Administration guide

PRISMAdirect

Administration settings and tasks

océ

A CANON COMPANY

Canon

Production Systems - Cutsheet

Contents

Chapter 2
Central server...75

Chapter 3
Web server...107

Chapter 4
Generic application..**145**

Index..**155**

Chapter 1
Global settings

Copyright

Trademarks

"Océ" and "PRISMA" are trademarks or registered trademarks of Océ.

Adobe®, Acrobat®, Reader® and Distiller® are registered trademarks of Adobe® Systems Incorporated.

Portions copyright © 2011 Enfocus BVBA; all rights reserved.

PostScript® 3™ is a registered trademark of Adobe® Systems Incorporated.

Microsoft®, Windows® , Windows NT®, Windows 98®, Windows 2000®, Windows XP®, Windows Server 2003® are either registered trademarks or trademarks of Microsoft® Corporation in the United States and/or other countries.

Xerox®, DigiPath®, DocuSP® and DocuTech® are registered trademarks of the Xerox® Corporation in the U.S. and/or other countries.

Fiery®, Command WorkStation® and EFI® are registered trademarks of Electronics for Imaging (EFI®), Inc.

SAP® Crystal Reports® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

Products in this publication are referred to by their general trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks of their respective companies.

Software version

This documentation describes the functionality of PRISMAdirect v1.2.

[Login]

[Login]

Introduction

Depending on the application configuration, it may be necessary to identify yourself. You have to enter your user name and password.

Procedure

1. Enter your user name.
2. Enter your password.
3. Click [Log in].

📝 NOTE
A [Web user] or [LDAP user] can login to the server when that user belongs to the [Services] group.

📝 NOTE
A system administrator can login to the server.

[General settings]

Define the [General settings]

Introduction

[You can configure the general settings in this dialog.]

These settings are used by the application regardless if the application is installed on one PC or as a distributed system.

[Web server settings]

Settings	Description
[Allow Web Submission user to change the language]	Enable this option to allow a user to change the language of the Web Submission. If this option is disabled, Web submission is displayed in the installation language and the user is not able to change the language.
[Copyright administration]	Enable this option to make the customer responsible that submitted files are not copyright protected. The customer can only submit a job with option [Copyright administration] enabled. When the customer enables this option, the customer indicates that the submitted files are not copyright protected.
[Enable 'Download' page]	You can enable or disable the 'downloads' link within Web Submission here. When the Web Submission user clicks the 'downloads' link, the 'Download' page will appear.
[Filter query:]	The defined filter determines which jobs are visible for a user of [Web Submission]. The filter is an SQL query. Click button [Edit filter] to open the [Define filter query] dialog. You can *Define a query* on page 15.

[Allowed file types]	You can select the following options:
	• [Custom]
	  This option allows you to configure the supported types of digital documents (for example PDF, DOC, PS, ...). Use a comma to separate the custom document types.
	• [All]
	  All document types are accepted.

[Custom columns]	Click the [Edit columns] button. You can add items to the [Active job ticket items] field. The items in field [Active job ticket items] are displayed as columns in the Operator Console(s). Click the [Move up] and [Move down] buttons to set the correct order of the columns. The item in the top becomes the leftmost column. The item at the bottom becomes the rightmost column.

Settings	Description
[Copyright administration message:]	A default message is displayed to the customer or operator when: • The [Copyright administration] option is enabled in this dialogue. • The [Copyright administration] option is not enabled by the customer or operator when a job is submitted. Click [Edit message] to change the default message.
[Motivation for job cost approval:]	In the Web Submission, the customer can type a motivation to approve the job cost. The default title of the text field is [Reason to approve job cost:]. Click [Edit message] to change the default title.

[Operator Console settings]

Settings	Description
[Allow the operator to change the files of jobs]	Enable this option to allow the operator to change the files of jobs in the job details of the selected job. When this option is enabled, the operator can: • [Add digital file], [Add paper original] and [Add other digital file]. • A product can contain a fixed document. The operator can remove the fixed document and can add other files to the job. • A product can contain a fixed VDP document. The operator can remove the fixed VDP document and can add other files to the job. • [Delete] a file. • [Replace] a file. • [Edit] a non-PDF file. NOTE [Web Submission] users submit files to the [Operator Console]. The [Web Submission] users must be confident that the files are printed exactly as submitted. When you enable this option, there is no guarantee that the submitted files will remain unchanged before the job is printed.
[Always add the JobID to the subject of the email]	Enable this option to add the JobID to the subject of each email which is sent from the application. To be able to identify the job in the email client, the JobID must be added to the subject. NOTE This option must be enabled when Microsoft Outlook is installed. The operator can create jobs and accept jobs in Microsoft Outlook.
[Assign imported jobs automatically to the operator]	Enable this option to assign imported jobs automatically to the operator that imports the jobs.

Settings	Description
[Current job number]	This option contains the job number of the last job. You can define any job number with a maximum value of 999999999. The next submitted job has job number: [Current job number] + 1. ✎ NOTE Multiple jobs with the same job number can appear in the job list, when you change the [Current job number].
[Delete finalized jobs automatically after]	Enable this option to delete finalized jobs automatically from the [Central server]. You can define after how many days the jobs must be deleted.

[Global settings]

Settings	Description
[Shop window]	Define the default shop window for the [Operator Console] and the [Web Submission] users. ✎ NOTE You can assign a different shop window for each user group.

[VDP settings]

Settings	Description
[Maximum pages for preview:]	Define the maximum number of pages of a variable data document shown in the [Preview] or [Proof PDF]. The maximum value for this option is 2000 pages. ✎ NOTE A high number of pages can decrease the performance of the application.

Define a query

Introduction

The defined filter determines which jobs are visible for a user of [Web Submission]. The filter is an SQL query.

Procedure

1. Drag and drop the job ticket items and operators in the query field'.
   To create an SQL query, you can use:
   • The available job ticket items
   • The available operators
   • The additional operators: ', ", +, -, /, %

   The following rules apply:
   • Numbers are integers. A decimal separator is not allowed.
   • String values are enclosed in quotation marks.
   • Dates are enclosed in quotation marks. A date must be a valid date according to the regional settings of the computer.
   • Enumeration values are enclosed in quotation marks.
   • Boolean values are enclosed in quotation marks.

   Examples:

Type	Valid value	Invalid value
Number	53	34.5
String	'Hello'	Hello
Dates	'1/1/10'	1/1/10
Enumeration	'Enum_value'	Enum_value
Boolean	'True'	True

2. Example of a valid SQL query:
   [Date] >= '1/1/10'

Job ticket print settings

Introduction

[You can configure the print settings for the job ticket in this dialog.]

Define the font settings

Procedure

1. Click [Edit] to start the [Edit print settings for job ticket] dialog.
   - [Job ticket title settings]
     Define how the title of the job ticket must be printed.
   - [Group item settings]
     Define how the group items of the job ticket must be printed.
   - [Item settings]
     Define how the job ticket items must be printed.
2. For each job ticket category, you can define the font with option [Font name:].
3. For each job ticket category, you can define the [Font size:].
4. For each job ticket category, you can define the [Font style:]
   - [Bold]
   - [Italic]
   - [Underline]
   - [Strikethrough]

Define the logo settings

Procedure

1. Click [Edit] to start the [Edit print settings for job ticket] dialog.
2. Click the [Edit logo settings] button.
3. Click button [Browse] to select an image.
   The allowed image file types are: .bmp, .jpg, .gif, .png.
4. Enable the [Print logo in job ticket] option to print the logo in the job ticket.
5. Determine the [Logo position:].
   Here are the available logo positions:
   • [Bottom left corner]
   • [Bottom right corner]
   • [Top left corner]
   • [Top right corner]
6. [Scale logo to page size]
   You can scale the logo to the page size. Enable the [Keep ratio] option to use the same relation between width and height for the logo as for the page size.
7. Click the [OK] button.

[Accounting settings]

Enable accounting

Introduction

You can collect accounting information. To collect accounting information, a job ticket must contain the following job ticket fields with these exact names:

1. [Account]
2. [Company]
3. [Copies]
4. [FinalCost]
5. [NrOfSourcePages]
6. [Plexity]
7. [PrintInColor]
8. [ReadyDate]

NOTE
The ReadyDate item is not visible in the Job Ticket Editor.

9. [User ID]

NOTE
The system administrator can edit the captions of these items.

NOTE
The accounting information cannot be collected if the job ticket definition contains an item with a name longer than 128 characters.

The job ticket is allowed to contain other job ticket fields.

The operator must be able to assign values to those job ticket fields which are used for accounting. Use the Job Ticket Editor to make these job ticket fields available for editing by the operator.

The accounting information is saved in an SQL database. A report of the accounting information can be generated with the Report Manager. To open the Report Manager:
• Type the URL "http://localhost/reports$printroom" when you use SQL 2005.
• Type the URL "http://localhost/reports_printroom" when you use SQL 2008.

Enable accounting

Procedure

1. Enable the [Enable accounting] option.

Disable accounting

Procedure

1. Disable the [Enable accounting] option.

SQL authentication type

Procedure

1. Click the [Configure credentials] button.
   The [Edit accounting and payment settings] dialog opens.
2. Define the [Computer name \ instance name:].
   With this option, you define where the accounting database is stored.
   For example: SQL_server_name\SQL_server_instance_name.

   ✎ NOTE
   A license is required to use the accounting functionality.

3. You must define how the Operator Console connects to the accounting database.

Setting	Description
[Windows authentication]	The current Windows user information is used for the authentication. The user is not prompted for a user name and password.
[SQL authentication]	The user must type a user name and password for the SQL server.

   ✎ NOTE
   Accounting information can be collected when the user has system administration rights on the accounting database.

4. Click the [Test connection] button.
   Click this button to test the connection to the defined server.
5. Click the [OK] button.

Upload the reports

Procedure

1. Define the report server settings:

Setting	Description
[Folder path:]	Define the reports location. This is the location where the Operator Console stores the accounting reports. The default location for the reports is: <installation path>\Oce \PRISMAaccess\Reports.
[URL of report server:]	Should be one of the following: • http://<computer name>/ReportServer$Printroom/ReportSer-vice2005.asmx for SQL Server 2005 • http://<computer name>/ReportServer_Printroom/ReportSer-vice2008.asmx for SQL Server 2008 The uploaded reports are retrieved from the defined URL of the re-port server. The available reports are displayed in dialogue [Edit email settings].

2. Select the [Overwrite existing reports] option to overwrite any existing reports on the report server.
3. Click the [Upload] button.
   The reports are uploaded from the reports location to the report server.

Edit email settings

Introduction

Accounting reports can be sent automatically by email, if:
- The [Email accounting reports automatically] option is enabled,
- Task AutomaticReportsEmailSender is configured, and
- One or more accounting reports are available in field [Selected reports:].

Procedure

1. Enable the [Email accounting reports automatically] option.
2. Define the [Reporting period:].
   The accounting reports for the defined reporting period are emailed.
3. Define the [Email address(es):].
   When you add more than one email address, you must use a semicolon to separate the addresses.
4. Define the subject of the email.
5. Define the body of the email.
6. Select the [File format for report:].
   The reports are converted into the selected format. The converted reports are attached to the email.
7. Select which reports you want to attach to the email.
   Select one or more of the [Available reports:]. Click [Add selected report(s)]. The reports are added to field [Selected reports:]. The selected reports are sent by email.
   Select one or more of the [Selected reports:]. Click [Remove selected report(s)]. The reports are added to field [Available reports:]. The available reports are not sent by email.
8. Click [OK].

NOTE
You must configure task AutomaticReportsEmailSender.

Create and edit task AutomaticReportsEmailSender

Introduction

Accounting reports can be sent automatically by email, if:
• The [Email accounting reports automatically] option is enabled,
• Task AutomaticReportsEmailSender is configured, and
• One or more accounting reports are available in field [Selected reports:].

Procedure

1. Click [Create task].
2. Define the [Password:].
3. Click [Create].
   The [AutomaticReportsEmailSender] task is created in the task scheduler. The task is executed with the provided credentials.
4. Click [Edit task].
   The task scheduler opens.
5. Click [Task Scheduler Library].
6. Right-click the [AutomaticReportsEmailSender] task and select [Properties].
7. Configure task [AutomaticReportsEmailSender].
   For example, you can change the schedule of the task.
8. Click [OK].
   Close the task scheduler.

Edit invoice settings

Introduction

In this dialog, you can define the company information for the invoice. The [Operator Console] uses the collected accounting information to generate the invoice.

Procedure

1. Click the [Edit invoice settings] button.
2. Click button [Browse] to select an image.
   The allowed image file types are: .bmp, .jpg, .gif, .png.
3. Type the company name.
4. Type the company address.
5. Define the [Tax rate(%):] that must be used for the invoice.
6. Click the [OK] button.

[Default cost settings]

Click [Edit] to define the default cost settings for all users.

Click [Edit formula(s)] to open the formula manager. In the formula manager, you can create and configure the cost estimation formula(s) and the job quotation formula(s).

Define the default cost settings

Introduction

In this dialog, you can define the default cost settings for all users. When a user is part of a user group, the [User group settings] overwrite the default cost settings of the user.

The payment providers offer a payment service for your users. When you select one or more payment providers, each user can pay for their orders directly. You can enable the payment service in this dialog. However, [Budget management] is disabled when you enable option [Use payment providers].

NOTE
In the Job Ticket Editor, you define the payment settings per product. The payment settings in the product overrule the default payment settings in this dialog.

NOTE
A license is required to use the job quotation functionality.

NOTE

A license is required to use the [Job cost approval] functionality.

[Edit default cost settings]

Job cost settings

Setting	Description
[Job cost estimation]	• [Yes] The [Job cost estimation] option is available in Web Submission. A user is always presented with an estimation of the job cost. • [No] The [Job cost estimation] option is not available in Web Submission. A user is never presented with an estimation of the job cost. • [Always] A user is always presented with an estimation of the job cost. The user cannot submit the job until the cost estimation to be presented.
	Click the [Select formula(s)] button to select a default cost estimation formula. **NOTE** You can select more than one cost estimation formula. [The first formula in the list is the default formula. All other formula(s) calculate an alternative job cost.] **NOTE** In the Job Ticket Editor, the system administrator selects a job cost estimation formula for each product. The formulas in the product overrule the formulas assigned to the user in this dialog.

Setting	Description
[Job quote]	• [Yes] The [Job quote] option is available in Web Submission. A user can request the calculated job cost. • [No] The [Job quote] option is not available in Web Submission. A user cannot request the calculated job cost. • [Always] A user is always presented with the calculated job cost. The user cannot disable the request to calculate the job cost. ✎ NOTE A license is required to use the job quotation functionality. The operator calculates the job cost and sends the job quotation to the customer.
	Option [Job cost can be accepted on behalf of the customer.] Enable this option to allow the operator to accept the job cost on behalf of the customer. Disable this option to force the customer to accept or reject the job cost.
	Option [A job can be printed only after the job cost is calculated.] Enable this option to force the operator to always calculate the job cost. The job cost must be calculated for a correct budget control.
	[You must select a job quotation formula.] ✎ NOTE In the Job Ticket Editor, the system administrator selects a job quotation formula for each product. The formulas in the product overrule the formulas assigned to the user in this dialog.
[Budget management]	Enable this option to enable the default [Job cost approval] workflow. In [User settings] and [User group settings] you can define the [Job cost approval] workflow for separate users and user groups. ✎ NOTE A license is required to use the [Job cost approval] functionality. ✎ NOTE [Budget management] is disabled when you enable option [Use payment providers].

Setting	Description
[Budget]	Define the total budget for all jobs per user. Click the value in the drop-down list to define a custom value. This budget is used for all users that have no budget defined in [User settings]. The default value is [Unlimited]. • [Unlimited]: There is no limit to the budget for this user. • Custom value: You can define the total budget for this user. Click the value in the drop-down list to define a custom value. ✎ NOTE You can type a value in the drop-down list for the budget.
[Send email to job cost approver(s) when the total job cost exceeds:]	Define a percentage of the [Budget]. When this percentage of the budget is exceeded, an email message is sent to the job cost approver of the customer. The [Job cost approver] is defined in the [Preferences] dialog of the [Web Submission]. The email message is predefined but it can be changed. It can be changed from the Operator Console, in the section E-mail templates. This option becomes available when you define a custom value for the [Budget] option. ✎ NOTE Independent of this setting, an email message is sent to the [Job cost approver] when the budget for this user is exceeded.
[Maximum job cost at level {0}:]	Define a maximum job cost for the current level. When the job cost exceeds the maximum job cost, a [Job cost approver] of the current level must approve or reject the job. If the job cost exceeds the maximum job cost of the next level, a [Job cost approver] of that level must also approve or reject the job. The default value is [Unlimited]. • [Unlimited]: There is no limit to the job cost for this level. The job cost approver for this level can accept an unlimited job cost. • Custom value: You can define a maximum job cost for this level. Click the value in the drop-down list to define a custom value. ✎ NOTE You can type a value in the drop-down list for the budget.
[Add new level]	Click the [Add new level] button to define a maximum job cost for the new level. The maximum job cost of the new level must be higher than the maximum job cost of the previous level.
[Remove last level]	Click the [Remove last level] button to remove the last level. ✎ NOTE You cannot remove level 1.

Setting	Description
[Email address of job cost approver(s):]	Define the email address of the job cost approver(s) for level 1. When you add more than one email address, you must use a semicolon to separate the addresses. The job cost approver(s) must approve or reject the job when the job cost exceeds the maximum job cost for level 1.
	🖉 **NOTE** You can only define the job cost approver(s) for level 1.
	🖉 **NOTE** The [Job cost approver] for level 1 can send the approval form to the [Job cost approver] for level 2.
	When a customer logs on to the [Web Submission] for the first time, the [Preferences] dialog opens. Setting [Job cost approver] is automatically filled with the defined email address(es) in this dialog.
	🖉 **NOTE** The customer can change the [Job cost approver] in the [Preferences] dialog of the [Web Submission].
[Allow a job cost approver to accept on behalf of higher level approver(s).]	Enable this option to [Allow a job cost approver to accept on behalf of higher level approver(s).].
	🖉 **NOTE** When you enable this option, each job cost approver can always accept or reject a job, regardless of the job cost.
[Create task] [Edit task]	See procedure [Edit task].

Setting	Description
[Generate report]	Click button [Generate report] to generate a comma-separated values (CSV) report. Browse to the location where you want to save the file. Enter a file name and click [Save].
	The report contains: • [Type] The user budget or the user group budget • [Name] The name of the user or user group • [Budget] The user budget or the user group budget • [Default budget] True: the user is part of a user group and uses the budget as defined for the user group. False: the user can be part of a user group, but a custom budget value is used. • [Used budget] The amount spent of the [Budget]. • [Send email to job cost approver(s) when the total job cost exceeds:] True: the defined percentage of the budget is exceeded. An email is sent to the job cost approver. • [Percentage] The defined percentage of the budget.
[Use payment providers]	When you enable this option, each user can pay for their orders directly. You can enable one or more payment providers. 🖉 NOTE You must enable job cost estimation if you want to use the payment service. 🖉 NOTE When you enable this option, [Budget management] is disabled.
[Payment providers]	You can enable one or more payment providers. A payment report is created and stored on the SQL server. You must configure the credentials for the SQL server to access the payment report. See *SQL authentication type payment* on page 30.
[Currency]	Select a currency from the drop-down list. You can also define a custom currency. Enable the [Custom] option to type a custom currency sign.
[Currency sign:]	Define the location of the currency sign: • [Before the amount] • [After the amount]
[Number of decimals:]	Configure the allowed number of decimals for the job cost.

[Edit task]

1. Click [Create task].

2. Define the [Password:].
3. Click [Create].
   The [BudgetApprovalQuotaCleaner] task is created in the task scheduler. The task is executed with the provided credentials.
4. Click [Edit task].
   The task scheduler opens.
5. Click [Task Scheduler Library].
6. Right-click the [BudgetApprovalQuotaCleaner] task and select [Properties].
7. Configure the [BudgetApprovalQuotaCleaner] task.
   For example, you can change the schedule of the task.
8. Click [OK].
   Close the task scheduler.

You can reset the [Used budget]:
1. Right-click [BudgetApprovalQuotaCleaner].
2. Select [Run]. The value of [Used budget] is reset to zero.

NOTE
By default, the value of [Used budget] is reset to zero monthly.

SQL authentication type

Introduction

You can enable one or more payment providers. A payment report is created and stored on the SQL server. You must configure the credentials for the SQL server to access the payment report.

The payment report is stored in the accounting database on the SQL server. You do not have to enable the accounting functionality to create and access the payment report. The accounting functionality and the payment report can be enabled independently.

Procedure

1. Click the [Configure credentials] button.
   The [Edit accounting and payment settings] dialog opens.
2. Define the [Computer name \ instance name:].
   With this option, you define where the accounting database is stored.
   For example: SQL_server_name\SQL_server_instance_name.
3. You must define how the Operator Console connects to the accounting database.

Setting	Description
[Windows authentication]	The current Windows user information is used for the authentication. The user is not prompted for a user name and password.
[SQL authentication]	The user must type a user name and password for the SQL server.

NOTE
The payment report can be collected when the user has system administration rights on the accounting database.

4. Click the [Test connection] button.
   Click this button to test the connection to the defined server.
5. Click the [OK] button.

LDAP servers

Introduction

The [LDAP servers] dialog displays the LDAP servers which are available to the application. The application searches for LDAP servers in the local network and domain during the start up of the application. All available LDAP servers are added to the list in the top of the dialogue.

The LDAP servers can be added to two different lists:
- [Servers used for authentication:]
  The first LDAP server in the list is used for the authentication of a user. If the user cannot be authenticated by the first server, then the second server is used, etc.
  Click the 'Up' and 'Down' buttons to set the correct order of the LDAP servers used for authentication.
  User data can be collected from each server in this list.
- [Servers used to retrieve user data:]
  The servers in this list are only used to retrieve user data that is available on an LDAP server. The retrieved user data is filled in automatically in the mapped profile attributes and the mapped job ticket items.

Click [Add] or [Edit] to open the [Edit LDAP server settings] dialog.

Click [Delete] to delete an LDAP server.

✎ NOTE
You can delete the LDAP servers that you do not use for the application. However, the application searches for LDAP servers at start up of the application. The found LDAP servers are added to the list in the top of the dialogue.

Click [Search] to search for any available LDAP servers in the local network and domain.

LDAP servers for the central server and the web server

If the central server and the web server are installed on the same machine, the [LDAP servers] dialogue is available in:
- The [Global settings] for both the central server and the web server.
  The servers in the list of [Servers used for authentication:] are used to authenticate:
  - The [Web Submission] users.
  - The users of the application. For example, the operators.

If the central server and the web server(s) are installed on separate machines in a distributed system, the [LDAP servers] dialogue is available in:
- The [Global settings] for the central server.
  The servers in the list of [Servers used for authentication:] are used to authenticate the users of the application. For example, the operators.
  In dialogue [Global settings], you define which LDAP servers are used for authentication and to retrieve user data for the central server. On all machines where dialogue [Global settings] is installed, the list of LDAP servers for the central server is the same.
- The [Web server] for the web server(s).
  The servers in the list of [Servers used for authentication:] are used to authenticate the [Web Submission] users.

✎ NOTE
If the [Web Submission] users cannot be authenticated, the application uses the LDAP servers in [Global settings] to authenticate the users.
For each web server, you can define which LDAP servers are used for authentication and to retrieve user data. The used LDAP servers can be different for each web server.

Refresh the LDAP information

Click [Refresh] to refresh the generic info about the LDAP, users and groups part of that LDAP.

PRISMAdirect stores some information about each LDAP locally. The information regards generic info about the LDAP, users and groups part of that LDAP. In order for it to be in sync with the real information, a service synchronizes this information automatically once a day, at midnight. If you want to synchronize this information manually, you have to use the [Refresh] functionality which starts an update of the information stored for all the LDAP servers.

The connection status of each LDAP server is displayed in column [Status].
- Green dot:
  The connection to the LDAP server is established.
- Orange dot:
  The connection to the LDAP server is not checked or the connection is being checked.

NOTE

After a reboot of the system, the dots are orange. Click [Test connection] to update the state of each LDAP server.

- Red dot:
  The connection to the LDAP server cannot be established. Check the settings of the LDAP server.

Add or edit an LDAP server

Procedure

1. Click [Add] or [Edit] to open the [Edit LDAP server settings] dialog.
   When you add a new LDAP server you have to configure the LDAP server settings.
2. You can configure the LDAP server(s) in this dialogue.

Setting	Description
[Domain name for LDAP server:]	You can define a custom name for the LDAP server. The custom name must be unique. ✎ NOTE An LDAP server can be used for Windows authentication of users.
[Credentials policy:]	The credentials policy defines which credentials are used by the JDF Framework service to connect to the LDAP server. ✎ NOTE [Use common credentials] is the default value for the drop-down list. This value can always be used for each LDAP server. You can select one of the following credential policies: • [Use common credentials] These are the credentials that are stored in the global settings of the LDAP server. These credentials are used for each connected LDAP server. These credentials are not defined in the application by the user. [Use common credentials] is the default value for the drop-down list. This value can always be used for each LDAP server. • [Use the credentials which are stored on the LDAP server] These are the credentials that you define in [LDAP server user name:] and [LDAP user password:]. • [Use the credentials of the Windows user who runs the JDF Framework service] You can select this credential policy only for Secure-based authentication types. This credential policy supports Integrated Windows Authentication (IWA) only. These credentials are defined by the user during the installation of the application. The Windows user can be DocWorker, a local user, or a selected domain user. You can identify the Windows user who runs the JDF Framework in the Services dialogue of Microsoft Windows: .\JdfFramework: local user .\DocWorker: DocWorker Secure authentication type

▶

Setting	Description
[LDAP server user name:]	You must supply a user name and password to retrieve information from the LDAP server. ✎ NOTE This option is available when you have selected [Credentials policy:] [Use the credentials which are stored on the LDAP server].
[LDAP user password:]	You must supply a user name and password to retrieve information from the LDAP server. ✎ NOTE This option is available when you have selected [Credentials policy:] [Use the credentials which are stored on the LDAP server].

[Server address:]	You must define the address of the LDAP server. If you define only the address of the LDAP server, the users are searched through the entire LDAP server. You can also define the server address and the search root. When you define the server address and the search root, the search for users starts at the defined root on the server.
	For example: LDAP://sro.company.net:389/DC=sro,DC=company,DC=net, where:
	• sro.company.net
	  The address of the domain controller.
	• 389
	  The port which is used to connect to the LDAP server.
	• DC=sro,DC=company,DC=net
	  The path to search for users in the active directory tree on the LDAP server.
	
	✎ NOTE
	The default port number for a non-secure connection is 389. The default port number for a secure connection is 636.

[Server type:]	Select a server type. The server types which start with "Native…" are preferred. The other server types are available for backwards compatibility.
[Use secure connection (SSL)]	Select this option if you want to create a secure connection to the LDAP server. To be able to select this option, the LDAP server has to support this. ✎ NOTE The default port number for a non-secure connection is 389. The default port number for a secure connection is 636. ✎ NOTE Please make sure that you update the port number if you want to use a secure connection.

▶

Setting	Description
[User filter:]	A default user filter is created automatically for new LDAP servers. You must define: 1. [Domain name for LDAP server:] 2. [Credentials policy:] 3. [Server address:] 4. [Server type:] 5. Click the [OK] button. 6. Select the new LDAP server. Click the [Edit] button. The default filter is now available in the [Edit LDAP server settings] dialog. You can edit the filter. The minimum filter is the LDAP attribute for user name, for example: (sAMAccountName=%u). The user filter must contain "%u" as placeholder for the user name. The minimum filter will always work, but it is not time efficient. Only users that pass the filter can be imported from the LDAP server. ✏ NOTE The filter must be updated when the [LDAP attribute for user name:] is changed.
[LDAP attribute for user name:]	You can define the LDAP attribute that contains the user name. ✏ NOTE The default LDAP attribute is used for the user name if this field is left empty. The default LDAP attribute depends on the server type.
[User group filter:]	A default user group filter is created automatically for new LDAP servers. You must define: 1. [Domain name for LDAP server:] 2. [Credentials policy:] 3. [Server address:] 4. [Server type:] 5. Click the [OK] button. 6. Select the new LDAP server. Click the [Edit] button. The default filter is now available in the [Edit LDAP server settings] dialog. You can edit the filter. The minimum filter is the LDAP attribute for group name, for example: (cn=%g). The user group filter must contain "%g" as placeholder for the user group name. The minimum filter will always work, but it is not time efficient. Only user groups that pass the filter can be imported from the LDAP server. ✏ NOTE The filter must be updated when the [LDAP attribute for group name:] is changed.

Setting	Description
[LDAP attribute for group name:]	You can define the LDAP attribute that contains the group name. ✎ NOTE The default LDAP attribute is used for the group name if this field is left empty. The default LDAP attribute depends on the server type.

Advanced settings

Authentication types

You can select an authentication type for the [Authentication used to connect to LDAP server:] option and the [Authentication used to connect user to the LDAP server:] option. The authentication types are described in the tables below.

✎ NOTE
In LDAP "authentication" is called "bind".

Authentication type	Description
None	None means a simple bind to the server using plain text credentials. A simple bind is the only binding mechanism defined in the LDAP specification itself. None has a high compatibility across LDAP server vendors. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: All server types, but this authentication type is not recommended.
NoneAndServerBind	This is the None authentication type combined with the ServerBind optimisation. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: ActiveDirectory, but this authentication type is not recommended.
NoneAndFastServerBind	This is the None authentication type combined with ServerBind and FastBind optimizations. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: ActiveDirectory, but this authentication type is not recommended.
Anonymous	Anonymous means that no authentication is done. Most LDAP servers do not allow anonymous access by default, or give a very restrictive access to the server. Possible usage: All server types, but this authentication type is not recommended.
AnonymousAndServerBind	This is the Anonymous authentication type combined with the ServerBind optimisation. Possible usage: ActiveDirectory, but this authentication type is not recommended.

Authentication type	Description
AnonymousAndFastServerBind	This is the Anonymous authentication type combined with ServerBind and FastBind optimizations. Possible usage: ActiveDirectory, but this authentication type is not recommended.
Secure	Secure is the Windows authentication method, which relies on the Windows Security Support Provider Interface (SSPI). The SSPI usually selects the Windows Negotiate protocol with Kerberos or NTLM authentication. Secure supports both explicit credentials and Integrated Windows Authentication (IWA). WARNING: ActiveDirectoryFastDelegationSecureBinding is preferred for better security over Secure. Possible usage: ActiveDirectory, NativeADS, NativeLDAP with a Windows-based LDAP Server.
FastSecureBinding	This is the Secure authentication type combined with the FastBind optimisation. WARNING: ActiveDirectoryFastDelegationSecureBinding is preferred for better security over FastSecureBinding. Possible usage: ActiveDirectory, NativeADS.

SecureSocketLayer	SecureSocketLayer means that a TLS/SSL communication channel is used to encrypt all the network traffic. The encryption includes the bind and exchange of credentials. This is the recommended setting for most LDAP servers, when security must be guaranteed without using the Windows authentication and security mechanisms. However, the setup is complex because SecureSocketLayer requires that the server has a valid server certificate installed. And the client must trust the Certificate Authority (CA) which issued the server certificate.
	The analysis of SecureSocketLayer problems can be complex:
	• For ADSI-based connectors:
	  Any SecureSocketLayer-related problems are reported in the Windows System Event log. If the server certificate is invalid, the SecureSocketLayer connection will fail.
	• For non-ADSI-based connectors:
	  Any SecureSocketLayer-related problems are reported in the dialogue that appears after you click button [Test connection]. If the server certificate is invalid, a warning is reported but the SecureSocketLayer connection will succeed.
	
	Possible usage: SunDirectoryServer, NativeLDAP, NativeADS.
	This authentication type is recommended.

Authentication type	Description
FastSecureSocketLayer	This is the SecureSocketLayer authentication type combined with the FastBind optimisation for ADSI-based connectors, or FastConcurrentBinding optimisation for non-ADSI connectors. Possible usage: SunDirectoryServer, NativeLDAP, NativeADS. This authentication type is recommended.
ActiveDirectoryFastSecureBinding	This is the Secure authentication type combined with the Sealing, Signing and FastBind optimization. The users are authenticated against ActiveDirectory servers. Possible usage: ActiveDirectory, NativeADS.
ActiveDirectoryFastDelegationSecureBinding	This is the Secure authentication type combined with the Sealing, Signing, Delegation, and FastBind optimization. The users are authenticated against ActiveDirectory servers. Possible usage: ActiveDirectory, NativeADS. This authentication type is recommended for ActiveDirectory.
Basic	Basic means a simple bind to the server using plain text credentials. This authentication type is very similar to None. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: All server types, but this authentication type is not recommended.
BasicWithFastConcurrentBinding	This is the Basic authentication type combined with the FastConcurrentBinding optimisation. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: All server types, but this authentication type is not recommended.
BasicWithFastConcurrentBindingAndSSL	This is the Basic authentication type combined with the FastConcurrentBinding optimization and a SecureSocketLayer communication channel. Possible usage: NativeLDAP. This authentication type is recommended.
Negotiate	This is the Windows Negotiate authentication, which means the same as Secure authentication. Negotiate results in Kerberos or NTML authentication. Possible usage: ADAM and NativeLDAP connectors against a Windows-based LDAP server.
Kerberos	The Kerberos authentication is almost the same as Secure authentication. Kerberos results in Kerberos authentication. WARNING: Negotiate is preferred over Kerberos. Possible usage: ADAM and NativeLDAP connectors against a Windows-based LDAP server.

Authentication type	Description
NTML	The NTML authentication is almost the same as Secure authentication. NTML results in NTML authentication. WARNING: Negotiate is preferred over NTML. Possible usage: ADAM and NativeLDAP connectors against a Windows-based LDAP server.
Digest	This is the Windows Digest Access authentication. Possible usage: ADAM and NativeLDAP connectors against a Windows-based LDAP server.

Authentication optimisations and options

Authentication optimisations and options	Description
ServerBind	With optimization ServerBind, only the server which is specified in the connection URL is addressed. It is usually safe to use ServerBind for most LDAP servers and for ActiveDirectory when the specific domain controller is addressed. Failover servers for ActiveDirectory are not addressed.
FastBind	With FastBind optimization, the objectClass attribute on the server is not used. This increases the performance. Optimization FastBind is only valid for ADSI-based connectors, such as ActiveDirectory or NativeADS.
FastConcurrentBinding	With optimization FastConcurrentBinding no security token is created. This increases the performance when only user authentication is needed. Optimization FastConcurrentBinding is only valid for non-ADSI based connectors, such as ADAM, NativeLDAP, SunDirectoryServer.
SecureSocketLayer	With option SecureSocketLayer, a TLS/SSL communication channel is created to encrypt all network traffic.
Sealing	Optimization Sealing activates additional encryption capabilities of SSPI.
Signing	Optimization Signing activates additional data integrity checking capabilities of SSPI.
Delegation	Optimization Delegation activates the ability of using the Windows security context across domains.

Procedure

1. Click button 'Advanced' and define:
2. [Authentication used to connect to LDAP server:]
   You can define the type of authentication which the application uses to connect to the LDAP server.
3. [Authentication used to connect user to the LDAP server:]
   You can define the type of authentication which the application uses to authenticate a user on the LDAP server.
4. Allow automatic creation of users:

Every user who logs on to the application with an [LDAP server user name:] and an [LDAP user password:] is created automatically.

The [User type] of an automatically created user becomes:

• [Windows user] if the user is authenticated via Windows authentication.

• [LDAP user] if the user is authenticated via Forms authentication.

An automatically created user belongs to the [Group] of 'Submitters'.

The users in the 'Submitters' group can access the [Web Submission].

Test the connection

Procedure

1. Click [Test connection] to test the connection to the selected LDAP server. The connection status of each LDAP server is displayed in column [Status].
    The following data is required for the test:
    • [LDAP server user name:]
    • [LDAP user password:]
    • [Server address:]
    • [Use secure connection (SSL)]

    The following checks are done :
    • Connect + bind to the server using the 4 settings you have specified;
    • Read of RootDSE;
    • Probe for a user entry to enumerate user attributes;
    • Probe for a group entry to enumerate group attributes.

Use LDAP server for authentication

Introduction

The [LDAP servers] dialog displays the LDAP servers which are available to the application. The application searches for LDAP servers in the local network and domain during the start up of the application. All available LDAP servers are added to the list in the top of the dialogue.

The LDAP servers can be added to two different lists:
- [Servers used for authentication:]
  The first LDAP server in the list is used for the authentication of a user. If the user cannot be authenticated by the first server, then the second server is used, etc.
  Click the 'Up' and 'Down' buttons to set the correct order of the LDAP servers used for authentication.
  User data can be collected from each server in this list.
- [Servers used to retrieve user data:]
  The servers in this list are only used to retrieve user data that is available on an LDAP server. The retrieved user data is filled in automatically in the mapped profile attributes and the mapped job ticket items.

Procedure

1. Select an LDAP server from the list of available LDAP servers.
2. Click the [Use for authentication] button.
   The LDAP server is added to the list [Servers used for authentication:].
3. Click [Test connection] to test the connection to the selected LDAP server.

Use LDAP server to retrieve user data

Procedure

1. Select an LDAP server from the list of available LDAP servers.
2. Click the [Use to retrieve user data] button.
   The LDAP server is added to the list [Servers used to retrieve user data:].
3. Click [Test connection] to test the connection to the selected LDAP server.

Map LDAP attributes to job ticket items

Introduction

You can map information that is available within the LDAP server to job ticket items. The job ticket items then automatically receive the data from the LDAP attribute.

Add a mapping

Procedure

1. Enable the [Collect user data from this LDAP server] option.
2. Click the [Set &ticket mapping] button.
   The [Map LDAP attributes to job ticket items] dialog opens.
3. Click the [Add] button.
4. Select a job ticket item from the list.
5. Define the LDAP attribute that contains the information that you want to use for the job ticket item.
6. Click the [Add] button.
   The defined LDAP attribute is mapped to the job ticket item.

Edit a mapping

Procedure

1. Click the [Set &ticket mapping] button.
   The [Map LDAP attributes to job ticket items] dialog opens.
2. Select a mapped LDAP attribute in the list.
3. Click the [Edit] button.
4. Define the LDAP attribute that contains the information that you want to use for the job ticket item.

   📝 NOTE
   The [Job ticket item] cannot be changed.

5. Click the [OK] button.
   The defined LDAP attribute is mapped to the job ticket item.

Remove a mapping

Procedure

1. Select a mapped LDAP attribute in the list.
2. Click the [Remove] button to remove an existing mapping.

Edit profile mappings

Introduction

You can map information that is available within the LDAP server to the [Profile settings] of the [Web Submission] users. The [Profile settings] of the [Web Submission] users then automatically receive the data from the LDAP server.

- If the LDAP attribute contains a value, the associated profile attribute is filled in. The Web Submission user cannot change the profile attribute.
- If the LDAP attribute does not contain a value, the associated profile attribute is left empty. The Web Submission user must define the value of the profile attribute.
- If you deselect a profile attribute, the user can change the value of the profile attribute.

NOTE
The LDAP attributes may not be present in all the LDAP servers or might not contain relevant information.

Procedure

1. Enable the [Collect user data from this LDAP server] option.
2. Click the [Set &profile mapping] button.
   The [Edit profile mappings] dialog opens.
3. Map the LDAP attributes to the profile attributes.
   Below you see the default LDAP attributes provided by PRISMAdirect. You can change these in order to retrieve other relevant information from the LDAP server.

Profile attributes	LDAP attributes
[First name:]	givenName
[Last name:]	sn
[Department:]	department
[Location:]	roomNumber
[Company:]	company
[Telephone number:]	telephoneNumber
[Email address:]	mail
[Account:]	departmentNumber

[Email settings]

Configure Email settings

You can configure the:
*   Email settings of the print room
*   SMTP server used by the Operator Console

Item	Description
[Email address:]	You can specify the e-mail address that will be used in the 'From' field of the e-mail message. When the e-mail message cannot be delivered to the user, the error message will be sent to this address.
[Name:]	You can specify the name that will be used in the 'From' field of the e-mail message. For example: 'Print room'
[Cc address(es):]	You can specify the e-mail address(es) that will be used in the 'Cc' field of the e-mail message.
[SMTP server:]	You can specify the address of the email server here. Ask your IT department for details.
[Port:]	You specify the port number of the email server here. Ask your IT department for details. Only SMTP mail servers are supported. The range for the port number is: 0 to 64000.
[Operator must have rights to send emails on behalf of:]	Defines if the Printroom Operator can always send an email on behalf of or that he needs rights. The IT department determines the rights of the Printroom Operator outside of PRISMAdirect.
[Send emails from Central server:]	Choose whether the e-mails are sent directly from the Operator Console(s) or from the Central Server. This can be important because of virus scanners, strict policy and firewall rules in place on the different PCs.
[IP-number of Web Submission server:]	The IP address of a web server which is connected to the Central server. The operator can send an email to the customer with a link to a job. The link consists of the IP address of a web server, the name of the virtual folder and the unique id of the job. • Jobs submitted from the web submission: The job ticket contains the IP address of the web server where these jobs were created. For these jobs, the IP address from the job ticket is used to build the link. • Jobs created in the Operator Console: The job ticket does not contain an IP address of a web server. For these jobs, the IP address of option [IP-number of Web Submission server:] is used.
[Web Submission virtual folder:]	Define a folder on the web server which you defined in option [IP-number of Web Submission server:]. The operator can send an email to the customer with a link to a job. The link consists of the IP address of a web server, the name of the virtual folder and the unique id of the job.

NOTE

Use the 'Operator console' application to specify the contents of the E-mail messages.

[Advanced email settings]

NOTE

"[Advanced email settings]" is not available if the Cc address is not filled in or not filled correctly.

1. Click the **Advanced** button.
   The [Advanced email settings] dialog opens.
2. You can define that an email is sent to the cc address(es) when:
   • [The job is accepted.]
   • [The job is ready.]
   • [The proof PDF is sent.]
   • [The job is finalized.]

[Test connection]

1. Click the [Test connection] button to test the connection to the [SMTP server:].

[Profile settings]

Edit profile settings

Introduction

You can map the [Profile settings] of the [Web Submission] user to job ticket items. When the [Web Submission] user submits a job, the job ticket items automatically receives the data from the [Profile settings].

- If the profile attribute contains a value, the associated job ticket item is filled in automatically. The Web Submission user cannot change the job ticket item.
- If the profile attribute does not contain a value, the associated job ticket item is left empty. The Web Submission user must define the value of the job ticket item.
- If you deselect a profile attribute, the Web Submission user must define the value of the job ticket item.

All the profile attributes are fixed and cannot be changed. All the job ticket items presented as default to a user can be changed to create another mapping from profile attributes to job ticket items, except for "Job Cost Approver" profile attribute which can be mapped **only** to "Job Cost Approver" job ticket item.

[Map profile attributes to job ticket items]

Profile attributes	[Job ticket items]
[First name:]	[First name]
[Last name:]	[Last name]
[Department:]	[Department]
[Location:]	[Location]
[Company:]	[Company]
[Telephone number:]	[Telephone number]
[Email address:]	[Email address]
[Account:]	[Account]
[Job cost approver]	[Job cost approver]

[User settings]

Add or edit a user

Introduction

You can configure the [Budget management] for each user in the [User settings] dialog. You can also configure the [Budget management] for the user groups. The [Budget management] settings do not overwrite each other. The [Budget management] settings for the user are applied to the user and the [Budget management] settings for the user group are applied to the user group.

Add or edit a user

User settings

Setting	Description
[User name:]	Define the [User name:]. The [User name:] must be unique. ✎ NOTE Be aware that the following characters are not allowed in a username: @";:<>|?/*[],=+ The [User name:] cannot be changed when you edit the user.
[Role:]	Define the [Role] of the user. • [Services] The users in the [Services] group have the highest rights. These users can access the System Administration, the [Job Ticket Editor], the [Operator Console] and the [Web Submission]. • [Operators] The users in the [Operators] group can access the [Job Ticket Editor], the [Operator Console] and the [Web Submission]. • Submitters The users in the 'Submitters' group can access the [Web Submission].
[User groups:]	You can add a user to one or more user groups.
[Set as default group]	When a user is added to one or more user groups: You must add a user to a default user group. The budget of the default user group is used for this user.
[Password:]	Define the [Password:] for this user. The password must be different from the user name. Use the following rules to define a strong password: • The password must have at least 8 characters. • The password must use both upper case and lower case characters. • The password must contain at least one number. • The password must be different from the user name. ✎ NOTE The password can not be changed for any user logged in to System Administration at the same time.

Setting	Description
[Confirm password:]	Confirm the password.
[Budget management]	In [User settings] and [User group settings] you can define the [Budget management] workflow for separate users and user groups.
[Budget]	Define the budget for all jobs for this user. You can type a value in the drop-down list for the budget. The default value is [Default]. • [Default]: The budget for this user is the value of option [Budget] in the [Default cost settings] dialog. • [Unlimited]: There is no limit to the budget for this user. • Custom value: You can define the budget for this user. Click the value in the drop-down list to define a custom value. 📝 NOTE You can type a value in the drop-down list for the budget. 📝 NOTE The user can be part of a default user group. In that case, the [Budget] of the default user group is used for the user.
Used budget	The used budget for this user is displayed on the right of option [Budget].
[Send email to job cost approver(s) when the total job cost exceeds:]	Define a percentage of the [Budget]. When this percentage of the budget is exceeded, an email message is sent to the job cost approver of the customer. The [Job cost approver] is defined in the [Preferences] dialog of the [Web Submission]. The email message can be changed in Tools - Email template editor. This option becomes available when you define a custom value for the [Budget] option. 📝 NOTE Independent of this setting, an email message is sent to the [Job cost approver] when the budget for this user is exceeded.

Setting	Description
[Maximum job cost at level {0}:]	Define a maximum job cost for the current level. When the job cost exceeds the maximum job cost, a job cost approver of the current level must approve or reject the job. If the job cost exceeds the maximum job cost of the next level, a job cost approver of that level must also approve or reject the job. The default value is [Default]. • [Default]: The maximum job cost as defined for this level in the [Default cost settings] dialog is used. • [Unlimited]: There is no limit to the job cost for this level. The job cost approver for this level can accept an unlimited job cost. • Custom value: You can define a maximum job cost for this level. You can type a value in the drop-down list. If job cost approval is required, an email message is sent to the job cost approver for level 1. The job cost approver for level 1 is defined by the customer in the [Preferences] dialogue of the [Web Submission]. NOTE You can type a value in the drop-down list. NOTE The job cost approver for level 1 can send the approval form to the job cost approver for level 2.
[Add new level]	Click the [Add new level] button to define a maximum job cost for the new level. The maximum job cost of the new level must be higher than the maximum job cost of the previous level.
[Remove last level]	Click the [Remove last level] button to remove the last level. You cannot remove level 1.
[Custom filter settings:]	Enable this option to [Allow only the use of custom filters.] for this user in the [Operator Console]. You can create the custom filters in the [Manage filters] dialog. When you enable this option, the other filters in the [Operator Console] are disabled.

[Reset spent budget]

1. Click the [Edit] button. The [Edit user settings] dialog opens.
2. Click the [Reset spent budget] button.
   The spent budget of the user is reset to zero.

NOTE
You can only reset the spent budget of a user if you have defined a custom value for the [Budget] option.

Import a user

Procedure

1. Click the [Import] button.
    The [Import users] dialog opens.
2. Select an LDAP server from the drop-down list for option 'Select LDAP server'.
3. Select which user(s) you want to import from the LDAP server.

    ### NOTE
    To be able to import groups or users from a LDAP server, the test connection should be successful.

    ### NOTE
    You cannot add a [User role] to an imported user. When you add the user to a user group, the user receives the role of the user group. You also can only change the default group of an imported user amongst the groups it belongs to in the LDAP server. Also, you cannot change its password.

4. Click the [Import] button.

Remove a user

Procedure

1. Select a user in the list of users.
2. Click the [Remove] button.
   The user is removed from the list of users.

Refresh the list of users

Procedure

1. Click button [Refresh] to update the list of users.
   The list of users is usually updated automatically.

   ✎ NOTE
   You use refresh only in exceptional cases when something went wrong and the automatic refresh did not work.

[User group settings]

Add or edit a user group

Introduction

You can define the default cost settings for each user in the [User settings] dialog. When a user is part of a user group, the [User group settings] overwrite the default cost settings of the user.

You can configure the [Budget management] for each user in the [User settings] dialog. You can also configure the [Budget management] for the user groups. The [Budget management] settings do not overwrite each other. Both are applied. The [Budget management] settings for the user are applied to the user and the [Budget management] settings for the user group are applied to the user group.

Add or edit a user group

Setting	Description
[User group name:]	Define the [User group name:]. The [User group name:] must be unique. ✎ NOTE Be aware that the following characters are not allowed in a user group name: @";:<>|?/*[],=+ The [User group name:] cannot be changed when you edit the user group.
[Role:]	Define the [Role] of the user group. • [Services] The users in the [Services] group have the highest rights. These users can access the System Administration, the [Job Ticket Editor], the [Operator Console] and the [Web Submission]. • [Operators] The users in the [Operators] group can access the [Job Ticket Editor], the [Operator Console] and the [Web Submission]. • Submitters The users in the 'Submitters' group can access the [Web Submission].
[Budget management]	You can define the [Budget management] workflow for separate user groups.
[Budget:]	Define the budget for all jobs for this user group. All users, which are part of this user group, use the [Budget]. You can type a value in the drop-down list for the budget. The default value is [Unlimited]. • [Unlimited]: There is no limit to the budget for this user group. • Custom value: You can define the budget for this user group. Click the value in the drop-down list to define a custom value. ✎ NOTE You can type a value in the drop-down list for the budget.

Setting	Description
Used budget	The used budget for this user group is displayed on the right of the [Budget] option.
[Send email to job cost approver(s) when the total job cost exceeds:]	Define a percentage of the [Budget]. When this percentage of the budget is exceeded, an email message is sent to the job cost approver of the customer. The [Job cost approver] for level 1 is defined by the customer in the [Preferences] dialog of the [Web Submission]. The email message is predefined and cannot be changed. This option becomes available when you define a custom value for the [Budget] option. NOTE Independent of this setting, an email message is sent to the [Job cost approver] when the budget for this user is exceeded.
[Maximum job cost at level {0}:]	Define a maximum job cost for the current level. When the job cost exceeds the maximum job cost, a job cost approver of the current level must approve or reject the job. If the job cost exceeds the maximum job cost of the next level, a job cost approver of that level must also approve or reject the job. The default value is [Unlimited]. • [Unlimited]: There is no limit to the job cost for this level. The job cost approver for this level can accept an unlimited job cost. • Custom value: You can define a maximum job cost for this level. You can type a value in the drop-down list. When job cost approval is required, an email message is sent to the job cost approver for level 1. The [Job cost approver] for level 1 is defined by the customer in the [Preferences] dialogue of the [Web Submission]. NOTE You can type a value in the drop-down list. NOTE The job cost approver for level 1 can send the approval form to the job cost approver for level 2.
[Add new level]	Click the [Add new level] button to define a maximum job cost for the new level. The maximum job cost of the new level must be higher than the maximum job cost of the previous level.
[Remove last level]	Click the [Remove last level] button to remove the last level. You cannot remove level 1.

Setting	Description
[Email address of job cost approver(s):]	Define the email address of the job cost approver(s) for level 1. When you add more than one email address, you must use a semicolon to separate the addresses. These job cost approver(s) must approve or reject the job when the job cost exceeds the maximum job cost for level 1. NOTE You can only define the job cost approver(s) for level 1. NOTE The job cost approver for level 1 can send the approval form to the job cost approver for level 2. When a customer logs on to the [Web Submission] for the first time, the [Preferences] dialog opens. Setting [Job cost approver] is automatically filled with the defined email address(es) of the job cost approver(s). NOTE The customer can change the [Job cost approver] in the [Preferences] dialog of the [Web Submission].
[Shop window]	• [Use global settings] Use the settings for [Shop window] as defined in the [General settings] dialog. • [Use custom value(s)] Use custom settings for [Shop window] for this user group.
[Allowed file types]	• [Use global settings] Use the settings for [Allowed file types] as defined in the [General settings] dialog. • [Use custom value(s)] Use custom settings for [Allowed file types] for this user group.
[Job cost estimation]	• [Use global settings] Use the settings for [Job cost estimation] as defined in the [Default cost settings] dialog. • [Use custom value(s)] Use custom settings for [Job cost estimation] for this user group. NOTE You can select more than one cost estimation formula. [The first formula in the list is the default formula. All other formula(s) calculate an alternative job cost.] NOTE In the Job Ticket Editor, the system administrator selects a job cost estimation formula for each product. The formulas in the product overrule the formulas assigned to the user group in this dialog.

Setting	Description
[Job quote]	• [Use global settings] Use the settings for [Job quote] as defined in the [Default cost settings] dialog. • [Use custom value(s)] Use custom settings for [Job quote] for this user group. ✎ NOTE In the Job Ticket Editor, the system administrator selects a job quotation formula for each product. The formulas in the product overrule the formulas assigned to the user group in this dialog.
[Copyright administration]	• [Use global settings] Use the settings for [Copyright administration] as defined in the [General settings] dialog. • [Use custom value(s)] Use custom settings for [Copyright administration] for this user group.
[Allow Web Submission user to change the language]	• [Use global settings] Use the settings for [Allow Web Submission user to change the language] as defined in the [General settings] dialog. • [Use custom value(s)] Use custom settings for [Allow Web Submission user to change the language] for this user group.
[Enable 'Download' page]	• [Use global settings] Use the settings for [Enable 'Download' page] as defined in the [General settings] dialog. • [Use custom value(s)] Use custom settings for [Enable 'Download' page] for this user group.
[Define filter for jobs in Web Submission]	• [Use global settings] Use the settings for the filter as defined in the [General settings] dialog. • [Use custom value(s)] Use custom settings for the filter for this user group. Click button [Edit filter] to open the [Define filter query] dialog. You can *Define a query* on page 15.
[Enable Océ PRISMAaccess archive module]	• [Use global settings] Use the settings for [Archive settings] as defined in the [Archive settings] dialog. • [Use custom value(s)] Use custom settings for [Archive settings] for this user group.
[Custom columns]	• [Use global settings] Use the settings for [Custom columns] as defined in the [General settings] dialog. • [Use custom value(s)] Use custom settings for [Custom columns] for this user group.

Setting	Description
[Use file hosting providers]	• [Use global settings] Use the settings for [File hosting providers] as defined in the [File hosting providers] dialog. • [Use custom value(s)] You can enable or disable the use of file hosting providers. ✎ NOTE You can select which payment providers are available in the [Default cost settings] dialog.
[Payment settings]	You can enable or disable the payment service for this user group. This option is available when option [Use payment providers] is enabled in the [Default cost settings] dialog.

[Reset spent budget]

1. Click the [Edit] button. The [Edit user group settings] dialog opens.
2. Click the [Reset spent budget] button.
   The spent budget of the user is reset to zero.

✎ NOTE
You can only reset the spent budget of a user if you have defined a custom value for the [Group budget:] option.

Define a query

Introduction

The defined filter determines which jobs are visible for a user of [Web Submission]. The filter is an SQL query.

Procedure

1. Drag and drop the job ticket items and operators in the query field'.
   To create an SQL query, you can use:
   • The available job ticket items
   • The available operators
   • The additional operators: ', ", +, -, /, %

   The following rules apply:
   • Numbers are integers. A decimal separator is not allowed.
   • String values are enclosed in quotation marks.
   • Dates are enclosed in quotation marks. A date must be a valid date according to the regional settings of the computer.
   • Enumeration values are enclosed in quotation marks.
   • Boolean values are enclosed in quotation marks.

   Examples:

Type	Valid value	Invalid value
Number	53	34.5
String	'Hello'	Hello

Type	Valid value	Invalid value
Dates	'1/1/10'	1/1/10
Enumeration	'Enum_value'	Enum_value
Boolean	'True'	True

2. Example of a valid SQL query:
   [Date] >= '1/1/10'

Copy a user group

Procedure

1. Select a user group.
2. Click the [Copy] button.
3. Define a group name.
4. Click the [OK] button.
   A new user group is created with the same settings as the selected user group.

Import a user group

Procedure

1. You can import user groups from an LDAP server, or from a file.
    Click button [Import from file]. Browse to the file. Click the [Open] button. The user group is imported.

    ✎ NOTE
    The file type can be csv or xml.

    The next steps describe how you can import a user group from an LDAP server.
2. Click button [Import from LDAP].
    The [Import LDAP user groups] dialog opens.
3. Select an LDAP server from the drop-down list for option 'Select LDAP server'.
4. Select which user group(s) you want to import from the LDAP server.

    ✎ NOTE
    To be able to import groups or users from a LDAP server, the test connection should be successful.

5. Define the [Role] of the users in the user group(s).
    *   [Services]
        The users in the [Services] group have the highest rights. These users can access the System Administration, the [Job Ticket Editor], the [Operator Console] and the [Web Submission].
    *   [Operators]
        The users in the [Operators] group can access the [Job Ticket Editor], the [Operator Console] and the [Web Submission].
    *   Submitters
        The users in the 'Submitters' group can access the [Web Submission].
6. Click the [Import] button.

Export a user group

Procedure

1. Click button [Export to file].

   ✎ NOTE
   Groups imported from LDAP servers can not be exported to a file.

2. Browse to a location.
3. Define a name for the file.
4. Select the file type.
   The file type can be csv or xml.
5. Click the [Save] button.

Remove a user group

Procedure

1. Select a user group in the list of user groups.

   NOTE
   Groups imported from LDAP servers can not be deleted .

2. Click the [Remove] button.
   The user group is removed from the list of user groups.

Refresh the list of user groups

Procedure

1. Click the [Refresh] button to update the list of user groups.
   The list of user groups is usually updated automatically.

   📝 NOTE
   You use refresh only in exceptional cases when something went wrong and the automatic refresh did not work.

[Preflight settings]

Configure the preflight rules

Introduction

[You can configure the preflight settings in this dialog.]

You can preflight a PDF file. The preflight operation checks if any rules are violated in the PDF file(s). The set of rules is fixed. You can configure some of the rules. The preflight operation automatically fixes the violations according to the configured rules. A preflight report and an annotated file are generated. The preflight report shows a summary of the problems that have been found and fixed.

✎ NOTE
If the preflight operation cannot fix a violation, the violation is reported.

Procedure

1. Configure the available rules:
   - [PDF actions and scripting rule:]
     Click this rule to configure the rule. If you configure this rule, the preflight operation automatically fixes the violations of this rule.
   - [Content too close to border rule:]
     Click this rule to configure the rule. If you configure this rule, the preflight operation automatically fixes the violations of this rule.
   - [Embedded fonts rule:]
     Click this rule to configure the rule. If you configure this rule, the preflight operation automatically fixes the violations of this rule.
   - [Hairline rule:]
     Click this rule to configure the rule. If you configure this rule, the preflight operation automatically fixes the violations of this rule.
   - [Image compression is too high rule:]
     Click this rule to configure the rule. If you configure this rule, the preflight operation automatically fixes the violations of this rule.
   - [Image resolution is too high rule:]
     Click this rule to configure the rule. If you configure this rule, the preflight operation automatically fixes the violations of this rule.
   - [Image resolution is too low rule:]
     Click this rule to configure the rule. If you configure this rule, the preflight operation automatically fixes the violations of this rule.
   - [Restricted permissions rule:]
     You can only enable or disable this rule. You cannot configure this rule.
   - [Transparency rule:]
     You can only enable or disable this rule. You cannot configure this rule.
   - [Overprint rule:]
     You can only enable or disable this rule. You cannot configure this rule.
2. Enable or disable each rule in the [Enabled] column.
3. Define the [Severity] of each rule.
   - [Warning]
     A violation of the rule is detected. You can ignore the warning, or the preflight operation can fix the violation.
   - [Error]

A violation of the rule is detected. The violation of the rule must be fixed by the preflight operation.

4. You can define a [Timeout for preflight [min.]].
   Enable the [Timeout value for preflight [min.]] option and define a value. The value is the timeout value in minutes.
   When the timeout value is exceeded, the preflight operation is canceled.

5. Click [OK].

[Archive settings]

Edit the archive settings

Introduction

[You can configure the archive settings in this dialog.]

Procedure

1. Click [Edit] to start the [Edit archive settings] dialog.
2. Option [Enable Océ PRISMAaccess archive module]:
   • Enabled: the Océ PRISMAaccess archive module is available in the Operator Console.
   • Disabled: The Océ PRISMAaccess archive module is not available in the Operator Console.

   NOTE
   A license is required to use the Océ PRISMAaccess archive module.

3. Define the [Archive server:].
   You must define the FQDN of the [PRISMAarchive] server .
4. Define the [Archive folder for Job Ticket Editor:].
   The Job Ticket Editor stores any files from the archive in this folder. For example, you create a product with a fixed document. The fixed document is a file which is retrieved from the archive. The file is stored in the defined folder.

   NOTE
   When the file changes in the archive, the file in the folder must be updated manually.

5. Click the [OK] button.

Manage filters

Introduction

You can create custom filters. The custom filter are SQL queries. The custom filters become available in the [Operator Console].

Add or edit a custom filter

Procedure

1. Define the [Assign filter to operators:] option.
    You can assign the filter to one or more operators.
2. Define the filter name.

    ✎ NOTE
    The name of the filter must be unique.

3. You can type a description of the filter.
4. Add or edit the filter. AND operators are used in the filter expression when more than one job ticket item is added to the filter.
    For each job ticket item that you want to use in the filter, do the following:
    1. Select an item from the list of [Job ticket items].
        For example, you select item [1-sided or 2-sided].
    2. Enable the [Use job ticket item in filter] option.
        The job ticket item is marked with a funnel icon when it is used in the filter.
    3. Select which value of the item must be used for the filter.
        For example, you select value [2-sided].

Delete a custom filter

Procedure

1. Select a custom filter from the list of filters.
2. Click the [Remove] button.
   The custom filter is removed from the list of filters.

Refresh the list of custom filters

Procedure

1. Click the [Refresh] button to update the list of custom filters.

[Clone printers]

Introduction

You have several Operator Consoles installed. The printer drivers are installed and configured on one of the Operator Consoles. You can clone the printer drivers. Cloning means that the printer drivers are automatically installed and configured on another [Operator Console]. The [Clone printers] procedure consists of the following two steps:

1. Collect the printer data of the printer drivers.
   Once the printer data is collected, you can clone the printer driver(s).
2. Clone the printer drivers.
   The cloned printer drivers are installed on the selected [Operator Console]. The printer drivers are configured with the collected printer data.

   NOTE
   You can use the collected printer data only on similar operating systems.
   For example, you have collected the printer data from a Microsoft Windows XP system. You can only use the collected printer data on another Microsoft Windows XP system.

[Collect printer data]

Introduction

Collect the printer data of the printer drivers that are installed and configured on one of the Operator Consoles. Once the printer data is collected, you can clone the printer driver(s).

Procedure

1. Click the [Collect printer data] button.
   The [Printer data] dialog opens.
2. Select the printer driver(s) you want to collect the printer data from. You can select one or more printer driver(s).
3. Click the [OK] button.
   A message appears when the printer data is collected. The printer data is stored on the [Central Server].

   NOTE
   You can use the collected printer data only on similar operating systems. For example, you have collected the printer data from a Microsoft Windows XP system. You can only use the collected printer data on another Microsoft Windows XP system.

4. Close the [Collect printer data] dialog.

[Clone printer(s)]

Before you begin

The printer data must be collected. Once the printer data is collected, you can clone the printer driver(s).

Do this procedure on each [Operator Console] where you want to clone the printer driver(s).

Procedure

1. Click the [Clone printer(s)] button.
   The [Printer data] dialog opens. The [Printer data] dialog displays:
   - The printer driver(s) for which printer data is collected.
   - The printer driver(s) for the operating system of the selected [Operator Console].
     For example, the [Operator Console] is installed on a Microsoft Windows XP system. You have collected printer data from a Microsoft Windows 7 system. No printer driver(s) are available in the [Printer data] dialog.
2. Select the [Operator Console] on which you want to clone the printer driver(s).
3. Select which printer driver(s) you want to clone. You can select one or more printer driver(s).
4. Click the [OK] button.
   A message appears when the printer driver(s) are installed and configured on the selected [Operator Console].
5. Close the [Collect printer data] dialog.

Result

Directly after cloning, the cloned printer driver uses the same printing preferences as the original printer driver, i.e. setting [1-sided or 2-sided]. An operator can change the printing preferences of the original printer driver and/or the cloned printer driver. Now, the printing preferences between original and cloned printer driver deviate.

Open the Printer Settings administration console via the Start menu. You can enable the [Share printer settings] option to share a number of printer settings between the original and the cloned printer driver. See the Printer Settings help file to determine which printer settings can be shared.

[Delete collected printer data]

Before you begin

The printer data must be collected.

Procedure

1. Click the [Delete collected printer data] button.
   The [Printer data] dialog opens.
2. Select the system that contains the collected printer data.
3. Select for which printers you want to delete the collected printer data.
4. Click the [OK] button.
   The collected printer data is deleted for the selected printers,
5. Close the [Collect printer data] dialog.

[File hosting settings]

Manage the file hosting settings

Introduction

[You can manage the file hosting providers in this dialog.]

The file hosting providers provide an Internet hosting service specifically designed to host user files. When you enable file hosting providers, the users can add files from the hosting service - the "cloud" - to their job.

Procedure

1. Click [Edit] to start the [Manage file hosting settings] dialog.
2. Option [Use file hosting providers]:
   • Enabled: The user can select files from file hosting providers. You can select which file hosting providers are available for the user. For example: Dropbox.
   • Disabled: The user cannot select files from file hosting providers.
3. Click the [OK] button.

Chapter 2
Central server

Copyright

Trademarks

"Océ" and "PRISMA" are trademarks or registered trademarks of Océ.

Adobe®, Acrobat®, Reader® and Distiller® are registered trademarks of Adobe® Systems Incorporated.

Portions copyright © 2011 Enfocus BVBA; all rights reserved.

PostScript® 3™ is a registered trademark of Adobe® Systems Incorporated.

Microsoft®, Windows® , Windows NT®, Windows 98®, Windows 2000®, Windows XP®, Windows Server 2003® are either registered trademarks or trademarks of Microsoft® Corporation in the United States and/or other countries.

Xerox®, DigiPath®, DocuSP® and DocuTech® are registered trademarks of the Xerox® Corporation in the U.S. and/or other countries.

Fiery®, Command WorkStation® and EFI® are registered trademarks of Electronics for Imaging (EFI®), Inc.

SAP® Crystal Reports® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

Products in this publication are referred to by their general trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks of their respective companies.

Software version

This documentation describes the functionality of PRISMAdirect v1.2.

[Login]

[Login]

Introduction

Depending on the application configuration, it may be necessary to identify yourself. You have to enter your user name and password.

Procedure

1. Enter your user name.
2. Enter your password.
3. Click [Log in].

📝 NOTE
A [Web user] or [LDAP user] can login to the server when that user belongs to the [Services] group.

📝 NOTE
A system administrator can login to the server.

[General settings]

Define the [General settings]

Introduction

[You can configure the general settings in this dialog.]

[General settings]

General details

Setting	Description
[Collection of job data]	Enable this option to collect data of the jobs in the application and the operations performed on the jobs. ✎ NOTE Collection of job data can impact the performance of the application.
[Archive folder for Operator Console:]	Define the path to the import folder in the [Archive folder for Web Submission:] option. The Central server uses this folder to import jobs and documents from the archive. For example: C:\PRISMAaccessArchive\JobsFromArchive
[Print Prepare Manager service port:]	Define the port for the Print Prepare Manager Service. The VDP functionality is available in PRISMAaccess/prepare Core version 6.1.1 or higher. The PRISMAaccess/prepare Core is installed on the Central server. Therefore, all actions and validations concerning the VDP functionality are executed on the Central server. Jobs are created via the Web Submission and the Operator Console. Therefore, these applications must have access to the Central server when they are installed on separate computers. The Operator Console and the Web server connect to the Central server via the port for the Print Prepare Manager Service. ✎ NOTE The port for the Print Prepare Manager Service must be accessible from the Operator Console and the Web server.

[Import service settings]

Add an import folder

Introduction

The operator can manually import jobs into the [Operator Console], but it is also possible to automatically import jobs.

You can automatically import PDF files into the [Operator Console] via import folders.

Procedure

1. Click the [Edit] button.
   The [Edit import service settings] dialog opens.
2. Click the [Add] button.
   The [Edit import folder settings] dialog opens.
3. Define the [Import folder path].
   Click button [Browse] to select or create an import folder.
4. Enable or disable option [Preserve job state].
   - When this option is enabled for legacy jobs:
     If the job state of the legacy job was [Ready], the job state of the imported job is set to [Ready]. Else, the job state of the imported job is set to [New]

   📝 NOTE
   For jobs older than 5.0 the job state cannot be preserved and the state of the job will always be [New]

   - When this option is enabled for normal jobs:
     The job state of the imported job is equal to the job state of the exported job. All the allowed job operations and restrictions imposed by the job state apply on the imported job.
   - When this option is disabled for normal jobs:
     The job state of the imported job is set to [New]
5. Select the [Import job type].
   - [Always accept job]
     This import folder accepts only PDF files.
     Click button 'Edit default ticket' to define a custom ticket for all jobs in this particular import folder.
     The jobs will be imported using the current Default Generic Product. All the jobs will have the state Accepted.
   - [Normal job]
     This import folder accepts all jobs of the current application version 5.2, or higher.
     Normal jobs will be imported using the product with which they were created if this product still exists. If it does not exist they will be imported using the current Default Generic Product.
   - [JDF ticket job]
     This import folder must contain a JDF ticket. You must copy a JDF ticket in this import folder.
     The jobs will be imported using the current Default Generic Product.
     If this folder does not contain a JDF ticket, an empty JDF ticket is used for the jobs.
   - [Legacy job]
     You can copy legacy jobs to this import folder. A legacy job is a job created with an application version older than 5.2.
     The legacy job ticket is automatically converted to the default job ticket version on the Central server. All the Legacy jobs will be imported using the Legacy product.

- [Default ticket job]

  This import folder accepts only PDF files.

  Click button 'Edit default ticket' to define a custom ticket for all jobs in this particular import folder.

  The jobs will be imported using the current Default Generic Product.

- [PDF only job]

  This import folder accepts only PDF files

  The jobs will be imported using the current Default Generic Product.

- [Scanned job]

  This import folder accepts only scanned files.

  The operator must create a job which contains a [Paper Original]. The scanned file in the folder is automatically attached to the job which contains a [Paper Original].

  The default job ticket on the Central server is used for these jobs.

  Note: the scanned file must contain the job number. Then the scanned file is automatically attached to the job.

6. Click the [OK] button.

   The import folder is configured and added to the list of import folders.

Pause the import service

Introduction

You can pause the automatic import of jobs from the configured import folders.

Disable option [Pause import service:] to start the automatic import service again.

Procedure

1. Click the [Edit] button.
2. Enable the [Pause import service:] option.
   The import service is paused. Jobs are not imported anymore.

Related information

Restart the import service on page 84

Restart the import service

Procedure

1. Click the [Edit] button.
2. Disable the [Pause import service:] option.
   The import service is restarted.

Define the trace level

Introduction

You can define the trace level for the import service.

Procedure

1. Click the [Edit] button.
2. Define the trace level:
   - [Debug]
     The [Debug] trace level provides the most detailed log information.
   - [Error]
     The errors are logged.
   - [Info]
     The errors and information messages are logged

   NOTE
   The [Debug] trace level can impact the performance of the application.

[Export service settings]

Add or edit an export folder

Introduction

The operator can manually export jobs from the [Operator Console], but it is also possible to automatically export jobs. You can automatically export jobs from the [Operator Console] via export folders. You must create an export query. If the query is valid for a job, then that job is exported.

By default, all available files of a job are exported. You must configure if you want to export jobs of type [Stationery]. Jobs of types other than [Stationery] are exported by default when the query is valid for the job.

Procedure

1. Click the [Edit] button.
   The [Edit export service settings] dialog opens.
2. Click the [Add] button.
   The [Edit export folder settings] dialog opens.

   NOTE
   Click the [Edit] button to edit an existing export folder.

3. Define the [Export folder path].
   Click the [Browse] button to select or create an export folder.
4. Define the export query.
   If the query is valid for a job, then that job is exported.
   The export query is an SQL query which is uses job ticket items. You can *Define a query* on page 86 per export folder.
5. Enable or disable option [Delete job after export].
   When you enable this option, all exported jobs are removed from the [Operator Console].
6. Enable or disable option [Export original file(s) and job ticket only].
   If you enable this option, only the original file and the job ticket are exported.
   The following files are not exported:
   • The JDF ticket
   • The conversion file, if available
   • The redistill file, if available
   • The merged document, if available
7. Enable or disable option [Export jobs of type "Stationery"].
   When you enable this option, the JDF ticket and the job ticket are exported for [Stationery] type jobs. When you disable this option, nothing is exported for [Stationery] type jobs.
8. Click the [OK] button.
   The export folder is configured and added to the list of export folders.

Define a query

Procedure

1. Drag and drop the job ticket items and operators in the query field'.
   To create an SQL query, you can use:

- The available job ticket items
- The available operators
- The additional operators: ', ", +, -, /, %

The following rules apply:
- Numbers are integers. A decimal separator is not allowed.
- String values are enclosed in quotation marks.
- Dates are enclosed in quotation marks. A date must be a valid date according to the regional settings of the computer.
- Enumeration values are enclosed in quotation marks.
- Boolean values are enclosed in quotation marks.

Examples:

Type	Valid value	Invalid value
Number	53	34.5
String	'Hello'	Hello
Dates	'1/1/10'	1/1/10
Enumeration	'Enum_value'	Enum_value
Boolean	'True'	True

2. Example of a valid SQL query:
   [Date] >= '1/1/10'

Define the path to the job ticket for exported jobs

Introduction

A default job ticket is used for the jobs in the [Operator Console]. When jobs are exported, they are exported with the current default job ticket.

This default job ticket can be changed in the [Job Ticket Editor]. When the default job ticket is changed, the jobs in the [Operator Console] are automatically updated. However, the job ticket of the exported jobs must also be updated.

All exported jobs use a centrally-shared copy of the default job ticket which is used in the [Operator Console]. When the default job ticket is changed, the centrally shared copy of the job ticket for the exported jobs is also automatically updated.

You can define the folder where the centrally shared copy of the job ticket is stored for all exported jobs.

Procedure

1. Click the [Edit] button.
   The [Edit export service settings] dialog opens.
2. Define the [Default job ticket path:].
   Click the [Browse] button to select or create the folder for the job ticket for exported jobs.
   The centrally shared copy of the default job ticket is stored in this folder for all exported jobs.

Pause the export service

Introduction

You can pause the automatic export of jobs from the configured export folders.

Procedure

1. Click the [Edit] button.
2. Enable the [Pause export service:] option.
   The export service is paused. Jobs are not exported anymore.

Related information

Restart the export service

Procedure

1. Click the [Edit] button.
2. Disable the [Pause export service:] option.
   The export service is restarted.

Define the trace level

Introduction

You can define the trace level for the export service.

Procedure

1. Click the [Edit] button.
2. Define the trace level:
   - [Debug]
     The [Debug] trace level provides the most detailed log information.
   - [Error]
     The errors are logged.
   - [Info]
     The errors and information messages are logged

   NOTE
   The [Debug] trace level can impact the performance of the application.

[Ticket mappings]

Use job ticket settings in printer driver

Introduction

You can use the values in the job ticket directly in the corresponding settings in the printer driver. You can create [PTT mappings] and [UPP mappings]. You can use the [UPP mappings] for a printer, when the printer is available in the drop-down list of the [UPP mappings]. All the printers installed on your machine that support the [UPP mappings] will be available in the drop-down list of the [UPP mappings]. The Unified Print Path (UPP) printers use the same technology as PRISMAprepare to print page programmed documents.

✏ NOTE

A printer can be available in the drop-down lists of the [UPP mappings] and the [PTT mappings]. The printer which supports the [UPP mappings] is used to print.

The job ticket items that you can use are defined in the [Job Ticket Editor]. You can use job ticket items of type: [Choice], [Yes/No] and [Number]. For [UPP mappings] you can also map [Text] items.

You can use the values of the job ticket in:
- [All printers]
  The values of the job ticket are used in all printer drivers.
  At least one printer that supports [UPP mappings] must be installed to see items in the [Printer parameters].
- To specific printers
  The values of the job ticket are used in a specific printer driver. The values of the job ticket are only used when you print to that printer.
  You can use the values of the job ticket differently in different printer drivers.

✏ NOTE

At least one printer must be installed.

You can use the job ticket settings for [All printers]. You can use the same job ticket settings for one or more specific printers. The job ticket settings for a specific printer driver overwrite the use of these settings for all printers.

Procedure

1. Select if you want to use the job ticket settings in:
   - [All printers]
   - A specific printer
     You must select a printer.

✏ NOTE

At least one printer must be installed.

2. Click button [Edit mappings].
   The [Edit mappings] dialog opens.
3. Select a [Job ticket item] in the left pane.
   The possible values for this [Job ticket item] are displayed in the center pane.
4. Select one of the 'Connected values' and enable the [Supported] option.
   The available printer settings are activated in the right pane.
5. Select the corresponding printer setting in the right pane.

6. Repeat above steps for each job ticket item that you want to use in the printer driver.
    For example:
    You can use a job ticket item like 'Document type' with value 'Internal report' for multiple printer settings in the printer driver. You can use this job ticket key 'Internal report' for the printer driver settings 'Duplex = On' and 'Staple = Off'. When a user specifies the 'Document' type as 'Internal report,' the document will be printed duplex and with a staple.

Use job tickets settings in document

Introduction

You can use the values of the job ticket items in document attributes. The document attributes are used when you page program the document.

The job ticket items that you can use are defined in the [Job Ticket Editor]. You can use job ticket items of type: [Text], [Choice], [Yes/No] and [Number].

NOTE
Job ticket item [Copies] is only visible when the document is printed.

NOTE
You can use the job ticket settings only if the document is not already page programmed.

Procedure

1. Click the [Edit mappings] button in the [Use job ticket settings in document] option.
   The [Use job ticket settings in document] dialog opens.
2. Select a [Job ticket item name] in the left pane.
   The possible values for this [Job ticket item] are displayed in the center pane.
3. Select one of the [Job ticket item values].
   The available [Document attributes] are activated in the right pane.
4. Select the corresponding document attribute in the right pane.

NOTE
You can map one job ticket item per document attribute.

5. Repeat above steps for each job ticket item that you want to use in the document attributes.

NOTE
You can use the job ticket settings only if the document is not already page programmed.

Backup and restore

Introduction

It is recommended that you create a backup after each installation and patch installation.

You can do a backup and restore of:
• The [Configurations] of the application.
• The jobs on the [Central server].

When you backup the [Configurations], you create a backup of:
• The job ticket definition.
• The used job tickets settings in the document attributes.
• The general configurations of the application.
  This includes the configuration of the [Central server] and the [Operator Console].
• The formula(s) that are defined in the formula manager.
• The products that are defined in the [Job Ticket Editor].
• The used printer tables.
• The invoice templates.
• The used job ticket settings for accounting attributes.

When you backup the [Job data], you create a backup of:
• The jobs on the [Central server].
• Job specific information.
  For example, accounting information of the jobs and custom job queues.

You must define the [Temporary data folder:] before you can backup the [Job data]. For example, your jobs are stored on a drive, which is nearly full. You can define the [Temporary data folder:] on an other drive. The [Job data] backup file is created in the [Temporary data folder:]. You can store the [Job data] backup file in an other folder.

The backup files for the [Configurations] and the [Job data] are password protected zip files.

✎ NOTE
You can only restore a backup file when:
• The computer name is the same.
• The installation paths are the same.
• The application version is the same as the application version that created the backup file.

Backup

Procedure

1. The [PRISMAaccess Administration] must be open. Close all other parts of the application on all workstations.
   Make sure you have defined the [Temporary data folder:]. This folder is used to create the temporary backup file.
2. Click the [Configurations]button.
   The 'Browse for Folder' dialog opens.
3. Browse to the folder where you want to create the [Configurations] backup file.
4. Click the [OK] button.
   The [Login information for SQL server] dialog opens.
   • To create the backup file with the credentials of a custom user:
     The custom user must have login rights and system administrator rights to the SQL server.

Select the [Use custom user] option. Define the credentials of the custom user for the JDF Framework. Click [Test connection] to test the credentials.

🖉 NOTE

If you click button [OK] while the custom user has insufficient rights to the SQL server, the backup file is not created.

- To create the backup file with the credentials of the logged in user:
  Deselect the [Use custom user] option.
  Click the [OK] button.

The [Configurations] backup file is created.

5. Click button [Job data].
   The 'Browse for Folder' dialog opens.
6. Browse to the folder where you want to store the [Job data] backup file.
7. Click the [OK] button.
   The [Login information for SQL server] dialog opens.
   - To create the backup file with the credentials of a custom user:
     The custom user must have login rights and system administrator rights to the SQL server.
     Select the [Use custom user] option. Define the credentials of the custom user for the JDF Framework and the [Print accounting] database. Click [Test connection] to test the credentials.

🖉 NOTE

If accounting is enabled, you can define the credentials for the [Print accounting] database.

🖉 NOTE

If you click button [OK] while the custom user has insufficient rights to the SQL server, the backup file is not created.

- To create the backup file with the credentials of the logged in user:
  Deselect the [Use custom user] option.
  Click the [OK] button.

The [Job data]backup file is created.

Restore

Procedure

1. The [PRISMAaccess Administration] must be open. Close all other parts of the application on all workstations.
2. Click the [Configurations]button.
3. Browse to the folder where the [Configurations] backup file is located.
4. Click the [Open] button.
   The [Login information for SQL server] dialog opens.
   - To restore the backup file with the credentials of a custom user:
     The custom user must have login rights and system administrator rights to the SQL server. Select the [Use custom user] option. Define the credentials of the custom user for the JDF Framework. Click [Test connection] to test the credentials.

   📝 NOTE
   If you click button [OK] while the custom user has insufficient rights to the SQL server, the backup file is not restored.

   - To restore the backup file with the credentials of the logged in user:
     Deselect the [Use custom user] option.
     Click the [OK] button.

   The [Configurations] of the application are restored.
5. Open the [Job Ticket Editor].
   Save the job ticket definition in the [Job Ticket Editor].
6. Click button [Job data].
7. Browse to the folder where the [Job data] backup file is located.
8. Click the [Open] button.
   The [Login information for SQL server] dialog opens.
   - To restore the backup file with the credentials of a custom user:
     The custom user must have login rights and system administrator rights to the SQL server. Select the [Use custom user] option. Define the credentials of the custom user for the JDF Framework and the [Print accounting] database. Click [Test connection] to test the credentials.

   📝 NOTE
   If accounting is enabled, you can define the credentials for the [Print accounting] database.

   📝 NOTE
   If you click button [OK] while the custom user has insufficient rights to the SQL server, the backup file is not restored.

   - To restore the backup file with the credentials of the logged in user:
     Deselect the [Use custom user] option.
     Click the [OK] button.

   The [Job data] of the application are restored.

   📝 NOTE
   You can only restore a backup file when:
   - The computer name is the same.
   - The installation paths are the same.
   - The application version is the same as the application version that created the backup file.

Corrupted jobs

Introduction

The [Operator Console] can contain jobs that remain with the internal state [Failed], [Editing], [Uploading], [Preparing], [Converting], [Preflighting], [Merging], [Printing], [Redistilling], [Exporting] or [Closing]. These jobs are corrupt.

Corrupt jobs cannot be deleted in the [Operator Console]. Corrupt jobs must be deleted in the [PRISMAaccess Administration].

Delete corrupted jobs

Procedure

1. Select a job from the list of corrupted jobs.
2. Click the [Delete] button.
   The corrupted job is deleted from the [Central server].
3. Click button [Refresh] to update the list of corrupted jobs.
   The list of corrupted jobs is not updated automatically.

Save corrupted jobs

Procedure

1. Select a job from the list of corrupted jobs.
2. Click the [Save] button.
3. Browse to a location. Click the [Save] button.
   The corrupted job and the job ticket are saved.

📝 NOTE

The saved job and job ticket can be sent to the help desk to analyze why the job became corrupted.

Refresh the list of corrupted jobs

Procedure

1. Click button [Refresh] to update the list of corrupted jobs.
   The list of corrupted jobs is not updated automatically.

[JDF service settings]

Introduction

In this dialog you can setup the JDF access points.

JDF access points can be used to transfer jobs to PRISMAdirect and receive status information back from PRISMAdirect.

The Job Definition Format (JDF) is a technical standard being developed by the CIP4 organization. The purpose of the standard is to facilitate interaction between different systems in a printing or print-related workflow. PRISMAaccess offers an interface based on the JDF standard which allows communication with external JDF-enabled software components.

The CIP4 JDF specification is a very extensive standard covering all areas in the life cycle of a print job, from preflight to image rendering to finishing and packaging. Océ has developed a proprietary standard for the JDF ticket which is a subset of the CIP4 description.

PRISMAaccess defines a proprietary job ticket with a set of ticket settings that can be configured and extended by the user. The user must be able to submit a job to PRISMAaccess via JMF messages by providing a JDF ticket and the required data files. A mapping file is used to construct a valid PRISMAaccess ticket with the values taken from the JDF ticket.

Click the [Edit] button to configure the JDF service settings.

Add or edit JDF access points

Procedure

1. Click the [Edit] button
   The [Configure JDF access point(s)] dialog opens.
2. Click the [Add] button to add a [JDF access point].
   Select a [JDF access point] and click [Edit] to edit an existing [JDF access point].
3. Define the [JDF access point] data.
   1. [Name:]
      This is the name you want to use to identify this [JDF access point].
   2. [Port:]
      This is the port number to be used by this [JDF access point].
      If you use a port number that is already in use you get an error message.
   3. [URL:]
      This is the URL used to access this [JDF access point].

   ✎ NOTE
   This field is automatically generated and cannot be changed.

4. Select the desired [Authentication] method and define the required data.
   1. [Windows authentication]:
      Select this option to use the [Windows authentication] method.
      The Windows user is actually the user under which the "Print JDF Service" is running.
      You can lookup the user of "Print JDF Service" in the Services dialogue of Microsoft Windows.
      This user must be an LDAP user and the LDAP server must exist in PRISMAaccess for the authentication of the access point to be successful.
   2. [Custom authentication]:

> If you want to use [Custom authentication] you need to specify the following credentials :
> [User name:] and [Password:].
> Here a valid PRISMAaccess user and its password must be provided.
> You can use the [Test connection] button to check the entered credentials.

5. If you want to use your own [Mapping files] you have to define the [Mapping files] section.
   Enable [Use custom mapping files].
   Use the browse button to browse to the mapping files that you want to use.
   Use [JDF ticket:] for the mapping of JDF to PRISMAdirect ticket items. A mapping file is used to construct a valid PRISMAaccess ticket with the values taken from the JDF ticket.
   Use [Job status:] for the mapping of the job status in PRISMAdirect to JDF.

📝 NOTE

The [Mapping files] are used every time the [JDF access point] is used.
Do not move, delete or rename these files.

6. Click [OK].
7. Click [OK] to return to the main screen.
   You receive a notification that the JDF service is restarted.

Delete a [JDF access point]

Procedure

1. Click the [Edit] button
2. Select the [JDF access point] that you want to delete.
3. Click the [Delete] button
   You will receive the warning [Do you want to delete the JDF access point?].
   Click [Yes].
4. Click [OK] to return to the main screen.
   You receive a notification that the JDF service is restarted.

Enable or disable JDF access points

Procedure

1. Click the [Edit] button
   The [Configure JDF access point(s)] dialog opens. The dialog offers an overview of all available JDF access points.
2. Use the check box in column [Enabled] to enable or disable the [JDF access point].
3. Click [OK] to return to the main screen.
   You receive a notification that the JDF service is restarted.

Pause or restart the JDF service

Procedure

1. Click the [Edit] button
   The [Configure JDF access point(s)] dialog opens.
2. Use the [Pause JDF service] check box to pause or restart the JDF service.
3. Click [OK] to return to the main screen.
   You will receive a notification that the JDF service has been restarted.

Chapter 3
Web server

Copyright

Trademarks

"Océ" and "PRISMA" are trademarks or registered trademarks of Océ.

Adobe®, Acrobat®, Reader® and Distiller® are registered trademarks of Adobe® Systems Incorporated.

Portions copyright © 2011 Enfocus BVBA; all rights reserved.

PostScript® 3™ is a registered trademark of Adobe® Systems Incorporated.

Microsoft®, Windows® , Windows NT®, Windows 98®, Windows 2000®, Windows XP®, Windows Server 2003® are either registered trademarks or trademarks of Microsoft® Corporation in the United States and/or other countries.

Xerox®, DigiPath®, DocuSP® and DocuTech® are registered trademarks of the Xerox® Corporation in the U.S. and/or other countries.

Fiery®, Command WorkStation® and EFI® are registered trademarks of Electronics for Imaging (EFI®), Inc.

SAP® Crystal Reports® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

Products in this publication are referred to by their general trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks of their respective companies.

Software version

This documentation describes the functionality of PRISMAdirect v1.2.

[Login]

[Login]

Introduction

Depending on the application configuration, it may be necessary to identify yourself. You have to enter your user name and password.

Procedure

1. Enter your user name.
2. Enter your password.
3. Click [Log in].

✏ NOTE
A [Web user] or [LDAP user] can login to the server when that user belongs to the [Services] group.

✏ NOTE
A system administrator can login to the server.

[General settings]

Define the General settings

Introduction

[You can configure the general settings in this dialog.]

Procedure

1. Click the [Edit] button.
   The [Edit general settings] dialog opens.
2. Define the [General settings]:

General details

Setting	Description

[Security]	You can select the following options:
	• [Use secure connections (HTTPS)]
	  Use this option to specify if you want to use the secure HTTPS connection for Web Submission.
	  If you select this option you have to use the 'Certificates' tab to configure the appropriate Certificates. A certificate guarantees a secure (HTTPS) connection to the Web Submission server.
	• [Use only HTTP connections to the Central server]
	  Enable this option if you want to use HTTP only connections to the central server.
	  For example, the firewall is allowed to open only one HTTP port.
	  Disable this option if you want to use HTTP and TCP connections to the central server. You must open the TCP port on the central server.
	• [Allow users to change their password]
	  Enable this option to allow users of [Web Submission] to change their password.
	• [Remember the user name and password]
	  Remember the user name and password of the Web Submission user.

[Trace level]	Define the trace level:
	• [Debug]
	  The [Debug] trace level provides the most detailed log information.
	• [Error]
	  The errors are logged.
	• [Info]
	  The errors and information messages are logged
	
	✎ NOTE
	The [Debug] trace level can impact the performance of the application.

Setting	Description

[Login page]	You can select the following options:
	• [Language:]
	  Select the language of the Web Submission logon page here.
	• [Web Submission login instructions:]
	  You can type in the user instructions that will be displayed on the Web Submission logon page. [These login instructions are visible in Web Submission when the user logs on via custom authentication.]

[Number of jobs per page:]	You can define how many jobs are displayed on one page in the [Web Submission].
[Desk submission users:]	You can add or remove Desk Submission users, see procedure [Edit desk submission users]. A Desk Submission user can create jobs on behalf of other users in the [Web Submission].
[Archive folder for Web Submission:]	Define the path of the import folder for the Web Submission. Syntax: \\FQDN\folder_name For example: \\PC1-PA\JobsToWebserver
[Preview resolution (in DPI):]	You can define the resolution of the preview of the job in the [Web Submission]. The higher the resolution, the higher the quality of the preview. ✎ NOTE A high DPI value can decrease the performance of the application.
[Pause web server]	You can pause the web server. When you pause the web server, the licence for the paused web server becomes available for another web server.
[Overview of warnings]	When you enable this option, the user can open the overview of warnings in the Web Submission. The order is checked for warnings before the order is submitted. The [Overview of warnings] dialog displays any detected warnings. It is recommended that the user solves any warning(s) before the user submits the order. Therefore, it is recommended that you enable the [Enable overview of warnings] option.

[Edit desk submission users]

Procedure

1. Click the [Edit] button.
   The [Edit general settings] dialog opens.
2. Click the [Change] button in the [Desk submission users:] area.
   The [Edit desk submission users] dialog opens.
3. Select the group of users.
4. Select a user.
5. Click the [Add] button.
   The user has Desk Submission rights.

[Contact information settings]

[Define contact information]

Introduction

[You can configure the contact information in this dialog.]

The [Contact information settings] are used for the [Support] link in [Web Submission].

[Contact information settings]

Contact information details

Setting	Description
[Name:]	The name of the contact person
[Telephone number:]	The telephone number of the contact person.
[Location:]	The location where the contact person can be found.
[Email address:]	The email address of the contact person.

[Automatic process settings]

[Automatic process settings]

Introduction

[You can configure the automatic process settings in this dialog.]

The automatic conversion service converts non-PDF files to PDF. The service uploads both the original files and the converted files.

The automatic merge service merges two or more PDF files into one PDF file. For example, two or more PDF files are automatically merged when you view a job with multiple PDF files.

This application contains default conversion applications.

✎ **NOTE**
A license is required to use the automatic conversion functionality.

Procedure

1. Click the [Edit] button.
   The [Define automatic conversion settings] dialog opens.
2. Define if you want to use the automatic conversion service.
   - Enable the [Enable automatic conversion] option:
     Automatic conversion is enabled.
     When a customer submits a non-PDF file in [Web Submission] the file is automatically converted to a PDF file. The [Operator Console] receives a job which contains the PDF file(s).
   - Disable the [Enable automatic conversion] option:
     Automatic conversion is disabled.
     When a customer submits a non-PDF file in [Web Submission], the [Operator Console] receives a job which contains the original non-PDF file.
     The operator must convert the file before the job can be printed.
3. [Select the conversion application:]
   Select a conversion application from the drop-down list.
   When you select the HotfolderConverter, you must define the [Input folder] and the [Output folder] for the converter.
   - [Input folder]: The converter receives the files for conversion via this input folder.
   - [Output folder]: The converter places the converted files in this output folder.

✎ **NOTE**
The selected conversion application must be installed on the web server.

4. [Select the merge application:]
   The automatic merge service merges two or more PDF files into one PDF file. For example, two or more PDF files are automatically merged when you view a job with multiple PDF files.
   Select a merge application from the drop-down list:
   - PDFNetMerge
     PDFNetMerge is the preferred merge application.
   - AcrobatMerge

✎ **NOTE**
Acrobat Professional must be installed on the [Web server] when you want to use AcrobatMerge.

Define the trace level

Procedure

1. Click the [Edit] button.
2. Define the trace level:
   - [Debug]
     The [Debug] trace level provides the most detailed log information.
   - [Error]
     The errors are logged.
   - [Info]
     The errors and information messages are logged

> 📝 NOTE
> The [Debug] trace level can impact the performance of the application.

[Certificates settings]

Introduction

Introduction

Web Submission allows you to create your own (self-signed) Certificates.

With option [&Remove certificate], you can remove self-signed Certificates.

✎ NOTE
The 'Installed Certificates' table lists all installed Certificates.

✎ NOTE
Select option [Show self-signed certificates only] to view company defined Certificates only.

Additional information

The Secure Socket Layer (SSL) protocol was created to ensure secure transactions between Web servers and Web browsers.

Data sent via an SSL connection is protected by encryption, a mechanism that prevents eavesdropping and tampering with any transmitted data. SSL provides that private data sent to a Web site, such as passwords, are kept confidential. Web server 'Certificates' are required to initialize an SSL session.

End users know that they have an SSL session with a website when their browser displays the little gold padlock and the address bar starts with 'https' rather than 'http'.

When connecting to the Web Submission website over SSL, the user's Web browser decides whether or not to trust the Web Submission website's SSL Certificate based on which Certification Authority has issued the actual SSL Certificate. To determine this, the browser looks at its list of trusted issuing authorities - represented by a collection of Trusted Root CA Certificates added into the browser by the browser vendor (such as Microsoft or Netscape).

Most SSL certificates are issued by CAs who own and use their own Trusted Root CA Certificates. These Trusted Root CA Certificates have already been added to all popular browsers, and are already trusted. These SSL certificates are known as 'single root' SSL certificates.

When you select option [Use secure connections (HTTPS)] in the [General settings] and assign a Certificate to the Web Submission Web site, end users will receive a 'Security Alert'. This shows the user more information about the Certificate that is used. The user can also view the Certificate details. When the user clicks 'Yes' the Certificate will be used and the secure connection will be established.

Related information

Create self-signed certificate

Introduction

You can create your own self-signed Certificate and use it for the secure transactions between the Web Submission users and the Web server.

✎ NOTE
Select option [Show self-signed certificates only] to view company defined Certificates only.

Procedure

1. Click button [Create certificate].
   The [Create self-signed certificate] dialog opens.
2. Define all [Certificate items].
3. Define the [Number of years that the certificate is valid:] option.
4. Click the [OK] button.
   The created Certificate will be added to the 'Installed Certificates' list.
   Self-signed certificates are automatically imported on the web server.

Remove certificate

Introduction

You can only remove self-signed Certificates here.

Procedure

1. Select the Certificate that you want to remove in the 'Installed Certificates' list.
2. Click 'Remove Certificate' on the 'Certificates' tab.
   A dialog will appear that asks you to confirm.
3. Click 'OK' to remove the selected Certificate.

> 🖉 NOTE
> You can only remove self-signed Certificates here.

[JDD service settings]

Introduction

The Job Data Dispatcher (JDD) service is used by the [Web Submission] to submit jobs to the [Central server].

In the [JDD service settings] dialog you can also handle failed jobs. A failed job is a job which is not successfully received on the Central server. You can handle only one failed job at a time. The failed jobs are displayed in a list.

You can resubmit a failed job.
1. If the job is received on the [Central server], the job is removed from the list.
2. If the job is not received on the [Central server], the job must be deleted manually.

Edit JDD service settings

Procedure

1. Click the [Edit] button.
    The [Edit JDD service settings] dialog opens.
2. Select a template to configure the JDD service.
    You can select one of the following templates:
    •   [Few submitters, small files]
    •   [Few submitters, large files]
    •   [Average number of submitters, medium files]
    •   [Many submitters, small files]
    •   [Many submitters, large files]

    Each template defines custom values which depend on the expected size and number of jobs submitted from the [Web Submission].

Define the trace level

Procedure

1. Click the [Edit] button.
2. Define the trace level:
   - [Debug]
     The [Debug] trace level provides the most detailed log information.
   - [Error]
     The errors are logged.
   - [Info]
     The errors and information messages are logged

📝 NOTE
The [Debug] trace level can impact the performance of the application.

Resubmit a failed job

Procedure

1. Select a failed job.
   You can select only one job at a time.
2. Click the button [Resubmit.]
   The job is submitted. If the job is received on the [Central server], the job is removed from the list.
3. Click the [Refresh] button to update the list of failed jobs.
   The list of failed jobs is not updated automatically.

Delete a failed job

Procedure

1. Select a failed job.
   You can select only one job at a time.
2. Click the [Delete] button.
   The selected job is deleted.
3. Click the [Refresh] button to update the list of failed jobs.
   The list of failed jobs is not updated automatically.

Backup and restore

Introduction

You can do a backup and restore of:
- The [&Configurations] of the application.

When you backup the [&Configurations], you create a backup of:
- The configuration of the local [Web server].
  If more than one [Web server] is installed, the backup procedure must be executed for each [Web server].

The backup file for the [&Configurations] is a password protected zip file.

> ✎ NOTE
> You can only restore a backup file when:
> - The computer name is the same.
> - The installation paths are the same.
> - The application version is the same as the application version that created the backup file.

Backup

Procedure

1. The System Administration must be open. Close all other parts of the application on all workstations.
2. Click the [Configurations]button.
   The 'Browse for Folder' dialog opens.
3. Browse to the folder where you want to create the [Configurations] backup file.
4. Click the [OK] button.
   The [Configurations] backup file is created.

Restore

Procedure

1. The System Administration must be open. Close all other parts of the application on all workstations.
2. Click the [Configurations]button.
3. Browse to the folder where the [Configurations] backup file is located.
4. Click the [Open] button.
   The [Configurations] of the application are restored.

✏ NOTE

You can only restore a backup file when:
- The computer name is the same.
- The installation paths are the same.
- The application version is the same as the application version that created the backup file.

LDAP servers

Introduction

The [LDAP servers] dialog displays the LDAP servers which are available to the application. The application searches for LDAP servers in the local network and domain during the start up of the application. All available LDAP servers are added to the list in the top of the dialogue.

The LDAP servers can be added to two different lists:
- [Servers used for authentication:]
  The first LDAP server in the list is used for the authentication of a user. If the user cannot be authenticated by the first server, then the second server is used, etc.
  Click the 'Up' and 'Down' buttons to set the correct order of the LDAP servers used for authentication.
  User data can be collected from each server in this list.
- [Servers used to retrieve user data:]
  The servers in this list are only used to retrieve user data that is available on an LDAP server. The retrieved user data is filled in automatically in the mapped profile attributes and the mapped job ticket items.

Click [Add] or [Edit] to open the [Edit LDAP server settings] dialog.

Click [Delete] to delete an LDAP server.

✎ NOTE
You can delete the LDAP servers that you do not use for the application. However, the application searches for LDAP servers at start up of the application. The found LDAP servers are added to the list in the top of the dialogue.

Click [Search] to search for any available LDAP servers in the local network and domain.

LDAP servers for the central server and the web server

If the central server and the web server are installed on the same machine, the [LDAP servers] dialogue is available in:
- The [Global settings] for both the central server and the web server.
  The servers in the list of [Servers used for authentication:] are used to authenticate:
  - The [Web Submission] users.
  - The users of the application. For example, the operators.

If the central server and the web server(s) are installed on separate machines in a distributed system, the [LDAP servers] dialogue is available in:
- The [Global settings] for the central server.
  The servers in the list of [Servers used for authentication:] are used to authenticate the users of the application. For example, the operators.
  In dialogue [Global settings], you define which LDAP servers are used for authentication and to retrieve user data for the central server. On all machines where dialogue [Global settings] is installed, the list of LDAP servers for the central server is the same.
- The [Web server] for the web server(s).
  The servers in the list of [Servers used for authentication:] are used to authenticate the [Web Submission] users.

✎ NOTE
If the [Web Submission] users cannot be authenticated, the application uses the LDAP servers in [Global settings] to authenticate the users.
For each web server, you can define which LDAP servers are used for authentication and to retrieve user data. The used LDAP servers can be different for each web server.

Refresh the LDAP information

Click [Refresh] to refresh the generic info about the LDAP, users and groups part of that LDAP.

PRISMAdirect stores some information about each LDAP locally. The information regards generic info about the LDAP, users and groups part of that LDAP. In order for it to be in sync with the real information, a service synchronizes this information automatically once a day, at midnight. If you want to synchronize this information manually, you have to use the [Refresh] functionality which starts an update of the information stored for all the LDAP servers.

The connection status of each LDAP server is displayed in column [Status].
- Green dot:
  The connection to the LDAP server is established.
- Orange dot:
  The connection to the LDAP server is not checked or the connection is being checked.

NOTE

After a reboot of the system, the dots are orange. Click [Test connection] to update the state of each LDAP server.

- Red dot:
  The connection to the LDAP server cannot be established. Check the settings of the LDAP server.

Add or edit an LDAP server

Procedure

1. Click [Add] or [Edit] to open the [Edit LDAP server settings] dialog.
   When you add a new LDAP server you have to configure the LDAP server settings.
2. You can configure the LDAP server(s) in this dialogue.

Setting	Description
[Domain name for LDAP server:]	You can define a custom name for the LDAP server. The custom name must be unique. ✎ NOTE An LDAP server can be used for Windows authentication of users.
[Credentials policy:]	The credentials policy defines which credentials are used by the JDF Framework service to connect to the LDAP server. ✎ NOTE [Use common credentials] is the default value for the drop-down list. This value can always be used for each LDAP server. You can select one of the following credential policies: • [Use common credentials] These are the credentials that are stored in the global settings of the LDAP server. These credentials are used for each connected LDAP server. These credentials are not defined in the application by the user. [Use common credentials] is the default value for the drop-down list. This value can always be used for each LDAP server. • [Use the credentials which are stored on the LDAP server] These are the credentials that you define in [LDAP server user name:] and [LDAP user password:]. • [Use the credentials of the Windows user who runs the JDF Framework service] You can select this credential policy only for Secure-based authentication types. This credential policy supports Integrated Windows Authentication (IWA) only. These credentials are defined by the user during the installation of the application. The Windows user can be DocWorker, a local user, or a selected domain user. You can identify the Windows user who runs the JDF Framework in the Services dialogue of Microsoft Windows: .\JdfFramework: local user .\DocWorker: DocWorker Secure authentication type ▶

Setting	Description
[LDAP server user name:]	You must supply a user name and password to retrieve information from the LDAP server. ✎ NOTE This option is available when you have selected [Credentials policy:] [Use the credentials which are stored on the LDAP server].
[LDAP user password:]	You must supply a user name and password to retrieve information from the LDAP server. ✎ NOTE This option is available when you have selected [Credentials policy:] [Use the credentials which are stored on the LDAP server].
[Server address:]	You must define the address of the LDAP server. If you define only the address of the LDAP server, the users are searched through the entire LDAP server. You can also define the server address and the search root. When you define the server address and the search root, the search for users starts at the defined root on the server. For example: LDAP://sro.company.net:389/DC=sro,DC=company,DC=net, where: • sro.company.net The address of the domain controller. • 389 The port which is used to connect to the LDAP server. • DC=sro,DC=company,DC=net The path to search for users in the active directory tree on the LDAP server. ✎ NOTE The default port number for a non-secure connection is 389. The default port number for a secure connection is 636.
[Server type:]	Select a server type. The server types which start with "Native…" are preferred. The other server types are available for backwards compatibility.
[Use secure connection (SSL)]	Select this option if you want to create a secure connection to the LDAP server. To be able to select this option, the LDAP server has to support this. ✎ NOTE The default port number for a non-secure connection is 389. The default port number for a secure connection is 636. ✎ NOTE Please make sure that you update the port number if you want to use a secure connection.

Setting	Description
[User filter:]	A default user filter is created automatically for new LDAP servers. You must define: 1. [Domain name for LDAP server:] 2. [Credentials policy:] 3. [Server address:] 4. [Server type:] 5. Click the [OK] button. 6. Select the new LDAP server. Click the [Edit] button. The default filter is now available in the [Edit LDAP server settings] dialog. You can edit the filter. The minimum filter is the LDAP attribute for user name, for example: (sAMAccountName=%u). The user filter must contain "%u" as placeholder for the user name. The minimum filter will always work, but it is not time efficient. Only users that pass the filter can be imported from the LDAP server. ✎ NOTE The filter must be updated when the [LDAP attribute for user name:] is changed.
[LDAP attribute for user name:]	You can define the LDAP attribute that contains the user name. ✎ NOTE The default LDAP attribute is used for the user name if this field is left empty. The default LDAP attribute depends on the server type.
[User group filter:]	A default user group filter is created automatically for new LDAP servers. You must define: 1. [Domain name for LDAP server:] 2. [Credentials policy:] 3. [Server address:] 4. [Server type:] 5. Click the [OK] button. 6. Select the new LDAP server. Click the [Edit] button. The default filter is now available in the [Edit LDAP server settings] dialog. You can edit the filter. The minimum filter is the LDAP attribute for group name, for example: (cn=%g). The user group filter must contain "%g" as placeholder for the user group name. The minimum filter will always work, but it is not time efficient. Only user groups that pass the filter can be imported from the LDAP server. ✎ NOTE The filter must be updated when the [LDAP attribute for group name:] is changed.

▶

Setting	Description
[LDAP attribute for group name:]	You can define the LDAP attribute that contains the group name. ✎ NOTE The default LDAP attribute is used for the group name if this field is left empty. The default LDAP attribute depends on the server type.

Advanced settings

Authentication types

You can select an authentication type for the [Authentication used to connect to LDAP server:] option and the [Authentication used to connect user to the LDAP server:] option. The authentication types are described in the tables below.

✎ NOTE
In LDAP "authentication" is called "bind".

Authentication type	Description
None	None means a simple bind to the server using plain text credentials. A simple bind is the only binding mechanism defined in the LDAP specification itself. None has a high compatibility across LDAP server vendors. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: All server types, but this authentication type is not recommended.
NoneAndServerBind	This is the None authentication type combined with the ServerBind optimisation. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: ActiveDirectory, but this authentication type is not recommended.
NoneAndFastServerBind	This is the None authentication type combined with ServerBind and FastBind optimizations. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: ActiveDirectory, but this authentication type is not recommended.
Anonymous	Anonymous means that no authentication is done. Most LDAP servers do not allow anonymous access by default, or give a very restrictive access to the server. Possible usage: All server types, but this authentication type is not recommended.
AnonymousAndServerBind	This is the Anonymous authentication type combined with the ServerBind optimisation. Possible usage: ActiveDirectory, but this authentication type is not recommended.

Authentication type	Description
AnonymousAndFastServerBind	This is the Anonymous authentication type combined with ServerBind and FastBind optimizations. Possible usage: ActiveDirectory, but this authentication type is not recommended.
Secure	Secure is the Windows authentication method, which relies on the Windows Security Support Provider Interface (SSPI). The SSPI usually selects the Windows Negotiate protocol with Kerberos or NTLM authentication. Secure supports both explicit credentials and Integrated Windows Authentication (IWA). WARNING: ActiveDirectoryFastDelegationSecureBinding is preferred for better security over Secure. Possible usage: ActiveDirectory, NativeADS, NativeLDAP with a Windows-based LDAP Server.
FastSecureBinding	This is the Secure authentication type combined with the FastBind optimisation. WARNING: ActiveDirectoryFastDelegationSecureBinding is preferred for better security over FastSecureBinding. Possible usage: ActiveDirectory, NativeADS.
SecureSocketLayer	SecureSocketLayer means that a TLS/SSL communication channel is used to encrypt all the network traffic. The encryption includes the bind and exchange of credentials. This is the recommended setting for most LDAP servers, when security must be guaranteed without using the Windows authentication and security mechanisms. However, the setup is complex because SecureSocketLayer requires that the server has a valid server certificate installed. And the client must trust the Certificate Authority (CA) which issued the server certificate. The analysis of SecureSocketLayer problems can be complex: • For ADSI-based connectors: Any SecureSocketLayer-related problems are reported in the Windows System Event log. If the server certificate is invalid, the SecureSocketLayer connection will fail. • For non-ADSI-based connectors: Any SecureSocketLayer-related problems are reported in the dialogue that appears after you click button [Test connection]. If the server certificate is invalid, a warning is reported but the SecureSocketLayer connection will succeed. Possible usage: SunDirectoryServer, NativeLDAP, NativeADS. This authentication type is recommended.

Authentication type	Description
FastSecureSocketLayer	This is the SecureSocketLayer authentication type combined with the FastBind optimisation for ADSI-based connectors, or FastConcurrentBinding optimisation for non-ADSI connectors. Possible usage: SunDirectoryServer, NativeLDAP, NativeADS. This authentication type is recommended.
ActiveDirectoryFastSecureBinding	This is the Secure authentication type combined with the Sealing, Signing and FastBind optimization. The users are authenticated against ActiveDirectory servers. Possible usage: ActiveDirectory, NativeADS.
ActiveDirectoryFastDelegationSecureBinding	This is the Secure authentication type combined with the Sealing, Signing, Delegation, and FastBind optimization. The users are authenticated against ActiveDirectory servers. Possible usage: ActiveDirectory, NativeADS. This authentication type is recommended for ActiveDirectory.
Basic	Basic means a simple bind to the server using plain text credentials. This authentication type is very similar to None. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: All server types, but this authentication type is not recommended.
BasicWithFastConcurrentBinding	This is the Basic authentication type combined with the FastConcurrentBinding optimisation. WARNING: this authentication is NOT SECURE because plain text credentials are used. Possible usage: All server types, but this authentication type is not recommended.
BasicWithFastConcurrentBindingAndSSL	This is the Basic authentication type combined with the FastConcurrentBinding optimization and a SecureSocketLayer communication channel. Possible usage: NativeLDAP. This authentication type is recommended.
Negotiate	This is the Windows Negotiate authentication, which means the same as Secure authentication. Negotiate results in Kerberos or NTML authentication. Possible usage: ADAM and NativeLDAP connectors against a Windows-based LDAP server.
Kerberos	The Kerberos authentication is almost the same as Secure authentication. Kerberos results in Kerberos authentication. WARNING: Negotiate is preferred over Kerberos. Possible usage: ADAM and NativeLDAP connectors against a Windows-based LDAP server.

Authentication type	Description
NTML	The NTML authentication is almost the same as Secure authentication. NTML results in NTML authentication. WARNING: Negotiate is preferred over NTML. Possible usage: ADAM and NativeLDAP connectors against a Windows-based LDAP server.
Digest	This is the Windows Digest Access authentication. Possible usage: ADAM and NativeLDAP connectors against a Windows-based LDAP server.

Authentication optimisations and options

Authentication optimisations and options	Description
ServerBind	With optimization ServerBind, only the server which is specified in the connection URL is addressed. It is usually safe to use ServerBind for most LDAP servers and for ActiveDirectory when the specific domain controller is addressed. Failover servers for ActiveDirectory are not addressed.
FastBind	With FastBind optimization, the objectClass attribute on the server is not used. This increases the performance. Optimization FastBind is only valid for ADSI-based connectors, such as ActiveDirectory or NativeADS.
FastConcurrentBinding	With optimization FastConcurrentBinding no security token is created. This increases the performance when only user authentication is needed. Optimization FastConcurrentBinding is only valid for non-ADSI based connectors, such as ADAM, NativeLDAP, SunDirectoryServer.
SecureSocketLayer	With option SecureSocketLayer, a TLS/SSL communication channel is created to encrypt all network traffic.
Sealing	Optimization Sealing activates additional encryption capabilities of SSPI.
Signing	Optimization Signing activates additional data integrity checking capabilities of SSPI.
Delegation	Optimization Delegation activates the ability of using the Windows security context across domains.

Procedure

1. Click button 'Advanced' and define:
2. [Authentication used to connect to LDAP server:]
   You can define the type of authentication which the application uses to connect to the LDAP server.
3. [Authentication used to connect user to the LDAP server:]
   You can define the type of authentication which the application uses to authenticate a user on the LDAP server.
4. Allow automatic creation of users:

Every user who logs on to the application with an [LDAP server user name:] and an [LDAP user password:] is created automatically.

The [User type] of an automatically created user becomes:

- [Windows user] if the user is authenticated via Windows authentication.
- [LDAP user] if the user is authenticated via Forms authentication.

An automatically created user belongs to the [Group] of 'Submitters'.

The users in the 'Submitters' group can access the [Web Submission].

Test the connection

Procedure

1. Click [Test connection] to test the connection to the selected LDAP server. The connection status of each LDAP server is displayed in column [Status].
    The following data is required for the test:
    • [LDAP server user name:]
    • [LDAP user password:]
    • [Server address:]
    • [Use secure connection (SSL)]

    The following checks are done :
    • Connect + bind to the server using the 4 settings you have specified;
    • Read of RootDSE;
    • Probe for a user entry to enumerate user attributes;
    • Probe for a group entry to enumerate group attributes.

Use LDAP server for authentication

Introduction

The [LDAP servers] dialog displays the LDAP servers which are available to the application. The application searches for LDAP servers in the local network and domain during the start up of the application. All available LDAP servers are added to the list in the top of the dialogue.

The LDAP servers can be added to two different lists:

- [Servers used for authentication:]
  The first LDAP server in the list is used for the authentication of a user. If the user cannot be authenticated by the first server, then the second server is used, etc.
  Click the 'Up' and 'Down' buttons to set the correct order of the LDAP servers used for authentication.
  User data can be collected from each server in this list.
- [Servers used to retrieve user data:]
  The servers in this list are only used to retrieve user data that is available on an LDAP server. The retrieved user data is filled in automatically in the mapped profile attributes and the mapped job ticket items.

Procedure

1. Select an LDAP server from the list of available LDAP servers.
2. Click the [Use for authentication] button.
   The LDAP server is added to the list [Servers used for authentication:].
3. Click [Test connection] to test the connection to the selected LDAP server.

Use LDAP server to retrieve user data

Procedure

1. Select an LDAP server from the list of available LDAP servers.
2. Click the [Use to retrieve user data] button.
   The LDAP server is added to the list [Servers used to retrieve user data:].
3. Click [Test connection] to test the connection to the selected LDAP server.

Map LDAP attributes to job ticket items

Introduction

You can map information that is available within the LDAP server to job ticket items. The job ticket items then automatically receive the data from the LDAP attribute.

Add a mapping

Procedure

1. Enable the [Collect user data from this LDAP server] option.
2. Click the [Set &ticket mapping] button.
   The [Map LDAP attributes to job ticket items] dialog opens.
3. Click the [Add] button.
4. Select a job ticket item from the list.
5. Define the LDAP attribute that contains the information that you want to use for the job ticket item.
6. Click the [Add] button.
   The defined LDAP attribute is mapped to the job ticket item.

Edit a mapping

Procedure

1. Click the [Set &ticket mapping] button.
   The [Map LDAP attributes to job ticket items] dialog opens.
2. Select a mapped LDAP attribute in the list.
3. Click the [Edit] button.
4. Define the LDAP attribute that contains the information that you want to use for the job ticket item.

   NOTE
   The [Job ticket item] cannot be changed.

5. Click the [OK] button.
   The defined LDAP attribute is mapped to the job ticket item.

Remove a mapping

Procedure

1. Select a mapped LDAP attribute in the list.
2. Click the [Remove] button to remove an existing mapping.

Edit profile mappings

Introduction

You can map information that is available within the LDAP server to the [Profile settings] of the [Web Submission] users. The [Profile settings] of the [Web Submission] users then automatically receive the data from the LDAP server.
- If the LDAP attribute contains a value, the associated profile attribute is filled in. The Web Submission user cannot change the profile attribute.
- If the LDAP attribute does not contain a value, the associated profile attribute is left empty. The Web Submission user must define the value of the profile attribute.
- If you deselect a profile attribute, the user can change the value of the profile attribute.

> **NOTE**
> The LDAP attributes may not be present in all the LDAP servers or might not contain relevant information.

Procedure

1. Enable the [Collect user data from this LDAP server] option.
2. Click the [Set &profile mapping] button.
   The [Edit profile mappings] dialog opens.
3. Map the LDAP attributes to the profile attributes.
   Below you see the default LDAP attributes provided by PRISMAdirect. You can change these in order to retrieve other relevant information from the LDAP server.

Profile attributes	LDAP attributes
[First name:]	givenName
[Last name:]	sn
[Department:]	department
[Location:]	roomNumber
[Company:]	company
[Telephone number:]	telephoneNumber
[Email address:]	mail
[Account:]	departmentNumber

File hosting and payment settings

Manage the file hosting and payment settings

Introduction

The file hosting providers provide an Internet hosting service specifically designed to host user files. When you select one or more file hosting providers, the users can add files from the hosting service - the "cloud" - to their job. You must enable the file hosting providers in PRISMAdirect. Enable the [Use file hosting providers] option in the dialog [Manage file hosting settings] of section [Global settings] in the System Administration. However, you can disable the file hosting providers in this dialog if your Web server has no Internet access. For example, your company uses a local area network.

✎ NOTE
You must configure the settings for the file hosting providers in this dialog.

The payment providers offer a payment service for your users. When you select one or more payment providers, each user can pay for their orders directly. You must enable the payment service in PRISMAdirect. Enable the [Use payment providers] option in the dialogue [Default cost settings] of section [Global settings] in the System Administration. However, you can disable the payment service in this dialog when your Web server has no Internet access. For example, your company uses a local area network.

✎ NOTE
You must configure the settings for the payment providers in this dialog.

[File hosting settings]

Setting	Description
[File hosting settings]	The [Use file hosting providers] option is enabled by default. • Enabled: The user can select files from file hosting providers. You can select which file hosting providers are available for the user. For example: Dropbox. • Disabled: The user cannot select files from file hosting providers. You can disable the file hosting providers in this dialog if your Web server has no Internet access. For example, your company uses a local area network. The user does not receive an unable to connect message from the file hosting provider.
[Cache settings]	You can store the data of the file hosting providers within a cache. If requested data is contained in the cache, the request can be served by simply reading the cache, which is comparatively faster. Otherwise, the data has to be fetched from its original storage location, which is comparatively slower. You must define the [cache size] and the [cache folder]. ✎ NOTE The JDD service user must have the permission "Full Control" over the cache folder.

Setting	Description
[File hosting providers]	Click [Edit] to configure the file hosting provider. For example, you can define the [Consumer Key] and the [Consumer Secret] when you use the Dropbox API. ✎ **NOTE** You can select the file hosting providers for PRISMAdirect in the dialog [Manage file hosting settings] of section [Global settings] in the System Administration.

[Payment settings]

Setting	Description
[Payment settings]	The [Use payment providers] option is enabled by default. • Enabled: The users can pay for their orders directly. You can enable one or more payment providers. For example: PayPal. • Disabled: The users cannot pay for their orders directly. You can disable the payment providers in this dialog when your Web server has no Internet access. For example, your company uses a local area network. The user does not receive an unable to connect message from the payment provider.
[Payment providers]	Click [Edit] to configure the payment provider. For example, you can define the setting [API username], et cetera when you use the PayPal API. PayPal delivers these settings to you when you create a merchant account in PayPal. ✎ **NOTE** You can select the payment providers for PRISMAdirect in the dialog [Default cost settings] of section [Global settings] in the System Administration.

[JDD service settings]

It is recommended that you change the users only when:
1. You want to use the file hosting providers and/or the payment providers. The users must have Internet access if you want to use the file hosting providers and/or the payment providers.
2. The users have a local system account.

A number of services will be restarted when the users in this dialog are changed. Jobs that are being submitted by Web Submission users will become corrupt. The following services and processed are restarted:
• The Message Queuing service
• The Print Job Data Dispatcher service
• The PrintroomAppPool process

When you disable the file hosting providers and the payment providers, the users can have a local system account. You can disable the providers when your Web server has no Internet access. For example, your company uses a local area network.

Setting	Description
[JDD service user:]	The read-only text box displays the current JDD service user. Click [Test connection] to test if the defined user has Internet access.
['PrintroomAppPool' application pool user:]	The read-only text box displays the current 'PrintroomAppPool' application pool user. Click [Test connection] to test if the defined user has Internet access.
Change the users	1. Click the [Change] button. The [Change JDD service user] dialog opens. 2. Select the domain and user name. Type the password. Letters in passwords must be typed using the correct case. The user must have Internet access if you want to use the file hosting providers and/or the payment providers. 3. Click the [OK] button. The JDD service user and the 'PrintroomAppPool' application pool user are changed.

Chapter 4
Generic application

Copyright

Trademarks

"Océ" and "PRISMA" are trademarks or registered trademarks of Océ.

Adobe®, Acrobat®, Reader® and Distiller® are registered trademarks of Adobe® Systems Incorporated.

Portions copyright © 2011 Enfocus BVBA; all rights reserved.

PostScript® 3™ is a registered trademark of Adobe® Systems Incorporated.

Microsoft®, Windows® , Windows NT®, Windows 98®, Windows 2000®, Windows XP®, Windows Server 2003® are either registered trademarks or trademarks of Microsoft® Corporation in the United States and/or other countries.

Xerox®, DigiPath®, DocuSP® and DocuTech® are registered trademarks of the Xerox® Corporation in the U.S. and/or other countries.

Fiery®, Command WorkStation® and EFI® are registered trademarks of Electronics for Imaging (EFI®), Inc.

SAP® Crystal Reports® is the trademark or registered trademark of SAP SE in Germany and in several other countries.

Products in this publication are referred to by their general trade names. In most, if not all cases, these designations are claimed as trademarks or registered trademarks of their respective companies.

Software version

This documentation describes the functionality of PRISMAdirect v1.2.

Introduction

In a distributed system, the [Generic component] is installed on all components of PRISMAdirect.

Operator Console settings

Define the [Operator Console settings]

Introduction

You can define the [Operator Console settings] here.

Procedure

1. Click the [Edit] button.
   The [Edit Operator Console settings] dialog opens.
2. Define the [Preview resolution (in DPI):]
   You can define the resolution of the preview of the job in the [Operator Console].
   The higher the resolution, the higher the quality of the preview.

   📝 NOTE
   A high DPI value can decrease the performance of the application.

3. Enable or disable the [Overview of warnings] dialog.
   The selected jobs are checked for warnings before being printed. A warning is reported when a setting in the job ticket differs from the corresponding setting in the document. The [Overview of warnings] dialog displays the detected warnings. It is recommended that you resolve the warnings before you print the selected jobs. You can [Cancel] the print operation and solve the warnings. You can click the [Print] button to ignore the warnings and print the jobs.
4. Define the [Trace level]:
   • [Debug]
     The [Debug] trace level provides the most detailed log information.
   • [Error]
     The errors are logged.
   • [Info]
     The errors and information messages are logged

   📝 NOTE
   The [Debug] trace level can impact the performance of the application.

General Settings

Define the general settings

Introduction

This application installs services in the Services dialog of Microsoft Windows. You must define the login information for the installed services.

Procedure

1. Click the [Edit] button.
    The [Edit general settings] dialog opens.
2. Define the [Central server name].
    The Central server stores all submitted jobs.
    You can define the server address in Fully Qualified Domain Name (FQDN). For example, <servername>.company.nl.

    ✎ NOTE
    The application restarts when you change the server address.

3. Select the authentication type.
    The selected authentication type is used for the:
    *   [Operator Console]
    *   [Web Submission]
    *   [Job Ticket Editor]

    The installed services and the System Administration always use [Custom authentication].
4. [Logon credentials for installed components:]
    Consider a distributed system. Several components of the application authenticate themselves to the [Central server] with this account. These components are: [PRISMAaccess Administration], [Operator Console], [Job Ticket Editor]).

    ✎ NOTE
    These components must use these logon credentials. You must define these logon credentials for each component when you install the component.

    *   Define a [User name].
    *   Define a [Password:]

    This user must belong to the [Services] group.

    ✎ NOTE
    The application restarts when you change the username or password.

5. You can define a folder for the temporary files which are created by the application.

Clean-up Settings

Define the Clean-up settings

Introduction

The application creates temporary files. The temporary files left behind by the application accumulate over time and can take up a lot of disk space. These temporary files can be cleaned-up by the Print Cleanup Service.

Procedure

1. Click the [Edit] button.
   The [Edit clean-up service settings] dialog opens.
2. Define the [Number of hours between two clean-up operations:].

📝 NOTE
If the "Number of hours between two clean-up operation" is 0, then the clean-up service cleans up one more time and only then it's deactivated.

3. Click the [OK] button.

Define the trace level

Procedure

1. Click the [Edit] button.
2. Define the trace level:
   - [Debug]
     The [Debug] trace level provides the most detailed log information.
   - [Error]
     The errors are logged.
   - [Info]
     The errors and information messages are logged

📝 NOTE
The [Debug] trace level can impact the performance of the application.

License Settings

Define the license server settings

Procedure

1. Click the [Edit] button.
   The [Define license server settings] dialog opens.
2. Define the [License server name:].
   Define the name or IP address of the license server.
   You can define the license server name in Fully Qualified Domain Name (FQDN). For example,
   <servername>.company.nl.
3. Define the [Port:].
   Define which port of the license server is used.

Index

Canon

Canon Inc.
www.canon.com

Canon U.S.A., Inc.
www.usa.canon.com

Canon Canada Inc.
www.canon.ca

Canon Europa Inc.
www.canon-europe.com

Canon Latin America Inc.
www.cla.canon.com

Canon Australia PTY. Ltd
www.canon.com.au

Canon China Co., Ltd
www.canon.com.cn

Canon Singapore PTE. Ltd
www.canon.com.sg

Canon Hongkong Co., Ltd
www.canon.com.hk