Administration
# Table of Contents

## I. Admin Center

1. ACCESS .......................................................................................................................... 1
   - Starting the Admin Center application ................................................................. 1
2. General Settings .............................................................................................................. 2
   - Home page ............................................................................................................. 3
   - Client ................................................................................................................... 4
   - Application ......................................................................................................... 5
   - VPPortal ............................................................................................................... 6
3. Password Configuration ................................................................................................. 6
4. SAML2 ............................................................................................................................ 7
   - Enable for Visual Planning .................................................................................. 8
   - Enable for VPPortal ............................................................................................ 8
   - SP ........................................................................................................................ 8
   - IdP ........................................................................................................................ 8
5. LDAP .............................................................................................................................. 8
   - Configuration ...................................................................................................... 8
   - Import users ....................................................................................................... 10
6. External access configuration ....................................................................................... 11
7. Database Request ......................................................................................................... 11
8. File storage and document browser ........................................................................... 12
9. Show server statistics ................................................................................................. 12
10. Show server logs ...................................................................................................... 13
11. Add ............................................................................................................................ 14
12. Export ....................................................................................................................... 14
13. Import ......................................................................................................................... 15

## II. License management

1. License types .................................................................................................................. 16
   - Named licenses .................................................................................................. 16
   - Floating licenses ............................................................................................... 16
2. License characteristics .................................................................................................. 16
3. Creating a license ......................................................................................................... 17
4. Changing a license ....................................................................................................... 18
   - Adding a description to a license ...................................................................... 19
   - Assigning users to a license .............................................................................. 19
5. Updating a license ........................................................................................................ 20
6. Deleting a license ........................................................................................................ 20

## III. Services management

1. DEFINITION .................................................................................................................. 22
2. CHARACTERISTICS OF SERVICES ............................................................................ 22
   - Viewing of services ............................................................................................ 22
   - Starting the service ............................................................................................ 22
   - Stopping the service ......................................................................................... 23
3. E-MAIL SENDING SERVICE ................................................................. 23
   Name .................................................................................................. 24
   Description ....................................................................................... 24
   Automatic start ................................................................................ 24
4. IMPORT/EXPORT SERVICE ................................................................. 24
   Name .................................................................................................. 25
   Description ....................................................................................... 25
   Automatic start ................................................................................ 25
5. AUTOMATIC BACKUP SERVICE ....................................................... 25
   Name .................................................................................................. 26
   Description ....................................................................................... 26
   Automatic start ................................................................................ 26
   Backup directory ............................................................................ 26
   Start time ......................................................................................... 26
   Number of days archived .................................................................. 27
   Sending mail .................................................................................... 27
   Sender ............................................................................................... 27
   Recipients ......................................................................................... 27

IV. Module Management ......................................................................... 28
   1. DEFINITION .................................................................................... 28
   2. ADMINISTRATION .......................................................................... 28
      Viewing the modules ...................................................................... 28
      Installing a module ....................................................................... 29
      Defining a module's administrators ............................................. 30

V. User Management ............................................................................. 32
   1. DEFINITION .................................................................................... 32
   2. ADMINISTRATION .......................................................................... 32
      Viewing of users ........................................................................... 32
      Creating a user .............................................................................. 33
      Modifying a user .......................................................................... 36
      Deleting a user ............................................................................. 37
      Send e-mail .................................................................................. 37
      Import users .................................................................................. 37

VI. Group management .......................................................................... 39
   1. Group management actors .......................................................... 39
   2. Group characteristics .................................................................... 39
   3. Creating a group ............................................................................ 40
      Name ............................................................................................... 41
      Description ..................................................................................... 41
      Assignment .................................................................................... 42
   4. Changing a group .......................................................................... 42
   5. Deleting a group ............................................................................ 42
   6. Send e-mail .................................................................................. 42
VII. Planner management

1. DEFINITION

8. Management of VP ONE planners

1. DEFINITION

2. ADMINISTRATION

Viewing planners
Creating a planner
Importing a planner
Planner Export
Deleting a planner

IX. Management of VP ENTERPRISE planners

1. DEFINITION

2. ADMINISTRATION

Viewing planners
Creating a planner
Modifying a planner
Deleting a planner
Restore a planner
Planner Export
Display export URL
Configuration
Log out users
Logged in users
Login history
Send e-mail

X. Permission management

1. DEFINITION

2. ADMINISTRATION

Viewing planner permissions
Assigning a user group to a planner
Creating a permission
Changing a permission
Duplicating a permission
Deleting a permission
Enabling permissions

3. TYPES OF PERMISSIONS

Read-only Permissions
Administration Permissions
Permissions on dimensions
Permissions on the valuation items
Permissions on the workflows
Permissions on event exports
Permissions on the predefined views
Permissions on event editors ................................................................. 101
Permissions on workloads ........................................................................ 103
Permissions on resource filters ............................................................... 109
Permissions on the dimensions’ resources ............................................... 116
Permissions on events ............................................................................. 124

XI. Display of the log ......................................................................................... 133
1. DEFINITION .............................................................................................. 133
2. USE ........................................................................................................ 133
   Display of the Client Log ......................................................................... 133
   Display of the Admin Center Client Log ................................................. 134
   Display of the Server Log ...................................................................... 135

XII. File storage ............................................................................................... 138
1. DEFINITION .............................................................................................. 138
2. CONFIGURATION ...................................................................................... 138
   VISUAL PLANNING Server .................................................................. 138
   DROPBOX .............................................................................................. 139
   GOOGLE DRIVE ...................................................................................... 142
Chapter I. Admin Center

ADMIN CENTER is a VISUAL PLANNING administration management application.

It only functions in the network version with VISUAL PLANNING ENTERPRISE.

This application is used to manage:

- licenses,
- users,
- groups,
- planners and their permissions (ENTERPRISE version only),
- services (ENTERPRISE version only),
- modules (ENTERPRISE version only).

Only a general administrator or planner administrator can access this functionality.

1. ACCESS

Starting the Admin Center application

To start ADMIN CENTER, open the Intranet/Internet browser

Then type in the address, which has the following structure: http://nomduserveur/vplanning/

When the page opens, click on ADMIN CENTER.

The login window opens:

To log in, type:
■ the login,
■ the password,
■ then click on the Validate button.

Admin Center opens.

2. General Settings

Use the **General Settings** menu to define the values of a group of settings:
**Home page**

**Title**

Use this field to change the title of the VISUAL PLANNING home page.

**Icon**

Use this field to change the Client button icon in the VISUAL PLANNING portal.

**Application name**

This field is used to change the name of the Client button in the VISUAL PLANNING portal.
Description
Use this field to personalize the home page by means of an editor. You can use html code if you wish.

Show 'Visual Planning' icon
Uncheck this box to hide display of the Visual Planning icon in the home page.

Show 'Admin Center' icon
Uncheck this box to hide display of the Admin Center icon in the home page.

Client

Refresh time limit
Use this characteristic to specify the refresh time limit of client workstations in minutes.
If the value is -1, the time limit is specified for each workstation.

Desktop Shortcuts
Check this box to create icons providing access to the application on the desktop of user workstations the first time the application is launched.

Clients verbose log
Check this box to enable verbose log mode on each user’s client workstations.

Locking time limit
This characteristic specifies the session locking time limit if the user performs no action.
If the value is -1, no locking time limit is specified. Application will not be locked.
If a time limit is chosen, the screen will display a window to log in once more. You must then type in the password again.
Application

Server Language
Use this field to select the server language. If no language is selected, VISUAL PLANNING automatically uses the installation server's language.

Deny access to logs
Check this box to deny users access to the logs page.

Deny access to activation
Check this box to deny users access to the license activation page.

Verbose log
Check this box to enable the server's verbose log.

Log deletion time limit
Use this characteristic to specify the server logs deletion time limit in days.
- If the value is -1, no server log will be deleted;
If the value is 30, only server logs from the last 30 days will be kept;
If the value is 60, only server logs from the last 60 days will be kept.

VPPortal

Title
Use this field to change the title of the VPPORTAL home page.

Force the planner
By default the user can choose the planner they want to log into from the list of existing planners.
Use the "Force the planner" field to force users to log into a single planner in VPPORTAL mode.

Description
Use this field to personalize the VPPORTAL home page header by means of an editor. You can use html code if you wish.

Skin
Use this field to change the skin of the VPPORTAL home page. You can choose from the themes shown in the list.

3. Password Configuration
You can define the password policy. To do so, click on Password Configuration.
The options are:

- Minimum number of characters;
- At least one uppercase;
- At least one special character (@#$%);
- At least one digit;
- Prohibit the last 3 passwords;
- Number of days of password validity (up to 90);
- Blocking the account after 3 failed attempts;
- Send an e-mail to a person if the account is blocked.

4. SAML2

SAML or « Security Assertion Markup Language » is a standard open protocol based on XML language that is used to exchange authentication and authorization data.

SAML allows a unique authentication or Single Sign-On (SSO) on the Internet. Through single sign-on, a user can browse several website without having to authenticate on each site.
Enable for Visual Planning
Tick this box to enable SAML2 authentication for the Visual Planning rich client.

Enable for VPPortal
Tick this box to enable SAML2 authentication for VPPortal.

SP
This is the Service Provider.

Sender URL
This address is automatically filled in the configuration prompt for SAML2.

ACS URL
This address is automatically filled in the configuration prompt for SAML2.

IdP
This is the Identity Provider.

Sender URL
Please enter the identification address given by the Identity Provider (URL Issuer).

SSO URL
Please enter the SSO URL address given by the Identity Provider.

X509 Certificate
Please enter the certificate given by the Identity Provider.

5. LDAP

Configuration
This function is for companies that use an LDAP directory server (Lightweight Directory Access Protocol), containing in particular all the logins and passwords of computer application users.

By connecting VISUAL PLANNING to this directory, authentication of users logging into VISUAL PLANNING will be performed automatically from the directory.

Users will be imported into VISUAL PLANNING once the LDAP configuration has been completed.
However the passwords must not be created or modified in the ADMIN CENTER. They will simply be typed in by users logging into VISUAL PLANNING, and will be automatically authenticated (or rejected) by the directory.

In this case define the following characteristics:

**Protocol**
Choose from the list of types of protocol used: LDAP or Active Directory.

**Host**
Specify the IP address or name of the machine hosting the LDAP server.
You can also specify the port and indicate whether or not the SSL protocol is to be used.

**Root DN**
Specify the username for logging in on the chosen Domain Name.

**Password**
Specify the password for logging in on the chosen Domain Name.
**Base DN**

Designates the Domain Name from which VISUAL PLANNING will search for users. This domain is a sub-set in the hierarchy of possible users.

**Validate**

If the login is successful and the option is enabled, the password of any user logging into VISUAL PLANNING whose login is recognized in the LDAP directory will be identified by this same directory, without requiring any administrator intervention.

**Import users**

Once the LDAP has been configured, start importing users.

The following screen appears:

- Show only new users: to only show new users in the list;
Do not show e-mail usernames: to display the username that will be used as the login;
Show only e-mail usernames: on the contrary, users will log in using their e-mail usernames.

6. External access configuration

VISUAL PLANNING allows login with FTP, HTTP or WEBDAV servers. Use the "External access configuration" button to enter the settings necessary to use them.

When you click on the "External access configuration" button, the following screen appears:

Enter the URL of the FTP server, Host or WEBDAV, then enter the login settings (login and password).

VISUAL PLANNING compares each URL (FTP, HTTP or WEBDAV) used in the planner configuration with the URLs declared in the FTP /HTTP/WEBDAV configuration in the ADMIN CENTER, and uses their access codes.

7. Database Request

You can access planner data from ADMIN CENTER. To do this, click on Database Request to open the following screen:
It is absolutely prohibited to use any queries other than SELECT in this tool.

If data is modified in the database, the maintenance contract will be terminated.

We strongly advise you to contact the STILOG I.S.T. technical department if data manipulations are necessary.

8. File storage and document browser

Files can be stored on Dropbox or Google Drive in addition to the Visual Planning server. To enable storage on one of these 2 platforms, you must enter the keys generated by DropBox or Google Drive.

Click on the document Browser to see the list of documents that have been downloaded.

See File storage

9. Show server statistics

You can obtain server statistics.

To do this, click on Show server statistics.

The following window is displayed:
File: to choose the server log file to be analyzed. It is usually a date.

Time period: to choose the time period during the day to be analyzed.

Data: to choose a data type to analyze.

10. Show server logs

This functionality displays the list of server logs.
The server log is displayed directly in the window.

- Click on the server log you are interested in to display it in the window.
- To download the server log, click on the download button ;
- Click on the Select/unselect all button to select / unselect them all;
- Click on the Delete all selected files button to delete the selected logs.

11. Add

Use this functionality to add:

- a planner:
  - from a planner backup in .VPS format,
  - based on a planner template.
- a new user,
- a new group.

12. Export

Use this functionality to export:
■ a specific planner: you must first select the planner;
■ the administration data.

13. Import

Use this functionality to import:

■ a planner;
■ users;
■ the administration data.
Chapter II. License management

License Management enables you to attach users to one of the subscribed licenses.

Admin Center enables you to create, modify and delete licenses and assign users to them.

1. License types

To obtain a more detailed description of the types of licenses and conditions for using them, contact STILOG I.S.T. directly.

Contact STILOG I.S.T.:
- E-mail: sales@stilog.com
- Tel: +33 1 47 29 29 66 (Europe), +1 (855) 589-9800 (USA)

Named licenses

The number of users attached to each license must be within the maximum number of users authorized for this license.

When the maximum number of users authorized for the license is reached, a warning message is displayed and it is no longer possible to associate additional users to the license.

Floating licenses

The number of users attached to each license can exceed the maximum number of users authorized for this license.

When the number of users simultaneously logged in is equal to the number of users authorized for the license, a warning message is displayed, and it is no longer possible to log into VISUAL PLANNING.

2. License characteristics

Licenses are visible directly in the Admin Center window.
By right-clicking on a license you can:

- **Modify** the license's characteristics (see [Changing a license](#));
- **Update** the license (see [Updating a license](#));
- **Send an e-mail**: to send an e-mail to the license's users.
- **Delete** a license (see [Deleting a license](#)).

### 3. Creating a license

During installation the licenses are installed automatically.

To add a new license, you should contact the STILOG I.S.T. technical support.

---

Any modifications to licenses can lead to malfunctions.  
*We strongly advise you to contact STILOG I.S.T. technical support if these types of manipulations are necessary.*

- **E-mail**: [support@stilog.com](mailto:support@stilog.com)
- **Tel**: +33 1 47 29 29 66 (Europe), +1 (855) 589-9800 (USA)
4. Changing a license

Any modifications to licenses can lead to malfunctions. *We strongly advise you to contact STILOG I.S.T. technical support if these types of manipulations are necessary.*

- E-mail: support@stilog.com
- Tel: +33 1 47 29 29 66 (Europe), +1 (855) 589-9800 (USA)

The only recommended modifications are:

- Adding a description to the license,
- Assigning users to the license.

We strongly advise you not to make any other modifications without the help of STILOG I.S.T. technical support.
Adding a description to a license

It is recommended to add a description to each of the existing licenses in order to identify them with certainty.

Assigning users to a license

To assign users to one of the licenses, choose the license users in the right-hand part and drag them to the left-hand part via the arrows.

If the number of authorized users has been exceeded, the arrows are grayed out.
You can also manage assignment of users to licenses via user management.

5. Updating a license

Select the license to update by right-clicking on it.

The following window appears:

![Serial number window](image)

Insert the license number in the **Serial number** field.

Click on **Validate** to obtain this activation code via Internet or enter the code given by STILOG I.S.T. technical support.

A license update is definitive.

6. Deleting a license

To delete a license, contact STILOG I.S.T. technical support

Deletion of a license changes the application’s architecture template. It should not be done without careful consideration.
Deletion of a license is definitive.
Chapter III. Services management

1. DEFINITION

Services management enables you to see, start and stop VISUAL PLANNING services. This relates to automatic importing and exporting of resources and events, as well as the automatic planner backup service.

This functionality only exists in the VISUAL PLANNING ENTERPRISE version.

2. CHARACTERISTICS OF SERVICES

Viewing of services

Planner services are accessed via the Admin Center.

You can see whether a service is installed or not by checking if it is grayed in the list of services.

Starting the service

To start a service, right-click on the service > Start the service.
Stopping the service

To stop a service, right-click on the service > Stop the service.

3. E-MAIL SENDING SERVICE

The e-mail sending service is used to automatically send e-mail if contexts for sending e-mail at a regular frequency exist in the planners.

To do this:

- In the Admin Center, you must:
  - Start the "Send mail" service,
    - Enable 'Send mail' on the relevant planner (see Planner Management),
- and enter the settings concerning services in e-mail contexts in the relevant planners.

To modify the service characteristics, right-click on Send mail > Modify.

The following window opens:
Name
This is the name of the service. This data cannot be modified.

Description
Give the service a description. The description is optional.

Automatic start
Use this checkbox to automatically start the service each time the VISUAL PLANNING application server starts.

4. IMPORT/EXPORT SERVICE
The import/export service launches automatic imports and/or exports if contexts for imports/exports at a regular frequency exist in the planners.

To do this:

■ In the Admin Center, you must:
  ■ ▪ Start the "Import/Export" service,
  ▪ Enable 'Import/export' on the relevant planner.
■ and enter the settings concerning services in import and/or export contexts in the relevant planners.

To modify the service characteristics, right-click on Import/Export > Modify.

The following window opens:
Name

This is the name of the service. This data cannot be modified.

Description

Give the service a description. The description is optional.

Automatic start

Use this checkbox to automatically start the service each time the VISUAL PLANNING application server starts.

5. AUTOMATIC BACKUP SERVICE

The backup service performs daily automatic backups of the planner in .VPS format.

To do this:

■ In the Admin Center, you must:
  ■ ▪ Start the "Backup" service,
  ▪ Enable 'Automatic backup' on the relevant planner.

To modify the service characteristics, right-click on Backup > Modify.

The following window opens:
Name
This is the name of the service. This data cannot be modified.

Description
Give the service a description. The description is optional.

Automatic start
Use this checkbox to automatically start the service each time the VISUAL PLANNING application server starts.

Backup directory
If no path is specified, the backup directory is the **backup** directory in VISUAL PLANNING's installation directory at webapps/vplanning.
This directory can be modified. To do so, type in the access path for the new directory. This directory must be accessible for the server.

Start time
Define the backup start time.
Number of days archived

Here, you define the number of backup days to keep in the backup directory.

Sending mail

Use this checkbox to send an e-mail when the backup has finished.

The e-mail will indicate whether or not the backup was successful. If a backup was not successful, the name of the planners for which the backup was not performed correctly will be indicated in the e-mail.

ℹ️ The e-mail will be sent provided the smtp settings in the automatic e-mail sending module are provided and correct.

Sender

Indicate the sender's e-mail address.

Recipients

Indicate the e-mail address of the recipient(s), separated if necessary by semi-colons.
Chapter IV. Module Management

1. DEFINITION

Module management enables you to install the module licenses and define administrators for the modules.

This functionality only operates in the VISUAL PLANNING ENTERPRISE version from the Admin Center.

At present the available modules are:

- Send Mail (standard),
- Send SMS (standard),
- RSS Feed (standard),
- Geolocation (standard),
- Mail Merge (standard),
- Web Calendar Publication (additional),
- VPGO (additional),
- VPPORTAL (additional),
- VPWhatsUp (standard).

2. ADMINISTRATION

Viewing the modules

The planner's modules are accessed in the Admin Center.
Installing a module

The Send Mail, Send SMS, RSS Feed, Geolocation, Mail Merge and VPWhatsUp modules are standard modules in the VISUAL PLANNING ENTERPRISE application. They do not require specific installation.

To install an additional module, you simply need to register its license.

To do so, **Right-click on the module > Register the license.**

- For VPPORTAL and VPGO, it is possible to register a Floating or Named license;
- For ICAL, it is only possible to register a named license.

The following window opens:
Enter the serial number.

You must now activate the license:

■ either via Internet,
■ or by typing in the number that VISUAL PLANNING technical support gave you by telephone.

Now click on the Validate button.

You can see whether a module is installed or not by checking whether or not it is grayed in the list of modules.

**Defining a module’s administrators**

A module may require specific settings.

These settings can only be configured by the module’s administrators.

Define which user(s) is/are a module's administrator(s) go to the relevant module > right-click > Modify.

The following window opens:
Click on the button in the *Administrators* field. Choose the module's administrators from the listed users.
Chapter V. User Management

1. DEFINITION

A VISUAL PLANNING User is principally identified by their username and password, which enable them to access one or more planners.

It is possible to define an unlimited number of users, but only users associated with a license have access to VISUAL PLANNING.

The effective number of users who can log into the application is therefore defined by the licenses purchased.

The Admin Center enables you to manually create, modify and delete users and assign them to licenses, groups and planners.

2. ADMINISTRATION

Viewing of users

Users are visible in the Admin Center.
You can see whether a user is enabled or not by checking if they are grayed in the list of users.

Creating a user

To create a user, right-click in the window dedicated to **Users > Add a user**.

The following window appears:

Now specify the user characteristics and click on one of the following buttons:

- **Validate** to create the user,
- **Cancel** to cancel creation of the user,
- **Apply** to create the user and subsequently create a new user. This button is available when creating a new user.

A user has the following characteristics:
Username
Define the user's username. This will be used as the user's login.
This username must be unique for each user.

Enabled
If this checkbox is checked, the user is enabled.
Uncheck this box to temporarily prevent this user from accessing VISUAL PLANNING.

You can see whether a user is enabled or not by checking if they are grayed in the list of users.

Profile Photo
You can add a profile photo to the user.
Click on:

➕ to add a photo,
➖ to delete a photo added earlier.

LDAP
This field is automatically filled in when a user is created. It is:

- empty if the user was created via the VISUAL PLANNING Admin Center;
- LDAP or AD if the user was imported via the LDAP import functionality.

Authentication via LDAP is forced for import if the user already exists.

This function is for companies that use an LDAP directory server (Lightweight Directory Access Protocol), containing in particular all the logins and passwords of computer application users.

New Password

Information about the password
The password is necessary to access VISUAL PLANNING.
The first password is empty. This password is unrestricted and can be left empty.

The user is responsible for the password. The first time the user logs in this password is empty, and the user is asked for a new password.

The password is case-sensitive.

For subsequent modifications of the password, **right-click on the user > Changed password**.

The following window appears:

![Change password window](image)

The user must enter the new password twice.

**Information about typing in a new password**

It is possible to ask a user to change their password, by checking the **New password** box.

In this case, the next time the user logs in, they must type in their old password, and then type in a new password.

**Resetting the password**

It is possible to reset a user's password by **right-clicking on it > Reset password**.

A window is displayed asking the user if they want to validate the reset or not.

The next time the user logs in, they will not be asked for a password. A window will then open enabling them to type in a new password.

**Full name**

This characteristic is optional. It is used to indicate the user's full name.

**E-mail address**

This characteristic is optional. It is used to indicate the user's e-mail address. It is necessary in order to send a manual e-mail from an event. (See [Sending e-mail from an event](#))
**Mobile phone**

This characteristic is optional. It is used to indicate the user's mobile phone number.

**Office Phone**

This characteristic is optional. It is used to indicate the user's landline phone number.

**Groups**

View and/or modify the group(s) the user belongs to.

**Licenses**

View and/or modify the license(s) the user is linked to.

**History**

This field contains the user creation and modification history. Click in this field to display a new window detailing the modifications made previously.

---

**Modifying a user**

To modify a user, right-click on the user > **Modify**. You can also double-click on the user to open the editing window.
Make the modifications you want and **Validate** to save the modifications.

**Deleting a user**

To delete a user, **right-click on the user > Delete**.

A window is displayed asking if you want to validate deletion or not.

It is not possible to cancel deletion of a user.

It is possible to disable a user temporarily (see [Enabled](#)).

**Send e-mail**

Use this option to send an e-mail from the Admin Center to the selected user. The mailer window opens, and the recipient is the user.

This option is only available if the [SMTP server](#) has been configured properly.

**Import users**

It is possible to import users from an external file.

**Prerequisites**

**Situation 1**: *.TXT file: The column separator must be a tabulation (TAB character). There is no need for a first line of headers containing the column names.

It must have the following columns in this order:
■ Column 1: The user's Name,

and optionally:

■ Column 2: The user's full name,
■ Column 3: The e-mail address,
■ Column 4: The mobile phone number,
■ Column 5: The landline phone number.

Remark: Repeated imports

When several users are imported in succession:

■ Existing users will not be duplicated or modified
■ Users yet to exist will be created
■ Deletion of users is not managed by importing; it must be performed manually.

Situation 2: *.CSV file: You must have a column named NAME containing the user logins, and the following optional columns (separated by semi-colons):

■ FULLNAME: User's full name,
■ PHONE: User's phone number,
■ MOBILE: User's mobile phone number,
■ E-MAIL: User's e-mail address,
■ GROUPS: Groups the user belongs to (separated by commas),
■ LICENSES: Licenses the user is linked to (separated by commas).

If the person has already been created and their group is different in the import file, then it will be modified in VISUAL PLANNING.

No passwords can be imported.

Launching importing

In the Admin Center, right-click on a user > Import Users.

Choose the *.TXT or *.CSV file to import, then click on Open.
Chapter VI. Group management

A User Group contains all the users that have the same access rights to a specific planner.

It is identified by:

■ Its name;
■ An optional description;
■ and a list of users.

To be used, the groups must be assigned to a planner.

Admin Center enables you to create, modify and delete groups, assign users to them and associate them with planners.

This only functions with VISUAL PLANNING ENTERPRISE.

1. Group management actors

Group management is available to central and local administrators.

When a local administrator opens ADMIN CENTER and clicks on the "Groups" button, they see the list of groups assigned to the planner(s) they administer.

They can create new groups, assign users to them and assign them to one or more planners that they administer.

2. Group characteristics

Groups are visible directly in the Admin Center window.
By right-clicking on a group you can:

- **Modify** the group's characteristics (see [Changing a group](#));
- **Add** a group (see [Creating a group](#));
- **Send e-mail**: to send an e-mail to the group’s users. This option is only available if the SMTP server has been configured properly;
- **Delete** a group (see [Deleting a group](#)).

### 3. Creating a group

To create a group, right-click in the window dedicated to **Groups > Add a group**.
Indicate the group's characteristics, then:

- **Validate** to validate creation,
- Otherwise **Cancel**,
- **Apply** to validate creation and subsequently create a new group. This button is available when creating a new group.

### Name

Give the group a name.

### Description

Give the group a description. The description is optional.
Assignment

Select users in the left-hand panel and move them to the right-hand window using the arrows to assign them to the group.

4. Changing a group

To modify a group, right-click on the group name > Modify. You can also double-click on the group to open the group’s window.

Make the modifications you want and Validate to save the modifications.

5. Deleting a group

To delete a group, right-click on the group name > Delete.

A window is displayed asking if you want to validate deletion or not.

It is not possible to cancel deletion of a group.

6. Send e-mail

Use this option to send an e-mail from the Admin Center to all the group's users. The mailer window opens, and the recipients are the group's users.

This option is only available if the SMTP server has been configured properly.
Chapter VII. Planner management

1. DEFINITION

In VISUAL PLANNING, each planner is a database.

You can manipulate these planners:

- create them,
- import them,
- restore them,
- export them,
- delete them.

All these functionalities are available to the VISUAL PLANNING general administrator:

- In ONE version: from VISUAL PLANNING,
- In ENTERPRISE version: from the Admin Center.
Chapter VIII. Management of VP ONE planners

1. DEFINITION

In VISUAL PLANNING ONE, planners are managed directly in the client.

For planners installed using VISUAL PLANNING ONE, it is possible to:

- create them,
- import them,
- restore them,
- export them,
- delete them.

2. ADMINISTRATION

Viewing planners

The planners are viewed in the Planner > Open tab.

Click on the planner you want to open.

Creating a planner

In this version, any user that has access to VISUAL PLANNING can create a new planner.

See Create a new planner

Importing a planner

Importing a planner creates a new planner, i.e. a new database, using a *.VPS file.

To import a planner, go to the Planner menu > Import Block > Import a planner.

In the window that is displayed:

- find the planner file with the *.VPS suffix,
- select it,
- then click on Open.

The following window appears:
Now enter:

- the **Name** of the new planner to import,
- the **Description** of this planner,
- Then click on **OK**.

If a planner with the same name already exists in the planner, the following window appears:

To replace the existing planner, click on **Yes**. Otherwise, click on **No**.

**Planner Export**

To export a planner, go to the **Planner menu > Export Block > Export a planner**.

There are two possibilities:

- Export in a file,
- Export as a template.
Export in a file
To export a backup of the planner in the *.VPS file format.
This file contains the whole planner.

Export as a template
To create a new planner template you can use to create a new planner.

Deleting a planner

Great care must be taken when envisaging deletion of a planner. Deletion of a planner is irreversible, and destroys:

- All the data (Resources, Events, etc.),
- the configuration.

We strongly recommend you check carefully that the planner in question can be deleted!
It is a good idea to make a backup of the planner beforehand.

To delete a planner, **right-click on the Planner > Delete**.

In the message that appears:

- To confirm deletion, click on **Yes**, 
- To cancel deletion, click on **No**.
Chapter IX. Management of VP ENTERPRISE planners

1. DEFINITION

In VISUAL PLANNING ENTERPRISE, planners are managed directly from the Admin Center.

You can manipulate these planners:

- create them,
- import them,
- restore them,
- export them,
- delete them.

2. ADMINISTRATION

Viewing planners

Planners are visible directly in the Admin Center window.

![Admin Center Window](image)
Creating a planner

Only the VISUAL PLANNING general administrator can create a new planner.

To create a new planner, right-click in the planners frame. Add a planner:

- From a vps file: Choose the planner in the window that opens;
- based on an existing planner template: Choose the planner template.

The following window appears:

![Planner window](image)

Now specify:

- The planner **Name**,
- Its **Description**.

Now validate by clicking on the **OK** button.

Modifying a planner

Modification of a planner usually concerns its settings.

In the Admin Center, modification of a planner concerns:
Assignments of the planner’s users and administrators.

This assignment is obtained by right-clicking on the planner - Modify.

The following window appears:

You can now modify its properties and validate by clicking on the Validate button.

**Name**

Give the planner a name, given when it was created. This name is unique to each planner.

**Description**

Give the planner a description. The description is optional.
Planner logo
You can associate the planner with a logo. This logo will be displayed on the VISUAL PLANNING portal if access to the planner has been allowed below.

Publish access with Visual Planning
Use this checkbox to add direct access to this planner's rich client.
A direct input on the planner is added on the VISUAL PLANNING home page.

Publish access with VPPortal
Use this checkbox to add direct access to the VPPortal version of this planner if the VPPortal settings have been configured.
A direct input on the VPPortal version of this planner is added on the VISUAL PLANNING home page.

Enable the SmartToolbar
Use this checkbox to modify the menu bar in VISUAL PLANNING using the SmartToolbar.

Enable deletion of history
Use this checkbox to automatically delete the history of entities deleted more than 60 days ago.

Restore date
This is the most recent planner restore date.

Access to private data
This checkbox enables the "admin" user to access private data if it is checked.

Configuration dimensions
Use this functionality to define the planner dimensions which are called Configuration dimensions.
E.g. This concerns dimensions governing the statuses.
Therefore the resources of dimensions present in this list will be modified or deleted if a configuration import is performed.

Enable Undo
Use this checkbox to enable the Undo function in the VISUAL PLANNING rich client.

Version
This is the version of the planner structure in the database.
STILOG I.S.T. Technical Support may ask you for this number when performing maintenance.

Admin Users
If necessary, define the list of users with planner administrator rights.

Block access
Check this box to log out all the planner’s users.

See [Logged in users](#)

A window will display enabling you to type a message that will be displayed on all the workstations where VISUAL PLANNING is open.

![Disconnect users](image)

Click on [Validate](#) to log out all the users.

- Once they are logged out, only the general administrator and planner administrators can log in again.
- The planner will be grayed out in the Admin Center.

Protection enabled
This checkbox is checked if the planner permissions are enabled.

Protected planners are indicated in the list by a padlock on the planner icon.

Enable ‘Import/export’
Check this checkbox if imports and/or exports have to be used frequently on this planner.

See [Export by service](#) and [Import by service](#)

Modification of this property will only take effect when the service restarts.
Enable ‘Send e-mail’

Check this checkbox to enable automatic sending of e-mails from one or more events from this planner.

See Automatic sending of e-mail

Modification of this property will only take effect when the service restarts.

Enable automatic backup

Check this checkbox to enable automatic backup of the planner.

See Automatic backup service

Enable export URL

Check this checkbox to enable planner export via an URL. To display the export URL, go below.

Authorized Users/Groups

In the corresponding tab, define the list of groups and/or users that have access in read/write mode.

Deleting a planner

Great care must be taken when envisaging deletion of a planner.

Deletion of a planner is irreversible, and destroys:

- all the data (Resources, Events, etc.),
- the configuration,
- the existing permissions.

We strongly recommend you check carefully that the planner in question can be deleted!

It is a good idea to make a backup of the planner beforehand (see Planner Export)

To delete a planner, right-click on the Planner > Delete.

The following warning message appears:
To confirm, click on Yes,  
To cancel, click on No.

## Restore a planner

Restoration of a planner overwrites an existing planner with a planner backed up in the *.VPS while keeping the same name.

You can restore a planner from a file or from an automatic backup.

To restore a planner, right-click on the planner to overwrite > Restore > Choose the correct option.

---

### Restore from a file

The window for choosing the file to restore then opens:
You must:

- find the planner file with the *.VPS suffix,
- select it,
- then click on Open.

The import may take a few minutes.

**Restore from a backup**

The window for choosing the backup date then opens:

Choose and date and click on OK to start the restore.

**Planner Export**

To export a planner, right-click on the planner to export" Export planner."
There are then two possibilities:

- Export in a file,
- Export as a template.

The .VPS file contains the entire planner as well as the associated groups and their permissions.

It also contains template files for e-mail merge as well as Image files that have been downloaded onto the server.

Export in a file

To export a backup of the planner in the *.VPS file format.

The following window opens:

Then:

- define the path where the *.VPS file will be saved,
- choose a Name,
- and click on the Save button.
**Export as a template**

To create a new planner template you can use to create a new planner.

The following window opens:

![Image of the Export a planner as model window]

You must then specify:

- a **Name**,
- a **Description**,
- and click on the **Validate** button.

This template is then visible when a new planner is created.

**Display export URL**

This functionality is only active if the URL enabling box has been checked. (See Enable export URL)

To display the planner's export URL click on this link.

![Image of the URL window]
To trigger export of the planner, simply copy/paste this URL into a web browser or the required functionality.

The name of the resulting file will be "Planner_name_yyyymmdd_hhmm.vps".

Configuration

In some situations, the planner may need to evolve.

For this purpose, it is recommended to modify a qualification planner before reproducing the configuration modifications in the production planner.

The configuration import/export functionality is useful in these situations.

This functionality enables you to modify the configuration in a backup copy of the planner, perform tests to verify the planner functions properly with the new configuration, and finally transfer the modifications to the production planner.

Export the configuration

After modifying the configuration and performing tests on the qualification planner, right-click on the planner > Configuration > Export to export the configuration.

The following window appears:

This will generate a .VPI file. This file contains the planner's structural entities (dimensions, forms, creation rules, creation hierarchies, etc.) as well as the dimension resources which have been defined as configuration dimensions.
Import the configuration

Once the .VPI file has been generated, right-click on the production planner > Configuration > Import to import the configuration modifications.

The following window appears:

Select the corresponding file and click on Open to import the configuration modifications into the planner.

These actions should be performed with great care.

If the structural entities no longer exist in the imported .VPI file they will be modified or even deleted.

Similarly, if the configuration dimensions' resources have been deleted, they will be deleted in the planner. Events associated with these resources will also be deleted.

Log out users

You can log out all a planner's users.

To do so, right-click on the planner” Log out users.

The following window appears:
Now enter a message for users before they are forced to log out, then click on Validate.

Logged in users

You can consult the list of users logged into a given planner.

To do so, right-click on the planner" Logged in users.

A window then opens, showing the list of users logged into the planner:
You can consult the history of logins to a given planner.

To do so, **right-click on the planner** "Login history"

A window then opens, showing the list of users logged into the planner:
You can then specify the beginning and end of the period you want to view.

You can define periods of time:

- with a relative Beginning and End,
- with a fixed Beginning and End,
- with a fixed Beginning and relative End,
- with a relative Beginning and a fixed End.

**Fixed Date**

You must specify a date and time.

This date is not connected to the moment when the period of time is used.

**Relative Value**

You must specify a period relative to the moment when the period of time is used.

Each sliding period is defined by:

- A **Relative value**: A number. The reference period is represented by the number 0.
- A **Relative unit**: Time, Day, Week, Month, etc.
Examples:

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Current date (when functionality is used)</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <strong>fixed date</strong> of 1st January 2018</td>
<td>regardless of the current date</td>
<td>always means 1st January 2018</td>
</tr>
<tr>
<td>The <strong>relative value 1 Day</strong></td>
<td>on the date 31 December 2017</td>
<td>means 1st January 2018</td>
</tr>
<tr>
<td>The <strong>relative value 1 Day</strong></td>
<td>on the date 1st January 2018</td>
<td>means 2 January 2018</td>
</tr>
</tbody>
</table>

Note that by double-clicking on a session, a window as shown below is displayed if modifications were made during the session.

The described information corresponds to the modifications made by the user.

If nothing has been created / modified / deleted, the following window is displayed:

### Send e-mail

Use this option to send an e-mail from the Admin Center to the planner's users. The mailer window opens, and the recipients are all users.
This option is only available if the SMTP server has been configured properly.
Chapter X. Permission management

1. DEFINITION

Permission Management enables you to protect each planner so as to restrict the rights of certain groups of users.

Planner use rights are defined in two steps:

1. Assignment of authorized groups and/or users,
2. Definition of permissions to view and modify a planner.

Now define in the Admin Center the rights for each group concerning the planner.

This functionality only exists in the ENTERPRISE version.

2. ADMINISTRATION

Viewing planner permissions

To access planner permissions right-click on the relevant planner > Edit permissions.

The permission editing window then opens:
In this window you can easily view the permissions by clicking on them.

In addition it is possible to quickly view the permissions of a single group by selecting it in the list of groups.

Example:

If you select the User group in this list you will only view the permissions of the User group.
Assigning a user group to a planner

The central and local administrators designated when protection is initialized can log into the Admin Center and define the user groups that have identical rights for this planner.

See Group management

Once the group is created, it must be assigned to the relevant planner:

- by dragging-dropping it onto the planner,
- by right-clicking on the planner > Modify > Authorized Users/Groups tab > Drag the groups from left to right.

The following window opens:

![Setting permissions](image)

This window enables you to initialize the permissions attributed to this new group:

- If the "Administrator" Permissions box is checked, this group will inherit all the administrator rights for the planner, except for the modules.
- If the "Planner" Permissions box is checked, this group will inherit all the rights for editing planner data, but not the rights for the planner structure,
- If the "Read only" Permissions box is checked, this group will not inherit any right apart from data viewing,
- If the Permissions box of "an existing group" is checked, this group will inherit the same permissions as the group selected in the pull-down list beneath this box,
- If the new group's permissions do not match the 4 possibilities, click the Cancel button. It will then not have any pre-set permissions.
Creating a permission

To create a permission, in the permission editing window choose the VISUAL PLANNING for which you want to create the permission:

You can also select the group that will possess the permission, using the list:

Example:
If you select the User group in this list you will only view the permissions of the User group.

Once the entity has been selected, you can add a permission by clicking on the button. Depending on the selected entity, you can create different types of permission:

- Administration Permission,
- Visibility Permission,
- Creation Permission,
- Modification Permission,
- Deletion Permission,
- 'Read only' Permission.
The right-hand part of the window then opens. Indicate the permission's characteristics:

- depending on its type,
- and the entity.

See Types of permissions

Changing a permission

To modify a permission, click on the relevant permission and modify the characteristics as you wish.

See Creating a permission

Duplicating a permission

To duplicate a permission on the planner, use the permission editing window.

Right-click on the permission to duplicate" Duplicate.

The permission is then duplicated for all groups using this permission.

Deleting a permission

To delete a permission on the planner, use the permission editing window.

Right-click on the permission to delete" Delete.

The permission is then deleted for all groups using this permission.

You cannot cancel deletion of a permission.
Enabling permissions

All the permissions can be enabled or disabled in the planner settings.

See Enabling permissions

3. TYPES OF PERMISSIONS

There are five types of permission:

- Visibility,
- Creation,
- Modification,
- Deletion,
- Administration (for structural entities only).

Permissions can be defined on the following entities/functionalities:

Click on the X symbol to access them directly

<table>
<thead>
<tr>
<th></th>
<th>Visibility</th>
<th>Creation</th>
<th>Modification</th>
<th>Deletion</th>
<th>Rights settings identical to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Forms</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Valuation items</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Valuation items</td>
</tr>
<tr>
<td>Events hierarchies</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Event creation rules</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Types of period</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Hourly templates</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Hourly calendars</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Daily templates</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Daily calendars</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Objective constraints</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Coherency constraints</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Time gap constraints</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Category</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---------------------</td>
</tr>
<tr>
<td>Workflows</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>Workflows</td>
</tr>
<tr>
<td>Time periods</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions</td>
</tr>
<tr>
<td>Event exports</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Event exports</td>
</tr>
<tr>
<td>Resource exports</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Event exports</td>
</tr>
<tr>
<td>Event imports</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Event exports</td>
</tr>
<tr>
<td>Resource imports</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Event exports</td>
</tr>
<tr>
<td>Predefined views</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Predefined views</td>
</tr>
<tr>
<td>Events Editors</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Events Editors</td>
</tr>
<tr>
<td>Resources Editors</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Events Editors</td>
</tr>
<tr>
<td>Workloads</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Workloads</td>
</tr>
<tr>
<td>VPPortal Templates</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Events Editors</td>
</tr>
<tr>
<td>VPGO Templates</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Events Editors</td>
</tr>
<tr>
<td>Mails Templates</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Events Editors</td>
</tr>
<tr>
<td>SMS Templates</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Events Editors</td>
</tr>
<tr>
<td>Mailmerge Templates</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>Events Editors</td>
</tr>
<tr>
<td>Resource filters</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Resource filters</td>
</tr>
<tr>
<td>Events filters</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Resource filters</td>
</tr>
<tr>
<td>Events reports</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Resource filters</td>
</tr>
<tr>
<td>Favorite displays</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Resource filters</td>
</tr>
<tr>
<td>Dimensions Resources</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Dimensions Resources</td>
</tr>
<tr>
<td>Events</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Events</td>
</tr>
</tbody>
</table>

**Read-only Permissions**

Use read-only permissions to restrict all the rights of all groups that have this permission.

Permissions created by "Read only" are the "forbidding on xxxx" type.

In the case of multiple groups or multiple permissions:
In creation, forbidding has priority over other permissions. This means that if it is checked, the forbidding overrides other permissions.

In modification and deletion, the other permissions are taken into account.

Administration Permissions

Use administration permissions to create permissions on structural entities.

An administration permission groups the creation, modification, and deletion permissions and gives all the rights to groups that have it.

Whenever an administration permission is created for a given entity, the other permissions are deleted. You must then assign the group(s) that has/have this administration permission. The remaining groups will not have any right over the relevant entity.

To give less restricted rights to other groups, you must create other permissions for them. At that point, the administration permission disappears to allow you to personalize the newly created permissions.

Permissions on dimensions

These permissions are the same as permissions for forms, event hierarchies, creation rules, period types, hourly templates and calendars, daily templates and calendars, time periods and constraints.
Creating dimensions

Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions with the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Deletion

Define the groups that have permission to delete on the dimensions thereby created.

The groups can be:

- **All groups**: all groups with the right to modify these dimensions can delete the dimension that is thereby created.
- **Creator groups**: only groups with the right to create these dimensions can delete the dimension that is created.
- **Permission groups**: only groups that have the permission can delete the dimension thereby created.

Modification

Define the groups that have permission to modify the dimensions thereby created.

The groups can be:

- **All groups**: all groups with the right to modify these dimensions can modify the dimension that is thereby created.
- **Creator groups**: only groups with the right to create these dimensions can modify the dimension that is created.
- **Permission groups**: only groups that have the permission can modify the dimension thereby created.

Forbid

Check this box to forbid creation of all dimensions.

In the event of multiple groups or multiple permissions, this option has priority over other permissions.

This means that if it is checked, the forbidding overrides other permissions.

Groups

Define groups that have this permission in the **Groups** tab.
Modification of the dimensions

Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions with the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Selection
Define the dimensions this permission makes it possible to modify.

Groups
Define groups that have this permission in the Groups tab.

Deletion of dimensions

A deletion permission makes it possible to delete one or more dimensions.

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions with the same type).
History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.
This property is updated automatically.

Selection
Define the dimensions that can be deleted.

Groups
Define groups that have this permission in the Groups tab.

Permissions on the valuation items

Visibility of valuation items
**Name**

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

**Description**

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions with the same type).

**History**

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

**Selection**

Define the valuation items this permission makes visible.

**Groups**

Define groups that have this permission in the Groups tab.
Creating valuation items

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Deletion
Define the groups that have permission to delete the valuation items thereby created.

The groups can be:

- **All groups**: all groups with the right to modify these valuation items can delete the item that is thereby created,
- **Creator groups**: only groups with the right to create these valuation items can delete the item that is created,
- **Permission groups**: only groups that have the permission can delete the valuation item thereby created.

Modification
Define the groups that have permission to modify the valuation items thereby created.

The groups can be:

- **All groups**: all groups with the right to modify these valuation items can modify the item that is thereby created.
- **Creator groups**: only groups with the right to create these valuation items can modify the item that is created.
- **Permission groups**: only groups that have the permission can modify the valuation item thereby created.

Visibility
Define the groups that have permission to view the valuation items thereby created.

The groups can be:

- **All groups**: all groups with the right to create these valuation items can view the item that is thereby created.
- **Creator groups**: only groups with the right to create valuation items can view the item that is created.
- **Permission groups**: only groups that have the permission can view the valuation item thereby created.

Forbid
Check this box to forbid creation of all valuation items.

In the event of multiple groups or multiple permissions, this option has priority over other permissions.
This means that if it is checked, the forbidding overrides other permissions.

Groups
Define groups that have this permission in the Groups tab.

Modification of valuation items

This type of permission has the following characteristics:

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).
History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change. This property is updated automatically.

Selection

Define the valuation items this permission makes it possible to modify.

Groups

Define groups that have this permission in the Groups tab.

Deletion of valuation items

A deletion permission makes it possible to delete one or more valuation items.
Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

Selection
Define which valuation items can be deleted.

Groups
Define groups that have this permission in the Groups tab.
Permissions on the workflows

Visibility of the workflows

**Name**

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

**Description**

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

**History**

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Selection
Define the workflows this permission makes visible.

Groups
Define groups that have this permission in the Groups tab.

Creation of workflows

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).
History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.
This property is updated automatically.

Deletion
Define the groups that have permission to delete the workflows thereby created.
The groups can be:
- **All groups**: all groups with the right to modify these workflows can delete the workflow that is thereby created.
- **Creator groups**: only groups with the right to create these workflows can delete the workflow that is created.
- **Permission groups**: only groups that have the permission can delete the workflow thereby created.

Modification
Define the groups that have permission to modify the workflows thereby created.
The groups can be:
- **All groups**: all groups with the right to modify these workflows can modify the workflow that is thereby created.
- **Creator groups**: only groups with the right to create these workflows can modify the workflow that is created.
- **Permission groups**: only groups that have the permission can modify the workflow thereby created.

Visibility
Define the groups that have permission to view the valuation items thereby created.
The groups can be:
- **All groups**: all groups with the right to create these workflows can view the workflow that is thereby created.
- **Creator groups**: only groups with the right to create the workflows can view the workflow that is created.
- **Permission groups**: only groups that have the permission can view the workflow thereby created.

Forbid
Check this box to forbid creation of all workflows.
In the event of multiple groups or multiple permissions, this option has priority over other permissions.

This means that if it is checked, the forbidding overrides other permissions.

Allow private only

Check this box to authorize creation of private workflows.

This function is only accessible if the Forbid box is not checked.

Groups

Define groups that have this permission in the Groups tab.

Modification of workflows
Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

Selection

Define the workflows this permission makes it possible to modify.

Groups

Define groups that have this permission in the Groups tab.
Deletion of workflows

A deletion permission makes it possible to delete one or more workflows.

Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Selection
This makes it possible to define the workflows that can be deleted.

Groups
Define groups that have this permission in the Groups tab.

Permissions on event exports

These permissions are the same as those for resource exports, event imports and resource imports.

Visibility of event exports

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.
**Description**

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

**History**

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

**Apply to data**

Define a visibility criterion for event exports.

- If the chosen criterion is **is in**, you must select the list of event export contexts,
- If the chosen criterion is **contains, does not contain, starts with, does not start with, ends with or does not end with**, you must define the value in the field provided for this purpose.

**Selection**

This option is visible if the chosen criterion is **is in**. Define the event export contexts that this permission makes visible.

**Value**

This option is visible if the chosen criterion is not **is in**. Type in the criterion verification value.

**Groups**

Define groups that have this permission in the Groups tab.
Creation of event exports

Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Deletion
Define the groups that have permission to delete on the event export contexts thereby created.

The groups can be:

- **All groups**: all groups with the right to modify these event export contexts can delete the context that is thereby created.
- **Creator groups**: only groups with the right to create these event export contexts can delete the context that is created.
- **Permission groups**: only groups that have the permission can delete the context thereby created.

Modification
Define the groups that have permission to modify on the event export contexts thereby created.

The groups can be:

- **All groups**: all groups with the right to modify these event export contexts can modify the context that is thereby created.
- **Creator groups**: only groups with the right to create these event export contexts can modify the context that is created.
- **Permission groups**: only groups that have the permission can modify the context thereby created.

Visibility
Define the groups that have permission to view the event export contexts thereby created.

The groups can be:

- **All groups**: all groups with the right to create these event export contexts can view the context that is thereby created.
- **Creator groups**: only groups with the right to create event export contexts can view the context that is created.
- **Permission groups**: only groups that have the permission can view the context thereby created.

Forbid
Check this box to forbid creation of all event export contexts.

In the event of multiple groups or multiple permissions, this option has priority over other permissions.

This means that if it is checked, the forbidding overrides other permissions.

Groups
Define groups that have this permission in the **Groups** tab.
Modification of event exports

This type of permission has the following characteristics:

**Name**

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

**Description**

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

**History**

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Apply to data

Define a criterion for modifying event exports.

- If the chosen criterion is **is in**, you must select the list of event export contexts,
- If the chosen criterion is **contains, does not contain, starts with, does not start with, ends with** or **does not end with**, you must define the value in the field provided for this purpose.

Selection

This option is visible if the chosen criterion is **is in**. Define the event export contexts this permission makes it possible to modify.

Value

This option is visible if the chosen criterion is not **is in**. Type in the criterion verification value.

Groups

To define groups that have this permission in the **Groups** tab.
Deletion of event exports

A deletion permission makes it possible to delete one or more event export contexts.

**Name**

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

**Description**

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

**History**

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Selection

Define the event export contexts that can be deleted.

Groups

Define groups that have this permission in the **Groups** tab.

Permissions on the predefined views

Visibility of the predefined views

Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Selection
Define the views this permission makes visible.

Groups
Define groups that have this permission in the Groups tab.

Creating predefined views

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).
History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.
This property is updated automatically.

Deletion
Define the groups that have permission to delete on the views thereby created.
The groups can be:

- **All groups**: all groups with the right to modify these dimensions can delete the dimension that is thereby created.
- **Creator groups**: only groups with the right to create these views can delete the view that is created.
- **Permission groups**: only groups that have the permission can delete the view thereby created.

Modification
Define the groups that have permission to modify on the views thereby created.
The groups can be:

- **All groups**: all groups with the right to modify these dimensions can modify the dimension that is thereby created.
- **Creator groups**: only groups with the right to create these views can modify the view that is created.
- **Permission groups**: only groups that have the permission can modify the view thereby created.

Forbid
Check this box to forbid creation of all views.

In the event of multiple groups or multiple permissions, this option has priority over other permissions.
This means that if it is checked, the forbidding overrides other permissions.

Groups
Define groups that have this permission in the **Groups** tab.
Modifying predefined views

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Selection
Define the views this permission makes it possible to modify.

Groups
Define groups that have this permission in the Groups tab.

Deleting predefined views

A deletion permission makes it possible to delete one or more predefined views.

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).
History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

Selection

This makes it possible to define the views that can be deleted.

Permissions on event editors

These permissions are the same as those for resource editors, VPPORTAL and VPGO templates.

Only visibility permissions can be defined for events editors.
**Name**

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

**Description**

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

**History**

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

**Selection**

Define the editors this permission makes visible.

**Groups**

To define groups that have this permission in the Groups tab.
Permissions on workloads

Visibility of workloads

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Apply to data
Define a visibility criterion for workloads.

- If the chosen criterion is **is in**, you must select the list of workloads,
- If the chosen criterion is **contains, does not contain, starts with, does not start with, ends with or does not end with**, you must define the value in the field provided for this purpose.

**Selection**
This option is visible if the chosen criterion is **is in**. Define the workloads this permission makes visible.

**Value**
This option is visible if the chosen criterion is not **is in**. Type in the criterion verification value.

**Groups**
Define groups that have this permission in the **Groups** tab.

**Creating workloads**
Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

Deletion
To define the groups that have permission to delete the workloads thereby created.

The groups can be:

- **All groups**: all groups with the right to modify these workloads can delete the context that is thereby created.
- **Creator groups**: only groups with the right to create these workloads can delete the context that is created.
- **Permission groups**: only groups that have the permission can delete the workload thereby created.

Modification
Define the groups that have permission to modify on the workloads thereby created.

The groups can be:

- **All groups**: all groups with the right to modify these workloads can modify the context that is thereby created.
- **Creator groups**: only groups with the right to create these workloads can modify the context that is created.
- **Permission groups**: only groups that have the permission can modify the workload thereby created.

Forbid
Check this box to forbid creation of all workloads.

In the event of multiple groups or multiple permissions, this option has priority over other permissions.
This means that if it is checked, the forbidding overrides other permissions.

Groups
Define groups that have this permission in the **Groups** tab.

Modifying workloads

**Name**
Give this permission a name. If you type in a name, it replaces the permission’s default name and is visible in the tree on the left.

**Description**
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).
History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

Apply to data

Define a criterion for modifying workloads

- If the chosen criterion is **is in**, you must select the list of workloads,
- If the chosen criterion is **contains, does not contain, starts with, does not start with, ends with** or **does not end with**, you must define the value in the field provided for this purpose.

Selection

This option is visible if the chosen criterion is **is in**. Define the workloads this permission makes it possible to modify.

Value

This option is visible if the chosen criterion is not **is in**. Type in the criterion verification value.

Groups

Define groups that have this permission in the **Groups** tab.
Deleting workloads

A deletion permission makes it possible to delete one or more workloads.

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Selection
This makes it possible to define the workloads that can be deleted.

Groups
Define groups that have this permission in the Groups tab.

Permissions on resource filters
These permissions are the same as those for event filters, event reports and favorite displays.

Visibility of resources filters

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.
Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

Apply to data

Define a visibility criterion for resource filters.

- If the chosen criterion is **is in**, you must select the list of resource filters,
- If the chosen criterion is **contains, does not contain, starts with, does not start with, ends with** or **does not end with**, you must define the value in the field provided for this purpose.

Selection

This option is visible if the chosen criterion is **is in**. Define the resource filters this permission makes visible.

Value

This option is visible if the chosen criterion is not **is in**. Type in the criterion verification value.

Groups

Define groups that have this permission in the **Groups** tab.
Creating resource filters

This type of permission has the following characteristics:

Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Deletion
To define the groups that have permission to delete the resource filters thereby created.
The groups can be:

- **All groups**: all groups with the right to modify these resource filters can delete the filter that is thereby created.
- **Creator groups**: only groups with the right to create these resource filters can delete the filter that is created.
- **Permission groups**: only groups that have the permission can delete the filter thereby created.

Modification
Define the groups that have permission to modify on the resource filters thereby created.
The groups can be:

- **All groups**: all groups with the right to modify these resource filters can modify the filter that is thereby created.
- **Creator groups**: only groups with the right to create these resource filters can modify the filter that is created.
- **Permission groups**: only groups that have the permission can modify the filter thereby created.

Visibility
Define the groups that have visibility permission on the resource filters thereby created.
The groups can be:

- **All groups**: all groups with the right to create these resource filters can view the filter that is thereby created.
- **Creator groups**: only groups with the right to create resource filters can view the filter that is created.
- **Permission groups**: only groups that have the permission can view the filter thereby created.

Forbid
Check this box to forbid creation of all event export contexts.

In the event of multiple groups or multiple permissions, this option has priority over other permissions.
This means that if it is checked, the forbidding overrides other permissions.

Allow private only
This field is active if the Forbid checkbox above is not checked.
In this case, if the box is checked it makes it possible to create private resource filters.

**Groups**

Define groups that have this permission in the **Groups** tab.

**Modifying resource filters**

![Modification permission](image)

**Name**

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

**Description**

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).
History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

Apply to data

Define a criterion for modifying resource filters.

- If the chosen criterion is **is in**, you must select the list of resource filters,
- If the chosen criterion is **contains, does not contain, starts with, does not start with, ends with** or **does not end with**, you must define the value in the field provided for this purpose.

Selection

This option is visible if the chosen criterion is **is in**. Define the resource filters this permission makes it possible to modify.

Value

This option is visible if the chosen criterion is not **is in**. Type in the criterion verification value.

Groups

Define groups that have this permission in the **Groups** tab.
Deleting resource filters

A deletion permission makes it possible to delete one or more resource filters.

**Name**

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

**Description**

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

**History**

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
Selection
This makes it possible to define the resource filters that can be deleted.

Groups
Define groups that have this permission in the **Groups** tab.

Permissions on the dimensions' resources

Visibility of resources
When you create the permission, you must select the resources' dimension.

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).
History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.
This property is updated automatically.

All headings
Use this checkbox to enable visibility of all headings of the dimension's resources.

Apply to headings
If the previous checkbox is not checked, select the dimension's visible headings.

History
Use this checkbox to make the history of resources on this dimension available or unavailable.

Input conditions
Define the resources this permission makes visible.
To do this you must:
■ either select an existing resource filter for the dimension, from the list,
■ or create a new resource filter for the dimension, personalized for this permission.

If you uncheck “All headings”; and do not select any heading to display, visibility of the first heading in the configuration tree is forced.

Groups
Define groups that have this permission in the Groups tab.

Creating resources
When you create the permission, you must select the resources’ dimension.
You may therefore need to define a creation permission for each dimension.
Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

All headings

Use this checkbox to be able to fill in all the resource headings when creating resources.
Apply to headings
If the previous checkbox is not checked, specify the headings that can be typed in when creating resources.

Mandatory headings
Specify if it is mandatory to type in the headings when creating resources.

All settings
Use this checkbox to select all the resource settings.

Apply to settings
If the previous checkbox is not checked, specify the settings to type in when creating resources.

Forbid for all
Use this checkbox to prevent creation, regardless of the dimension's resource.
This checkbox has priority over all others. When it is checked, the other options are grayed.

In the event of multiple groups or multiple permissions, this option has priority over other permissions.
This means that if it is checked, the forbidding overrides other permissions.

Output condition
Define the required condition of the resources once they have been created.
To do this you must:
■ either select an existing resources filter for the dimension, from the list,
■ or create a new resource filter for the dimension, personalized for this permission.
If the created resource does fulfill the output condition, it cannot be created.

Groups
Define groups that have this permission in the Groups tab.

Modifying resources
When you create the permission, you must select the resources’ dimension.
You may therefore need to define a modification permission for each dimension.

### Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

### Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

### History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

### All headings

Use this checkbox to enable modification of all the resources' headings.
Apply to headings

If the previous checkbox is not checked, define the headings that can be modified on the resources.

Mandatory headings

Define the modifiable headings that it is mandatory to fill in when modifying resources.

All settings

Use this checkbox to select all the resource settings.

Apply to settings

If the previous checkbox is not checked, select the settings that can be modified on the resources.

Forbid for all

Use this checkbox to prevent all modifications for all the dimension's resources.

This checkbox has priority over all others. When it is checked, the other options are grayed.

In the event of multiple groups or multiple permissions, if there is at least one permission which does not forbid any modification, this permission will be taken into account.

Input conditions

Define the condition of the resources that this permission makes it possible to modify.

To do this you must:

- either select an existing resources filter for the dimension, from the list,
- or create a new resource filter for the dimension, personalized for this permission.

Output condition

Define the required condition of the modifiable resources once they have been modified.

To do this you must:

- either select an existing resources filter for the dimension, from the list,
- or create a new resource filter for the dimension, personalized for this permission.

If the modification fulfills the input condition but not the output condition, modification is not possible.
Groups

Define groups that have this permission in the Groups tab.

Deleting resources

A deletion permission makes it possible to delete one or more entities.

Name

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.
This property is updated automatically.

**Forbid for all**

Use this checkbox to prevent any deletion of resources for the defined groups.

In the event of multiple groups or multiple permissions, if there is at least one permission which does not forbid any modification, this permission will be taken into account.

**Input condition**

If the previous checkbox is not checked, this characteristic enables you to define which resources can be deleted, by means of a filter.

Define the required condition of the resources before they are deleted.

To do this you must:

- either select an existing resources filter for the dimension, from the list,
- or create a new resource filter for the dimension, personalized for this permission.

**Groups**

Define groups that have this permission in the **Groups** tab.
Permissions on events

Visibility of events

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.
All headings
Use this checkbox to enable visibility of all the forms’ headings.

Apply to headings
If the previous checkbox is not checked, select the visible forms’ headings.

All items
Use this checkbox to enable visibility of all the valuation items.

Apply to items
If the previous checkbox is not checked, select the valuation items that are visible for these events.

Input conditions
Define the events this permission makes visible.
To do this you must:

- either select an existing events filter, from the list,
- or create a new events filter, personalized for this permission.

History
Use this check box to specify whether or not the user can view the events history.

Groups
Define groups that have this permission in the Groups tab.
Creating events

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

All attributes
Use this checkbox to be able to type in all the events' attributes when creating them.
Apply to attributes
If the previous checkbox is not checked, select the attributes to type in when creating events.

All headings
Use this checkbox to allow input of all the forms' headings when creating events.

Allow change of form
Use this checkbox to define whether a form can be changed when creating an event.

Apply to headings
If the All headings checkbox is not checked, select the form headings that can be typed in when creating events.

All dimensions
Use this checkbox to allow input of all the event's resources when creating events.

Apply to dimensions
If the previous checkbox is not checked, define the resources that can be typed in when creating events.

All items
Use this checkbox to allow input of all the valuation items when creating events.

Allow change of item
Use this checkbox to define whether a valuation item can be changed (addition, deletion of an item) in the scope of the permission.

Apply to items
If the All items checkbox is not checked, select the valuation items whose values can be typed in for these events.

Forbid for all
Use this checkbox to forbid creation of events.

In the event of multiple groups or multiple permissions, this option has priority over other permissions.
This means that if it is checked, the forbidding overrides other permissions.

**Output conditions**

Define the required condition of the events once they have been created.

To do this you must:

- either select an existing events filter, from the list,
- or create a new events filter, personalized for this permission.

**Groups**

Define groups that have this permission in the **Groups** tab.

**Modifying events**

![Modification permission](image)

**Name**

Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.
Description

Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History

This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.

This property is updated automatically.

All attributes

Use this checkbox to indicate if it is possible to modify all the events' attributes.

Apply to attributes

If the previous checkbox is not checked, select the attributes that can be modified on the events that can be modified.

All headings

Use this checkbox to allow modification of all the forms' headings.

Allow change of form

Use this checkbox to define whether a form can be changed within the scope of the permission.

Apply to headings

If the All headings checkbox is not checked, select the form headings that can be modified.

All dimensions

Use this checkbox to allow modification of all the event's resources.

Apply to dimensions

If the previous checkbox is not checked, specify the dimension that can be modified for these events.

All items

Use this checkbox to allow modification of all the valuation items.

Allow change of item

Use this checkbox to define whether a valuation item can be changed (addition, deletion of an item) in the scope of the permission.
Apply to items
If the *All items* checkbox is not checked, select the valuation items whose values can be modified for these events.

Forbid for all
Use this checkbox to prevent all modifications for all the events.

In the event of multiple groups or multiple permissions, if there is at least one permission which does not forbid any modification, this permission will be taken into account.

Input conditions
Define the events this permission makes it possible to modify.

To do this you must:

- either select an existing events filter, from the list,
- or create a new events filter, personalized for this permission.

Output conditions
Define the required condition of the modifiable events once they have been modified.

To do this you must:

- either select an existing events filter, from the list,
- or create a new events filter, personalized for this permission.

Groups
Define groups that have this permission in the **Groups** tab.
Deleting events

A deletion permission makes it possible to delete one or more entities.

Name
Give this permission a name. If you type in a name, it replaces the permission's default name and is visible in the tree on the left.

Description
Give the permission an optional description. This description will be visible in the permission's tooltip (useful especially when there are several permissions of the same type).

History
This indicates the creation date and time and the most recent change to the template, together with the login of the user who made the change.
This property is updated automatically.

Forbid for all
Use this checkbox to prevent any deletion of events for the defined groups.
In the event of multiple groups or multiple permissions, if there is at least one permission which does not forbid any modification, this permission will be taken into account.

**Input condition**

Define the events this permission makes it possible to delete.

To do this you must:

- either select an existing events filter, from the list,
- or create a new events filter, personalized for this permission.

**Groups**

Define groups that have this permission in the **Groups** tab.
Chapter XI. Display of the log

1. DEFINITION

The Log records some of the actions users perform on the tool:

■ during a VISUAL PLANNING session: VISUAL PLANNING Client Log (or Client Log),
■ during an ADMIN CENTER session: ADMIN CENTER Client Log (or Admin Center Client Log),
■ during a day: Server Log

This file may be required by the administrator, on demand from VISUAL PLANNING Technical Support (support@stilog.com).

2. USE

Display of the Client Log

There are 2 ways to access the Client Log file:

■ From the file manager,
■ From VISUAL PLANNING.

From the file manager

Depending on the operating system, the client log files are located:

On Windows XP
C:\Documents and Settings\Loginname\vp5\logs

Where Loginname is the WINDOWS user name

On WINDOWS VISTA or later
C:\Users\Loginname\vp5\logs

Where Loginname is the WINDOWS user name

From the VISUAL PLANNING client

The Client Log is accessed using this menu path Help > About Visual Planning > Click on button corresponding to the Client Log.
The log window is displayed. You can copy-paste the content of this window into a text file or into the Clipboard.

You can then send the log by e-mail.

**Display of the Admin Center Client Log**

The Client Log is accessed from the Help button > About Visual Planning > Click on the button corresponding to the Client Log.

The log window is displayed. You can copy-paste the content of this window into a text file or into the Clipboard.

You can then send the log by e-mail.
Display of the Server Log

The Server Log is only available in the ENTERPRISE version.

There are 3 ways to access the Server Log files:

- From the Admin Center,
- From a web browser,
- From the file manager.

A log file is created every day (several times a day if the server is restarted).

Each file's name is structured as follows: Log_YYYYMMDD.txt or Log_YYYYMMDD(X).txt

Where:

- YYYY represents the year,
- MM represents the month,
- DD represents the date,
- X represents the file number.

A file is created each time the server restarts, and the previous file is logged by adding a number as a suffix. The number increments upwards (the older the file is, the greater the number will be).

You can download and/or delete each server log file.

You can also prohibit access to the logs using the Admin Center General Settings.

From the Admin Center

Click on the Show server logs button.

The following window appears:
You can:

- switch from one log to another by clicking on the required file,
- download the log by clicking on ,
- select/unselect a log file,
- delete all the deleted files by clicking on

**From a web browser**

The Server Log files are accessible at the following address:

http://servername/vplanning/logs

Where *servername* is the name of the machine where VISUAL PLANNING is installed.

The following page is displayed:
You can:

- switch from one log to another by clicking on the required file,
- download the log by clicking on ,
- select/unselect a log file,
- delete all the deleted files by clicking on

From the file manager

The Server Log files are accessible on the server where VISUAL PLANNING installed, at the following address:

C:\stilog\VPServer Enterprise 6\webapps\vplanning\logs
Chapter XII. File storage

1. DEFINITION

VISUAL PLANNING’s default configuration stores all files from attachment headings in "file downloading" in the "documents" directory of the VISUAL PLANNING server. However the storage space for these files can be personalized. They can be stored either:

- On the VISUAL PLANNING server in another directory, or
- On a DropBox, or
- On a Google Drive.

It is not possible to configure several different storage spaces according to the attachment heading. This is because all the "in file downloading" attachment headings will store the files they contain in the same storage space.

If you have already used your attachment headings to store files on the VISUAL PLANNING server, these files will not be automatically transferred to your new storage space. The administrator must transfer the files manually from one space to another so that the user can access them. Any files that have not been transferred to the new storage space will not be accessible for users of the planner.

This functionality is only available with VISUAL PLANNING ENTREPRISE.

2. CONFIGURATION

Storage is configured in the Admin center. Choose "Storage Configuration" in the task bar and choose your storage space.

Click on Storage Configuration "File system.

Type in the storage path for your files on the VISUAL PLANNING server.
DROPBOX

To open your DropBox account, you must first have an e-mail address.

Registration

To register, go to https://www.dropbox.com/register

You can register with a Google account (GMAIL) or any other account.

- For a Google account (GMAIL), choose "Register free with Google"
- For any other type of account, fill in the data input fields on the page (First name / Last name / E-mail / Password), check the box to accept the conditions of use and register.

Downloading DropBox (optional step)

The following page appears:

Downloading of DropBox is optional. It will only be useful if you want to synchronize the content of DropBox with a local directory.

You can then continue or exit.

In either case, registration is now complete.

Creating an application

Type in the following URL: https://www.dropbox.com/developers/apps/create
Click on **Send e-mail for verification** to verify your e-mail address and finalize registration.

In the e-mail you received, click on **Validate your e-mail address**.

The following page appears:

Choose an API.

Choose how the application has access to DropBox.

Give the application a name (e.g. STILOG).

Accept the conditions.
Then click on:

![Create app button]

**Generate the Access Token**

Once the application is created the following page appears.

In the **Generate Access Token** heading, click on **Generate**.

![Application settings page]

The generated key looks like this:
This key must be kept in a safe place.

Enable the storage space in VISUAL PLANNING

Log into the Admin Center and click on Storage configuration "DropBox.

Do a copy/paste of the Access Token obtained in the previous step.

GOOGLE DRIVE

To open your Google Drive account, you must first have a Google address (GMAIL).

Logging into a Google account (GMAIL)

Log into a Google account (GMAIL).
Creating an application

Type in the following URL: https://console.developers.google.com/project.

The project creation page is displayed. Click on **Create a project**:

Click on **Create**.

Type in a project name, modify the ID and then click on **Create**.
Creating a project and a key

The following window opens and the project name is displayed top left.

In the API and services menu, choose IDs.

Click on Select, find the project and click on it.

The following window opens. Click on the OAuth authorization screen tab, enter a Product name (unrestricted text) and click on Save.
The "IDs" tab appears. Click on **Create IDs** then **OAuth client ID**.
Choose **Other**, give the client ID a name (unrestricted text), click on **Create** then **OK** to display the page of IDs.

Click on the button **download icon** to download the "json" file.

The file is download in the downloads directory associated with the browser.
Save this file in a safe place.

Enable the API

Click on Library.

In the search bar, type in Drive then click on Google Drive API.

Enable the API by clicking on Enable.
Enable the storage space in VISUAL PLANNING

Log into the Admin Center and click on **Storage configuration "DropBox."**

Copy/paste the content of the "json" file obtained in step 3.