Database policies > Signatures) overrides this permission for the entire database.

Remove all electronic signatures	Open the Signatures dialog to delete signatures that have been applied by the current or other users. **Note:** This task also requires permission to open the documents whose signatures are to be deleted. **Note:** The option "Deny signature removal" in the Database policies (System menu > Database policies > Signatures) overrides this permission for the entire database.

4.2.2 Security contexts

Define the Security contexts you need for the database. They allow you to control who can perform which tasks on documents stored in particular folders or folder trees.

To define security contexts, you simply assign Document roles to Subjects (users or groups). Security contexts consist of one or more such role-to-subject assignments.
System menu **>** Account management **>** Security contexts

Select the Security contexts entry in the Account management dialog to display the Security contexts tab where you create, modify, and delete security contexts for the database. Expand the Security contexts node and select one of the security contexts listed to display the General tab and the Folder tab where you can modify the settings of this security context, create and add new role-to-subject assignments, and view a list of all folders that belong to this security context.

Note: Every folder in the database has to be assigned to a security context. Folders inherit the security context of their parent folder unless you explicitly assign them to a different security context.

Tip: When you create a new database in PLA, one predefined security context—named "Root Security Context"—is included and accessible from the Account management dialog. In the default setup, this security context is needed because the Root folder is assigned to it and all other folders are assigned to it by inheritance.

Security contexts dialog
The following table explains the features and controls available in the Security contexts dialog.

Section	Item	Description

Security contexts tab	Add button	Opens the Add security context dialog, which allows you to create a new security context in the database. The dialog provides the following two text boxes: • Name: Enter a name for the new security context. **Note:** The names of Security contexts have to be unique within the database. • Description: Provide a brief description of the new security context.
	Edit button	Opens the General tab for the security context currently selected in the security context table, which allows you to modify this security context. Please consult the General tab section below for additional information.
	Remove button	Opens a dialog that allows you to delete the currently selected security context from the database.
	Filter text box	Modifies the security context table displayed to only include the security contexts whose name or description contains the character sequence you enter in the text box.
	Name column	Lists the names of all security contexts set up in the database or, if you set a filter, of the security contexts that match the filter.
	Description column	Provides brief descriptions of the security contexts listed in the Name column. **Tip:** To change the description of a security context, select it in the table and click Edit, which displays the General tab for this security context.
General tab, Details section	Name	Displays the name of the currently selected security context.
	Description text box	Allows you to edit the description of the currently selected security context.

	Translate button	Opens a dialog that allows you to provide translations of the description. **Tip:** If you provide translations in the preferred languages of your users, PLA displays the description in the language preferred by the current user according to the language settings of the operating systems. The dialog provides the following controls: • Add button: Opens the Add language dialog, which allows you to select a language or locale identifier from a drop-down list and add it to the language table. • Remove button: Opens a dialog that allows you to delete the currently selected language from the language table. • Usage column: Displays the default language and additional languages you have added to the table. Expand the node of a language to display items you can translate. • Value column: Displays the translations. Click a translation to edit the text.
General tab, Assigned roles table	Add button	Opens the Add role (security contexts) dialog, which allows you to select a single Subject (user or group) and a single Document role from a list. This defines a new role-to-subject assignment, which you can add to the current security context.
	Remove button	Deletes the currently selected role-to-subject assignment.
	Avatar column	Displays the avatars of the subjects (users and groups) listed in the Subject column.
	Subject column	Lists the users (login and display name) and groups (group name) who have document roles assigned in the current security context. **Tip:** Each role-to-subject assignment is listed in a separate table row. Subjects who have more than one role assigned are listed more than once in the table.
	Role column	Provides the names of the Document roles assigned to the users and groups listed in the Subject column.

Folders tab	Assigned folders/ Path list	Displays the database paths of all folders assigned to the current security context. **Tip:** Use the Change security context dialog to assign additional folders to the security context and to remove folders from it (File menu > Advanced > Security context (PLA 3.0.5)/ Change security context (PLA 3.0.4)).

4.3 Permissions of folders, documents, and data elements

Set up permissions to control access to folders, documents, and individual data elements.

The following three dialogs allow you to apply fine-grained permissions to folders, documents, sections within documents, and even individual data elements within documents:

- Change security context: Control what actions particular users and groups can perform in particular folders and folder trees.
- Folder properties: Control what content users can create and store in particular folders and folder trees.
- Document templates: Control what actions users can perform on particular documents, document sections, and individual data elements within documents.

4.3.1 Change security context

Assign folders to security contexts to control what actions particular users and groups can perform on documents stored in these folders and their subfolders.

File menu **>** Advanced **>** Security context (from PLA 3.0.5)/ Change security context (to PLA 3.0.4)

Select a folder in the PLA Navigator and open the Change security context dialog to assign a security context to this folder and its subfolders.

Note: Every folder in the database has to be assigned to a security context. Folders inherit the security context of their parent folder unless you explicitly assign them to a different security context. By default, all folders in PLA databases are assigned to the Root security context since they inherit the Root folder's default assignment to this context.

Change security context dialog

Note: To assign a folder to a different security context, PLA also has to lock all folders that inherit this change and the documents they contain. Please make sure that none of these folders and documents are locked by other users.

The following table explains the features and controls available in the Change security context dialog.

Section	Item	Description

dialog header	text displayed	Displays the unique identification Key of the folder to which the settings in the dialog apply.
Security context	Current	Displays the name of the old security context to which the folder is currently assigned.
	New drop-down list	Allows you to select the new security context to which you want to assign the folder and its subfolders. **Note:** Subtrees that are explicitly assigned to a different security context do not inherit the new assignment.

4.3.2 Folder properties

Set folder properties to restrict the content of particular folders to particular document types and to documents generated from particular document templates. Set the names of folders. Customize the identification key formats of folders and of the documents and templates they contain.

File menu **>** Properties

Select a folder in the PLA Navigator to open its Folder properties dialog.

This feature is only accessible if the security context of the folder allows users to perform the document task "Edit folder properties" (System menu > Account management > Document roles > General tab).

Note: Folders inherit the properties of their parent folder by default. If you change the properties of a folder, the changes apply to all subfolders. Changes do not apply to existing documents in the folder and its subfolders.

Tip: Please consult the User Guide and video tutorials available on our website for additional practical advice on how to use this feature.

Folder properties dialog
The following table explains the features and controls available in the Folder properties dialog.

Section	Item	Description
General tab, General	Document key	Displays the unique identification Key of the folder to which the settings in the dialog apply.
	Name text box	Allows you to edit the name of the folder.

General tab, Security	Security context	Displays the name of the security context to which the folder is currently assigned. **Tip:** Use the Change security context dialog to assign the folder to a different security context (File menu > Advanced > Change security context).
Document key format tab (bottom of tab)	Enable custom document keys	Permits changes to the counters that are part of document, template, and folder keys. Makes the Change document key dialog accessible to users (File menu > Advanced > Change document key). **Note:** This feature is only accessible if the option "Deny change document or folder key" in the Database policies is disabled (System menu > Database policies > Advanced tab). **Note:** This feature is only accessible if the security context of the folder allows users to perform the document task "Change document and folder key" (System menu > Account management > Document roles > General tab).
	Change configuration/ Reset configuration toggle	Activates all other controls on this tab, or resets all key formats defined on this tab to their default. **Tip:** See the two notes above.
Document key format tab, Default keys	text displayed	Displays the formats used to generate unique identification keys for new documents, templates, and folders added to the database.
	Change buttons	These three command buttons open the Document, Template, and Folder key format dialogs where you can modify the formats used to generate unique idenfitication keys for new documents, templates, and folders. **Note:** This feature is only accessible if the option "Deny change document or folder key" in the Database policies is disabled (System menu > Database policies > Advanced tab). **Note:** This feature is only accessible if the security context of the folder allows users to perform the document task "Change document and folder key" (System menu > Account management > Document roles > General tab).

Document key format tab, Document type-specific keys	command buttons	**Note:** This feature is only accessible if the option "Deny change document or folder key" in the Database policies is disabled (System menu > Database policies > Advanced tab). **Note:** This feature is only accessible if the security context of the folder allows users to perform the document task "Change document and folder key" (System menu > Account management > Document roles > General tab).
	Add	Opens the Add specific key format dialog, which allows you to select a document type from a drop-down list and define both a Document and a Template key format for this particular document type. **Tip:** See the two notes above.
	Remove	Deletes the Document and the Template key format of the Document type currently selected in the table. **Tip:** See the two notes above.
	Edit	Opens the Edit default key format dialog, which allows you to modify both the Document and the Template key format applicable to the document type currently selected in the table. **Tip:** See the two notes above.
	Document type	Lists the document types for which Document and Template key formats are defined for this folder.
	Document key, Template key	These two columns display the Document and Template key formats defined for the document types listed in the table.
Document restrictions tab (bottom of tab)	Change configuration/ Reset configuration toggle	Activates all other controls on this tab, or resets all restrictions defined on this tab to their default.

Document restrictions tab, Templates	Restrict available templates	Specifies the templates available to users to generate documents in the current folder. To specify the templates, you store them in another folder which you designate for this purpose. **Note:** The settings of the lower section on this tab (Document-type specific templates) override the settings of the upper section (Templates).
	Template folder text box	Allows you to enter the path to the folder you want to designate as template folder. The template folder is to hold all templates you want to make available to users to generate documents in the current folder.
	Change button	Opens the Select folder dialog, which allows you to navigate to and select the folder you want to designate as template folder. The template folder is to hold all templates you want to make available to users to generate documents in the current folder.
	New documents must be created using templates	Restricts how users can create new documents in the current folder. Hides all entries that are not templates in the Create a new document dialog (File menu > New) for the current folder.
Document restrictions tab, Document type-specific templates	Only documents of the listed document types can be saved to this folder	Specifies the document types that users can save to the current folder. To specify the document types, you add them to the table. **Note:** The settings of the lower section on this tab (Document-type specific templates) override the settings of the upper section (Templates).
	Add	Opens the Configure document type dialog, which allows you to select a document type from a drop-down list and assign it to the current folder. If the database has templates for the document type you select, the dialog also allows you to select and enable a "mandatory" template. This hides all entries that are not templates for the document type when users open the Create a new document dialog (File menu > New) for the current folder. **Tip:** For each document type, you can only assign one mandatory template to be used in the current folder. If you need several templates for a document type, put them in a single folder and enable both options in the Templates section of this tab.

Remove	Unassigns the Document type currently selected in the table from the current folder.
Edit	Opens the Configure document type dialog for the Document type currently selected in the table, which allows you to select and enable a "mandatory" template for the document type. This hides all entries that are not templates for the type when users open the Create a new document dialog (File menu > New) for the current folder. **Tip:** For each document type, you can only assign one mandatory template to be used in the current folder. If you need several templates for a document type, put them in a single folder and enable both options in the Templates section of this tab.
Document type	Lists the document types of which users can save documents to the current folder.
Template, Template key	These two columns display the name and unique identification key of any mandatory templates assigned to the document types for the current folder.

4.3.3 Document templates

Standardize the structure of documents and define initial values to be set in documents generated from templates. Exercise fine-grained control over user access to particular sections and even individual data elements within documents.

File **>** Open template or create New **>** Content editor **>** Protection settings pane

Open a template or create a new template to display the Protection settings pane at the bottom of the Content editor.

Document templates simplify tasks, standardize processes, and improve data security. They allow you to define document structures that are frequently needed, for example, to match the setup of an assay that is frequently run. Document templates also allow you to define initial values to be set in documents. And they enable you to exercise very fine-grained control over who can view and edit document sections and even individual data elements within documents.

PLA allows you to enforce the use of templates and prevent users from creating documents that are not generated from templates. To enforce templates, you define Document restrictions in the Folder properties. Please consult the Folder properties section of the Administration Guide for additional information.

When users work with documents generated from templates, the "Open with elevated permissions" command (File menu) enables them to override settings provided by the template. Users have access to this command if the security context of the document's folder allows them to perform the document task "Edit documents with elevated permissions" (PLA 3.0.5)/

"Edit field protections" (PLA 3.0.4) (System menu > Account management > Document roles > General tab).

When users open templates, the controls of the Protection settings pane are only accessible to the extent to which the security context of the template's folder allows them to perform related document tasks, that is, "Read documents" and "Edit documents" (System menu > Account management > Document roles > General tab).

Tip: Please consult the User Guide and video tutorials available on our website for additional practical advice on how to create and work with templates.

Protection settings pane
The following table explains the features and controls available in the Protection settings pane.

Section	Item	Description
Title of the Protection settings pane	Protection settings for <element name>	Displays the name of the element currently selected in the Content editor. The settings displayed in the Protection settings pane apply to this particular element. If you want to change the Protection settings of another element, you have to first select it in the Content editor. **Tip:** To prevent users from changing observation data, for example, select the Observation data element in the Content editor and adjust its Protection settings according to your needs.
Permissions section	View element	Shows this element in documents generated from the template. **Note:** If you disable this option, PLA hides this element in documents generated from the template, but still uses it in calculations and other processes.
	Edit value	Allows users to change the value of this element in documents generated from the template.
	Switch element	Applies to elements that belong to a set of options such as the six regression model types in Quantitative response assay documents. Displays the current element in a drop-down box that allows users to switch to another option. **Tip:** If you disable this option, PLA does not display the drop-down box and users cannot select an alternative.

	Delete element	Makes the Delete command available for this element if the element is not required by the document type. **Tip:** If you disable this option, PLA does not display the Delete command in context menus for this element.
	Add child element	Allows users to add subelements to this element. **Tip:** Subelements are not available for all element types. The availability of subelements for a particular element type also depends on the document type.
	Apply to descendants	Applies the Protection settings of the current element to every subelement of the current element. **Note:** This command applies to all subelements irrespective of whether PLA displays them in the Content editor.
Initial value section	text box	Defines the initial value to be set for the current element in all documents generated from the template. **Tip:** You can use placeholders to define initial values to be set in documents generated from templates.
	placeholder dialog	Lists all placeholders available to define the initial value. Allows you to select and insert placeholders. To insert a placeholder: 1. Click the Initial value text box and press CTRL + Space to display the dialog. **Tip:** Drag the bottom-right corner to expand the dialog. 2. Double-click the placeholder to insert it into the Initial value text box. **Tip:** Single-click placeholders to display brief descriptions. **Tip:** Please consult the table below for additional information on particular placeholders.

Initial value placeholders

The following table explains all placeholders available to define the initial values to be set in documents generated from templates.

Item	Description
currentdate	Inserts the current date when the document is generated from the template.
currentdatetime	Inserts the current date and time when the document is generated from the template.
currenttime	Inserts the current time when the document is generated from the template.
digest:DOCKEY: SECTIONKEY:PROPERTY	Inserts a property of an external document. Define the following parameters to specify the property to be inserted: • DOCKEY: Specifies the key of the document that contains the property. • SECTIONKEY: Specifies the key of the section that contains the property. **Note:** Do not enter a value for this parameter if the property is not part of a section. **Tip:** In Quantitative response assays, for example, the values of the Name subelements in Standard sample, Test sample, and Control sample elements serve as Section keys. • PROPERTY: Specifies the key of the property.
elementcolor	Applies the first predefined color that has not yet been assigned within the document.

elementcounter	Inserts the first number (smallest integer) that has not yet been assigned to this element type within the document. Example: 1. Add two Comment elements to a template, and add the Subject subelement to each Comment element. 2. In the Initial value text box of each of the two Subject subelements, type the word "Instruction", type a space, and insert the elementcounter. 3. Save the template, and generate a document from the template. Results: The first Comment element has the Subject line "Instruction 1", and the second has the Subject line "Instruction 2". **Note:** If you delete elements, PLA reuses the numbers that had been assigned to them. **Tip:** Use the keyedcounter placeholder rather than the elementcounter placeholder if you want to apply (1) two or more counters to one element type or (2) one counter across two or more element types within a single document. And use the sequence placeholder (from PLA 3.0.5) to apply a counter across two or more documents generated from the template.
empty	Applies to elements that have values assigned in the template. Omits the values in documents generated from the template.
generator	Applies to documents generated by other documents. Inserts the document key of the document that has generated the current document.

keyedcounter:KEY	Inserts the first number (smallest integer) that has not yet been assigned to this key within the document. Define the following parameter: • KEY: Specifies the key used to identify elements where the numbers provided by the counter are to be inserted. Example: 1. Add three Comment elements to a template, and add the Subject subelement to each Comment element. 2. In the Initial value text box of two of the Subject subelements, type the word "Instruction", type a space, insert the keyedcounter, and replace "KEY" with "comment_key_inst". 3. In the Initial value text box of the third Subject subelement, type the word "Requirement", type a space, insert the keyedcounter, and replace "KEY" with "comment_key_req". 4. Save the template, and generate a document from the template. Results: The first Comment element has the Subject line "Instruction 1", the second has the Subject line "Instruction 2", and the third has the Subject line "Requirement 1". **Note:** If you delete elements, PLA reuses the numbers that had been assigned to them. **Tip:** If you enter additional text—outside the curly braces—in the Initial value fields, this text also needs to be identical for all elements that are to share a single counter. **Tip:** Use the elementcounter placeholder rather than the keyedcounter placeholder if you want to apply a counter to elements of the same element type within a single document. And use the sequence placeholder (from PLA 3.0.5) to apply a counter across two or more documents generated from the template.

sequence:PADDING:PREFIX:SUFFIX (PLA 3.0.5)	Inserts a string that can serve as a key. The string consists of a suffix, a counter with padding, and a suffix. Define the following parameters to specify the string to be inserted: • PADDING: Specifies the minimum number of digits to be used for the counter. Enter a number (integer) such as "5" if the counter is to have at least five digits. • PREFIX: Specifies the prefix of the string to be inserted. • SUFFIX: Specifies the suffix of the string to be inserted. Example: 1. Add a Comment element to a template, and add the Subject subelement to the Comment element. 2. Insert the sequence placeholder in the Initial value text box of the Subject subelement, and replace "PADDING" with "5", "PREFIX" with "have_", and "SUFFIX" with "_coffee(s)". 3. Save the template, and generate two documents from the template. Results: • The first document has the Subject line "have_00001_coffee(s)". • The second document has the Subject line "have_00002_coffee(s)". **Note:** If you delete elements, PLA reuses the numbers that had been assigned to them. **Tip:** Please consult information on the elementcounter and keyedcounter placeholders provided above if you want to apply separate counters in each document generated from the template.
userdisplayname	Inserts the Display name of the current user when the document is generated from the template.
userloginname	Inserts the Login name of the current user when the document is generated from the template.