MEGA Administration-Supervisor

Web Administrator Guide

Bizzdesign

CONTENTS

Contents

Contents

Contents

Contents

ABOUT HOPEX ADMINISTRATION

Hopex Administration is managed via **Administration** (Windows Front-End) application and via **Administration** (Web Front-End) desktop.

The **Administration** application (Windows Front-End) is the **Hopex** administration application accessible from the Windows desktop. This application contains the tools required for management of environments and repositories. It is also used to manage scheduling and data accesses (writing access as well as confidentiality using reading access management).

> ☞ *To perform **Hopex** administration tasks from the **Administration** application (Windows Front-End), see the Hopex Administration - Supervisor guide.*

This guide is for the person responsible for administrating users and repositories from the **Hopex Administration** desktop (Web Front-End).

The **Administration** desktop (Web Front-End) is the **Hopex** Administration application accessible via an internet browser. This application is used to manage users (persons, person groups), and repositories (workspaces, locks, repository health, repository activity, repository snapshots). This application also provides access to tools (Scheduler, Import/Export of command files).

Some actions, like user management, can be performed by functional Administrators from a restricted Administration desktop accessible from other **Hopex** desktops (Web Front-End).

Certain features, like object management are only available with specific technical modules (**Hopex Power Studio** or **Hopex Power Supervisor**). These are indicated by a note.

HOPEX STRUCTURE

Some basic knowledge is required to understand the architecture and operation of **Hopex**.
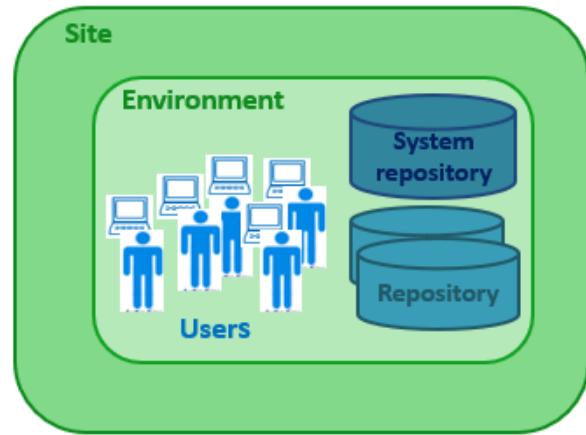
Hopex (Web Front-End) is organized on the following levels:

- **site**

  A site groups together everything that is shared by all **Hopex** users on the same local network: the programs, standard configuration files, online help files, standard shapes, workstation installation programs, and version upgrade programs.

- **environment**

  An environment groups a set of users, the repositories on which they can work, and the system repository. It is where user private workspaces, users, and system data are managed.

- **user**

  A user is a person (or person group) with a login and a profile assigned. A user:

  - has a specific workspace in each repository.
  - has a specific configuration and is authorized to access specific product functions and repositories in the environment.

WEB ADMINISTRATION DESKTOP

The points covered here are:

✓ Introduction to Web Administration Desktop
✓ Web Administration Desktop Description

INTRODUCTION TO WEB ADMINISTRATION DESKTOP

Web Administration Desktop

The Web Administration desktop is the **Hopex** administration application accessible via an internet browser.

This application is used to manage:

- *users*:
  - Persons and person groups,
  - profile assignments,
  - external authentication
  - API Key
- *repositories*:
  - workspaces
  - locks
- *scheduling*
  - jobs
  - Web sites
- *data*
  - import/export (command files, Excel)
  - comparison

This application gives also access to information regarding:

- *repository*
  - repository activity
  - repository snapshots
- *Data access* (with the **Hopex Power Supervisor** technical module)
  - writing access areas
  - reading access areas

Accessing Web Administration Desktop

To perform Administration operations via the Web, you must have connection rights to the Web Administration desktop, that is connect with an administration profile.

☛ *See Administration Profiles Provided.*

☛ *At installation, only the Mega user can connect to the Web Administration desktop.*

To access **Hopex Administration** desktop:

1. Start the **Hopex** application using its HTTP address.

    ☛ *If you do not know this address, contact your administrator.*

    The authentication page appears.
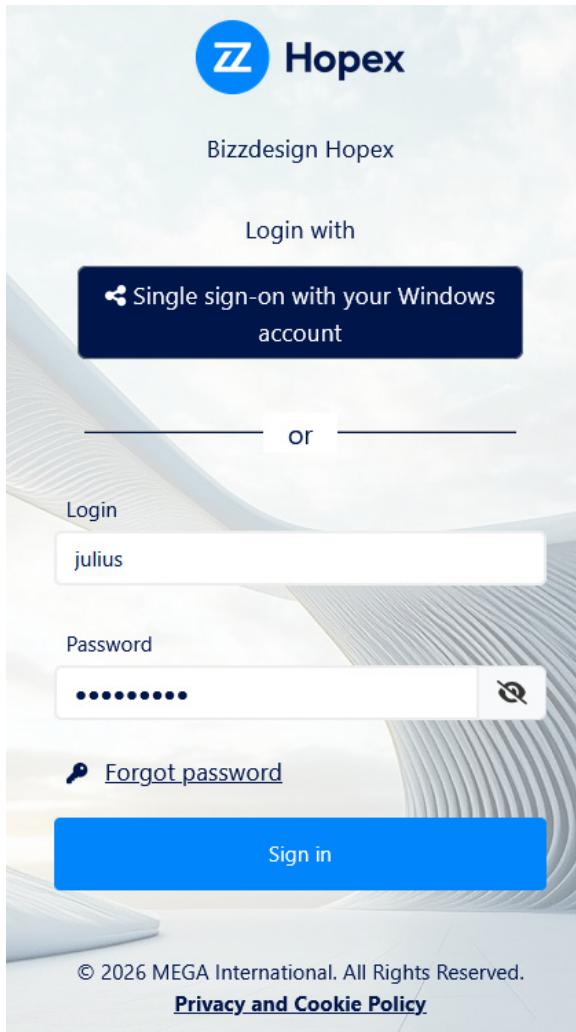
2. Click your own log in button, or use the log in managed by Hopex:
    - in the **Login** field, enter your connection identifier.
    - In the **Password** field, enter your password.

      ☛ *To view your password, click* .

      ☛ *If you have lost your password, click* ***Forgot password***, *see*
      Resetting your Password.
3. Click **Sign in**.
    When you have been authenticated, the connection page appears.

4. (If you belong to a person group) In the drop-down menu for groups, select the group with which you want to connect or "My assignments" to connect with one of your own assignments.

5. in the **Repository** field, use the drop-down list to select your work repository.

> ☛ *If you can access only one repository, this is automatically taken into account and the repository selection field does not appear.*

6. in the **Profile** field, use the drop-down list to select your administration profile:
   - **Hopex Administrator**, for global management of users and repositories.
   - **Hopex Administrator - SaaS** (in Production environment only).
   - **<Solution name> Functional Administrator**, for a management limited to users.

   > ☛ *For information on these profiles, see Administration Profiles Provided.*

   > ☛ *If you have only one (administration) profile, this is automatically taken into account and the profile selection field does not appear.*

7. Click the **Privacy and Cookie Policy** link and read the privacy policy, then select **I have read and accept the privacy policy**.
   The **Enter** button is active.

   > ☛ *When you have read and accepted the confidentiality policy, a certificate is automatically linked to your person and this step is not required anymore.*

Hopex Administration-Supervisor (Web)
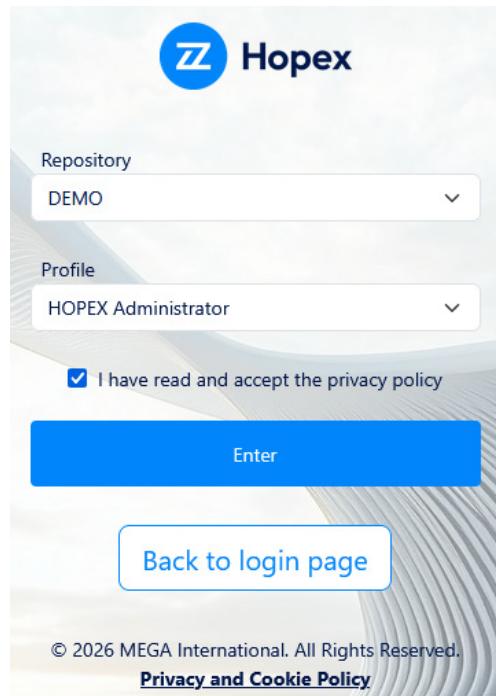
8. Click **Enter**.

☛ *Click **Back to login page** if you want to return to the authentication page.*

The **Administration** desktop appears and the session is opened.

☛ *See Web Administration Desktop Description.*

WEB ADMINISTRATION DESKTOP DESCRIPTION

To access the **Administration** desktop, see Accessing Web Administration Desktop.

The **Administration** desktop includes:
- a toolbar common to all desktops

    ☛ *See Platform - Common Features > Interface Presentation > Toolbar documentation.*

- administration-specific navigation menus, which give access to sub-menus in the browse area

    ☛ *See Navigation Menus.*

- a homepage with a direct access to specific objects
- an edit area to manage the objects.

Navigation Menus

The **Administration** desktop includes the following navigation menus:

- **Users** to manage *users*:
  - *Persons*
    - ☞ The **Persons** submenu gives access to the persons in the browse area, as well as to the persons listed by group, by profile, by writing access area, and by reading access area.
  - *Person groups*
    - ☞ The **Person Groups** submenu gives access to the person groups in the browse area, as well as to the person groups listed by profile, by writing access area, and by reading access area.
  - *Profiles*
    - ☞ The **Profiles** submenu gives access to the profiles in the browse area.
  - *License Dashboard*
  - *External Authentication*
    - ☞ The **External Authentication** submenu gives access to the authentication groups and authentication parameters in the browse area.
  - *API Keys*
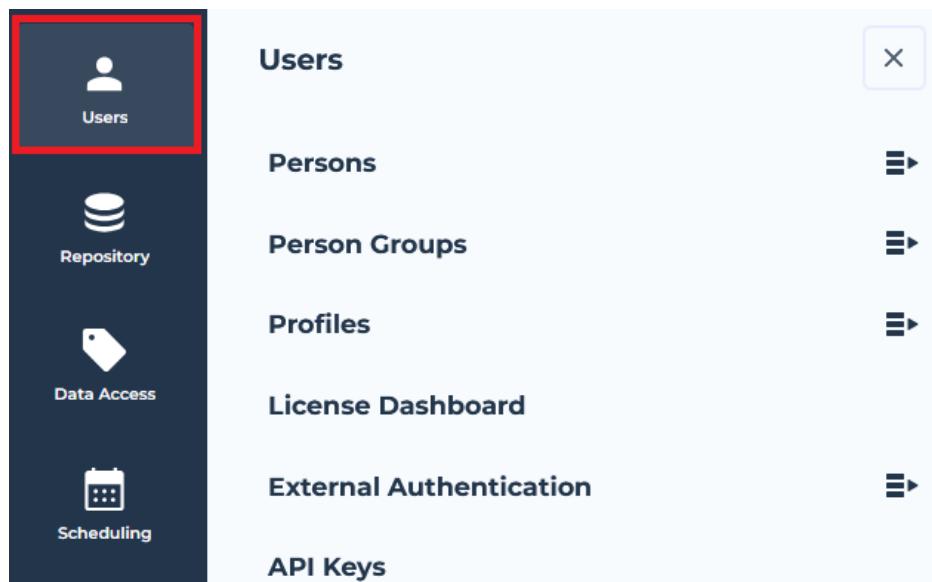
- **Repository** to:
  - manage *Workspaces* and notify by email connected users
  - access *Repository health reports*
  - manage *Locks*
  - access *Repository activity*
    - ☞ The **Repository Activity** submenu gives access to dispatches, displayed as a tree ordered by date, in the browse area.

- manage **_Repository snapshots_**
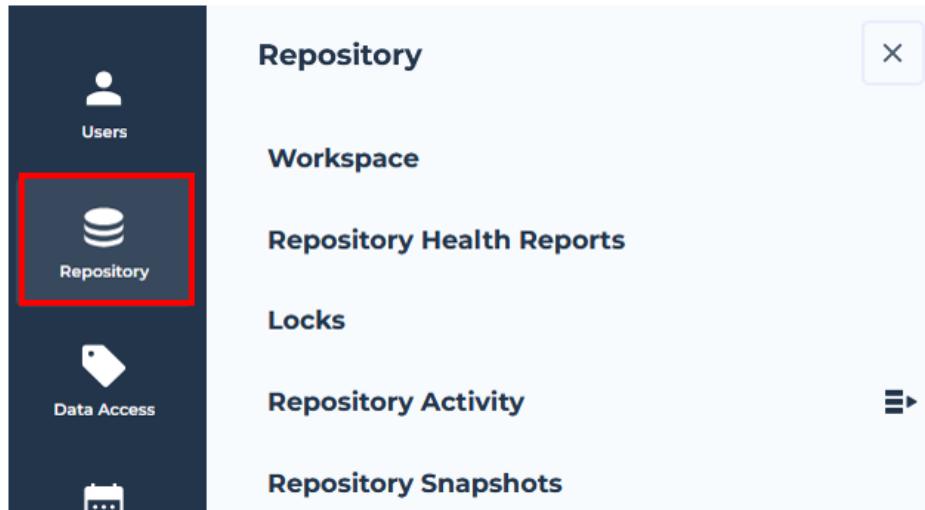
- **Data Access** (with **Hopex Power Supervisor technical module**) to access:
  - writing access areas
  - reading access areas
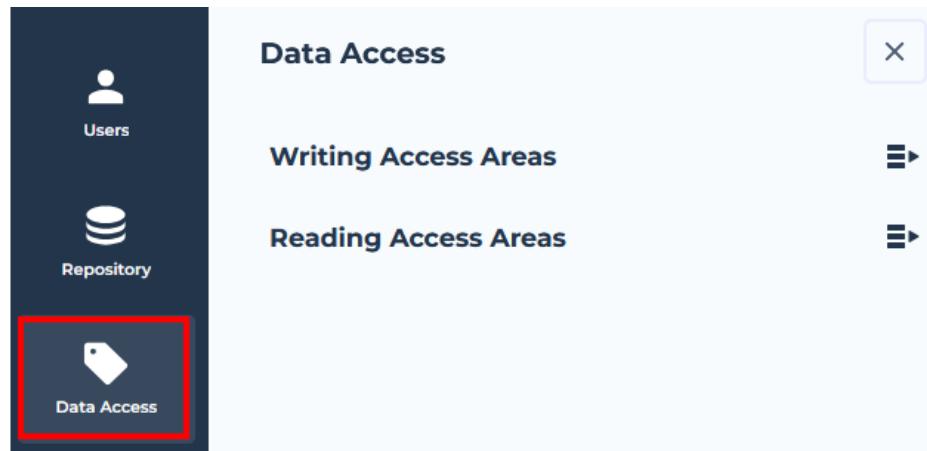
- **Scheduling**, to manage scheduling (Triggers)
  - ☛ *In read-only mode for the **Hopex Administrator - SaaS** profile.*
- **Environment Options**, to manage environment level options

Administration Desktop Homepage

The administration desktop homepage includes indicators useful to manage:

- ***persons***
    - inactive persons
    - active persons with no assigned profile
        - ☛ See *Assigning a Profile to a Person.*
    - active persons with no writing access area
        - ☛ See *Connecting a Person to a Writing Access Area.*
    - locked persons
        - ☛ See *Initializing a User Web Account* or *Defining a Temporary Password to a User.*
    - active persons who have never logged in
        - ☛ See *Preventing a User Connection* and *Deleting a User.*
    - persons whose login is about to be disabled
    - orphan logins
- ***person groups***
    - inactive person groups
    - active person groups with no assigned profile
        - ☛ See *Assigning a Profile to a Person Group.*
    - person groups with no writing access area
        - ☛ See *Connecting a Person Group to a Writing Access Area.*
    - unused active person groups
        - ☛ See *Defining a Person Group.*

It also gives ***direct access*** to inventory lists of:

- persons
- person groups
- profiles
- authentication groups
- authentication parameters
- API keys

My scope

Person Statistics

Refreshed 1 hour ago

10 Inactive Persons

32 Active Persons with no assigned Profile

0 Active Persons with no Writing Access Area

0 Locked Persons

118 Active Persons who have never logged in

0 Persons whose login is about to be disabled

1 Orphan Logins

Person Group Statistics

Refreshed 1 hour ago

0 Inactive Person Groups

0 Active Person Groups with no assigned Profile

0 Person Groups with no Writing Access Area

0 Unused Active Person Groups

Inventory

Refreshed 1 hour ago

883 Persons

0 Person Groups

48 Profiles

0 Authentication Groups

0 Authentication Parameters

0 API Keys

USERS

This chapter details how to create and manage *users*, individually or as a group (*person group*), and how to define and modify their characteristics.

The following points are covered here:

Big Picture

✓   Big Picture: Actions to Define a User

Introduction

✓   Introduction to Profiles
✓   Introduction to Users
✓   Introduction to Person Group Management

Management

✓   Access to User Management
✓   Creating and Managing Users
✓   Creating and Managing a Person Group
✓   Managing Profiles
✓   Managing Named Licenses
✓   Managing User-Related Options
✓   Authentication in Hopex
✓   Mapping
✓   Managing the Password of a Web User
✓   Managing API Keys
✓   Managing Languages
✓   Managing Responsibilities

BIG PICTURE: ACTIONS TO DEFINE A USER

To define a *user*, some actions are compulsory, while others are only necessary depending on **Hopex** options selected, and others are optional.

📖 *A user is a person with a login.*

See:

- Before Defining a User: Profile and Person Group Concepts
- Compulsory Actions to Define a User
- Compulsory Actions to Define a User Group
- Optional Actions to Define a User
- Other Actions to Set or Manage a User
- Checking the Configuration of Users

Before Defining a User: Profile and Person Group Concepts

Before defining a user, identify if the user will be part of a person group or not.

☛ *See Creating a User.*

☛ *See Creating a Person Group.*

To connect to **Hopex** a user selects the profile with which he/she wants to work. If the person belongs to a person group, the person can connect either with:

- a profile assigned to the person, or
- a profile assigned to the person group.

This profile defines:

- the products accessible

💣 **If a user already has restricted access rights to products (see Viewing the Characteristics of a Login), the products accessible to this user are at the intersection of the values of the Command Line attribute of the user login and profile.**

☛ *See Products accessible on the license (Command Line).*

- the desktops to which the user can access

☛ *See Administration Profiles Provided.*

- the UI access rights (permissions) of the user

Assigning a profile to a person defines:

☛ *See Assigning a Profile to a Person.*

- the repository concerned by the assignment
- the repository access rights of the person with this profile assignment
- (optional) the validity period of the assignment

Compulsory Actions to Define a User
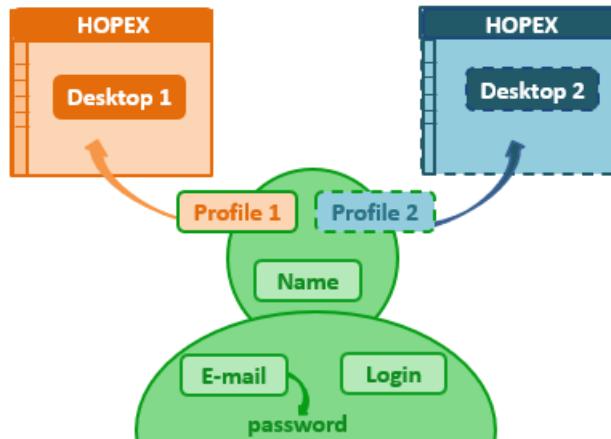
To create a user who can access **Hopex** you must:

- define the ***name*** of the person

    ☛ *See Creating a User.*

- define the ***login*** of the user

    💣 **A person must have a login to be able to connect to Hopex.**

    The login of the user is automatically created at creation of the person (see Creating a User).

    ☛ *If needed, see Creating the Login of a Person.*

    ☛ *The Status (Login) must be active so the person can connect, see Defining the Login of a Person.*

- define the ***e-mail*** address of the person
    The e-mail address is required, for example, for the user to define his/her password, for distributing documents, receiving notifications and questionnaires, or when a user loses his/her password.

    ☛ *See Creating a User or Defining a Person.*

    ☛ *See also Configuring SMTP Settings.*

- assign a ***profile*** to the person

    💣 **To access Hopex, the user must have at least one profile assigned, or must belong to a person group.**

    A person belonging to a person group can log in with a profile assigned to the person group. It is not necessary to assign a profile to this person.

    ☛ *See Assigning a Profile to a Person or Adding persons to a static person group.*

E-mail, password, and SMTP parameters

With the Hopex authentication system (UAS), a user needs a password to log in.

The user defines his/her password on reception of his/her Hopex account activation e-mail. This e-mail includes a link valid for 48 hours.

If the Hopex SMTP settings:
- are configured:

  ☞ *See Configuring SMTP Settings.*

  As soon as the user email is entered, the user automatically receives an e-mail to define his/her password.

  ☞ *To resend the account activation e-mail, see Initializing a User Web Account.*

- are not configured:
  The **Password** field is available at user creation. You must then define this temporary password, that the user has to change at first connection.

If needed (e.g.: troubles with password or e-mail reception), the administrator can define a temporary password for the user.

☞ *See Defining a Temporary Password to a User.*

Compulsory Actions to Define a User Group
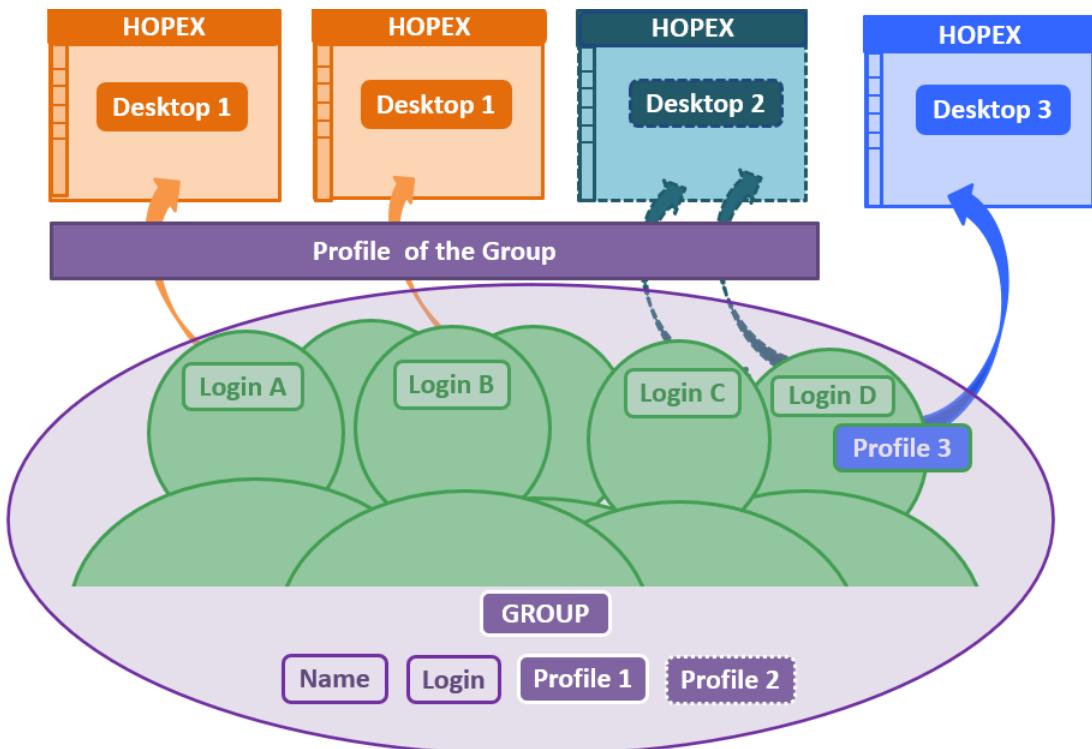
To create a user group and allow the persons belonging to this group to connect to **Hopex** you must:

- define the *name* of the person group

    ☛ *See Creating a Person Group.*

    ☛ *The login of the person group is automatically created at creation of the person group.*

    💣 **The login of the person group is used for configuration purposes only. A person belonging to a group connects with his/her own login.**

    ☛ *See Modifying a Person Group Login.*

- assign a *profile* to the person group

    💣 **The person group must have at least one profile assigned for the persons belonging to the group to connect to Hopex.**

    ☛ *When a person belongs to a person group, the person cumulates the profiles assigned to him/her to the profiles assigned to the person group.*

    ☛ *See Assigning a profile to a person group.*

    ☛ *See Performing of mass profile assignment to person groups.*

See Defining a Person Group.

See also the authentication in the case of a person group, Managing an SSO Authentication Group.

Optional Actions to Define a User

According to the selected options you must:

- (recommended) define the e-mail address of the person

    ☛ *The e-mail address is necessary, for example, for distributing documents, receiving notifications or questionnaires.*

    ☛ *See Defining a Person.*

- (with writing access management activated) define the writing access area of the user

    ☛ *See Defining a Person.*

    ☛ *See Connecting a Person to a Writing Access Area.*

- (with reading access management activated) define the reading access area of the user

    ☛ *See Defining a Person.*

    ☛ *See Connecting a Person to a Reading Access Area.*

- define if the person belongs to a person group

    ☛ *See Defining a Person.*

- assign named licenses to the user

    ☛ *See Assigning Named Licenses.*

Other Actions to Set or Manage a User

You can:

- define the phone number and initials of the person

    ☛ *See Defining a Person.*

- define the data language of the user

    ☛ *See Defining a Person.*

- restrict the user access to certain products

    ☛ *The products accessible to this user are at the intersection of the values of the **Command Line** attribute of the user login and profile.*

    ☛ *See Defining the Login of a Person.*

    ☛ *See Configuring a Profile.*

- modify the user authentication mode

    ☛ *See Defining the Login of a Person.*

- make the user inactive.

    ☛ *See Defining the Login of a Person.*

    ☛ *See Preventing a User Connection.*

Checking the Configuration of Users

You can check the persons who do not comply with all the definition rules.

To check the configuration of users:

1. Access the **Persons** management page.

    ☛ *See Accessing the User Management Pages.*

2. In the person list, select the persons whose configuration you want to check.

    ☛ *If you do not select a person, the check is performed on all the persons.*

3. In the list menu bar, click ⋮ **> Check** ✓ .

Each user for whom the configuration rules are not all compliant is detailed in the report.

Persons		
Persons	Check	
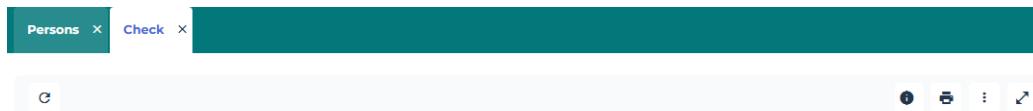
The persons (or person groups) with correct parameters are not displayed in the list.

Persons	Result	Details

Result	Rule Definition	Diagnosis
😐	*Requirement* A person must have a login	*This rule is verified.*
❌	*Requirement* A person must have an e-mail	✕ A person must have a mail
❌	*Requirement* If the person does not belong to a group, the person must have: - at least one profile assigned - a writing access area - a reading access area, if confidentiality (data reading access) is customized.	*- A person must have at least one profile assigned*

Alexander ❌

Result	Rule Definition	Diagnosis
😐	*Requirement* A person must have a login	*This rule is verified.*
😐	*Requirement* A person must have an e-mail	*This rule is verified.*
😐	*Requirement* If the person does not belong to a group, the person must have: - at least one profile assigned - a writing access area - a reading access area, if confidentiality (data reading access) is customized.	*This rule is verified.*

Alex 😐

INTRODUCTION TO PROFILES

Managing users involves managing profiles. A user connects to **Hopex** with a specific profile that determines the **Hopex** application to which the user connects and the desktops with which it is associated.

See:

- Profile Description
- Administration Profiles Provided
- Profile Properties

Profile Description

A profile enables definition of the same connection parameters and rights to a set of users.

☛ *See Viewing Profile Characteristics.*

The description of a profile includes:

- the definition of the profile
- the definition of the profile assignment to a person

☛ *See Profile Properties.*

Profile Definition

A profile defines the function of a person or person group in the enterprise

```
E.g.: EA Functional Administrator, Enterprise Architect
```

☛ *See Viewing Profile Characteristics.*

The profile defines:

- the products accessible

☛ *See Products accessible on the license (Command Line).*

☺ *The command line of each profile is also described in the Concepts > Profiles.*

💣 **If a user already has restricted access rights to products (see Viewing the Characteristics of a Login), the products accessible to this user are at the intersection of the values of the Command Line attribute of the user login and profile.**

- the desktops to which the user can access

☛ *See Profile level.*

- the UI access rights (permissions) of the user
- the same options for all the users connected with this profile

☛ *For detailed information on profiles, see Hopex Studio > Managing Profiles guide.*

Profile assignment

You must assign each person at least one profile so that this person can access **Hopex**.

☞ *By default, no profile is assigned to a person or person group.*

Assigning a profile to a person or a person group defines:
- the repository concerned by the assignment
- the data (reading, writing) access rights of the person with this profile assignment
- (optional) the validity period of the assignment

☞ See *Assigning a Profile to a Person.*

☞ See *Assigning a Profile to a Person Group.*

Administration Profiles Provided

Administration profiles are provided at installation with defined rights and access to applications.

When several users with an Administration profile access **Hopex Administration** desktop at the same time, certain actions, such as user management, are exclusive.

These profiles are dedicated to:
- global Administration (Windows Front-End and Web Front-End), with exclusive access to **Administration** application (Windows Front-End) and to **Hopex Administration** desktop:
  Hopex Administrator

  ☞ See *HOPEX Administrator profile.*

- administration (Web Front-End), with exclusive access to **Hopex Administration** desktop:
  Hopex Administrator - SaaS

  ☞ See *HOPEX Administrator - SaaS profile.*

- functional administration (Web Front-End), with access to the **Hopex Administration** desktop and to Solution-specific features:
  <Solution name> Functional Administrator

  Example: the **GRC Functional Administrator** gives access to the GRC features as well as to person and person group management.

  ☞ See *Functional Administrator profile of a Solution.*

Hopex Administrator profile

☞ *When several users with an Administrator profile connect to HOPEX Administration at the same time, certain actions are exclusive (example: user management).*

In the **Hopex Administration** desktop, the **Hopex Administrator** profile allows, in particular, to manage:

> ☞ *For information on the Hopex Administrator profile in the Administration application (Windows Front-End), see HOPEX Administration guide.*

- *users* (**Persons** and **Logins**)

> ☞ *See Creating and Managing Users.*

- *user groups* (**Person groups** and **Logins**)

> 📖 *A person group groups persons in a group. These persons share the same connection characteristics.*

> ☞ *See Creating and Managing a Person Group.*

- **Authentication**

> ☞ *See Authentication in Hopex.*

It also allows to perform tasks linked to:

- **Repository management**:
  - workspace management

> ☞ *See Repository and Workspaces.*

  - repository activity management

> ☞ *See Managing Updates.*

  - lock management

> ☞ *See Managing locks.*

  - snapshot management

> ☞ *See Managing Repository Snapshots.*

- **Tools** such as:
  - Scheduler

> ☞ *See Scheduling.*

  - XMG/MGL/MGR file import into the data and SystemDb repositories

> ☞ *See Importing a Command File into Hopex.*

> ☞ *See Exporting Objects.*

  - Excel file import/export

> ☞ *See the **Hopex Common Features** guide, "Exchanging Data With Excel" chapter.*

Hopex Administrator - SaaS profile

The **Hopex Administrator - SaaS** profile allows to perform the same actions as the **Hopex Administrator** profile in the **Hopex Administration** desktop with the following restrictions:

- *Importing*
  It does not allow to import metamodel or technical data (i.e: importing data into the SystemDb repository is not allowed).

- *Scheduling*
  It gives read-only access to:
  - **Predefined Triggers** (**Scheduling** page)

    E.g.: modifying a predefined Trigger scheduling is not allowed.

    ☛ *Defining and modifying customized Triggers as well as generating Web Site is possible.*
  - **Scheduler** page

    E.g.: Stopping/Starting the scheduler is not allowed.

- *Profiles*
  It gives read-only access to profiles.

Functional Administrator profile of a Solution

A **<Solution name> Functional Administrator** gives access to some **Hopex Administration** desktop features and to the Solution-specific features.

Example: the **GRC Functional Administrator** gives access to the GRC features as well as to person and person group management.

From an administration point of view, the **<Solution name> Functional Administrator** profile allows, in particular, to manage **Persons** and **Person groups**. It allows to perform, in particular, the following actions:

- managing a *user*
  - initializing a user account
    - ☞ *See Initializing a User Web Account.*
  - inactivating a user
    - ☞ *See Defining the Login of a Person.*
  - defining a default library
    - ☞ *See Defining a Person.*
- creating and managing a **Person Group**
  - ☞ *See Creating and Managing a Person Group.*
- managing **profile** assignments
  A Functional Administrator of a Solution, can only assign profiles related to this Solution, except the Functional administrator profile of the Solution (its **Administrator profile** value is "No").
  See Managing Profiles.
- managing responsibilities:
  - assignment transfer (profile and/or objects)
  - assignment duplication (profile and/or objects)
    - ☞ *See Managing Responsibilities.*

A **<Solution name> Functional Administrator** profiles can also customize the desktop of their Solutions. This profile can in particular:

- **Overview** property **page** of an object:
  - define the report or diagram displayed by default
- **Homepage**:
  - define the content of "My priorities" and "Need Help" headers
  - define the default report
- **Dendrogram** type instant report:
  - add the report to the **Reporting** property page of the source object concerned
  - save the report as a report template

Profile Properties

A profile enables definition of the same connection parameters and rights to a set of users.

☞ *See Profile Description.*

☞ *To assign a profile to a person or a person group, see Assigning a Profile to a Person and Assigning a Profile to a Person Group.*

☞ *For a complete description of profiles, see Hopex Studio > Managaging Profiles documentation.*

Name

The **Name** of a profile can comprise letters, figures and/or special characters.

Profile status

The **Profile Status** attribute is used to define the profile as inactive if necessary.

Only the profiles with "active" status can be assigned. An "inactive" profile does not allow to connect to **Hopex**.

Administrator profile

💣 **For security reasons, Hopex Customizer cannot modify this field. It is restricted to Hopex Administrator profile.**

The **Administrator Profile** attribute enables to differentiate the administration profiles.

- "Yes" authorizes a user connected with the current profile to:
  - assign the administrator profile to another user.
  - declare a profile as administrator.

  That is, set the **Administrator Profile** attribute value of any profile to "Yes".
- "Functional" defines a functional administration profile.

  ☛ *See Functional Administrator profile of a Solution.*
- "No" is the default value.

Products accessible on the license (Command Line)

☺ *The command line of each profile is also described in the online documentation: **Concepts > Profiles**.*

The **Command Line** field enables definition of products that can be accessed by users with the current profile.

Format of the command is:

/RW'<accessible Product A code>;<accessible Product B code>;<...>'

For example: you have licenses for products **Hopex Business Process Analysis, Hopex IT Portfolio Management** and other **Hopex** products. To authorize only **Hopex Business Process Analysis** and **Hopex IT Portfolio Management** modules to users that have this profile, enter:

/RW'HBPA;APM'

☛ *To know the product code, see the online documentation: **Concepts > Products**.*

💣 **If a user already has access rights restricted by the *Command Line* attribute on his/her Login (see Viewing the Characteristics of a Login), the products accessible to this user**

are at the intersection of values of the **Command Line** attribute of the user login and profile.

	Profile 1	Profile 2
Command line	**/RW'APM'**	**none**
User A	/RW'APM;HBPA'	user A has access to **Hopex IT Portfolio Management**	user A has access to: **Hopex IT Portfolio Management** and **Hopex Business Process Analysis**
User B	/RW'HBPA'	user B cannot access any product	user B has access to **Hopex Business Process Analysis**
User C	none	user C has access to **Hopex IT Portfolio Management**	user C can access all of the products for which he has the license (**Hopex IT Portfolio Management** and **Hopex Business Process Analysis**)

Restrictions on products for users and profiles that have licenses for Hopex IT Portfolio Management and Hopex Business Process Analysis.

Description

The **Description** field is used to describe the profile.

Persons and Person Groups

The **Persons** and **Person Groups** pages list all the persons or person groups to whom the current profile is assigned.

INTRODUCTION TO USERS

☛ *Only a user with Administrator type profile has management rights. In particular, he/she is the only user who can modify user characteristics.*

User management involves the following concepts:

- *users*:

  📖 *A user is a person with a login.*

  - *persons*

    📖 *A person is defined by his/her name and e-mail.*

  - *logins*

    📖 *A Login uniquely defines a user or user group. It can be assigned to only one Person or Person Group.*

- *profiles*

    📖 *A profile defines what a person can see or not see and do or not do in the tools, and how the person sees the tools and can use them. The profile defines options, access rights to repositories and products, read/write and read-only rights on objects.*

Instead of managing each user individually, to facilitate their configuration, you can manage users by *person group*.

☛ See *Introduction to Person Group Management.*

The following points are detailed here:

- introduction:
  - Users Provided
  - User: Definition
- properties:
  - Person Properties
  - Login Properties (Person)

See also:

- access:
  - Accessing the User Management Pages
- characteristics:
  - Viewing the Characteristics of a Person
  - Viewing the Characteristics of a Login

Users Provided

By default, at installation the environment includes:

- persons indispensable to the system:
  - **Administrator** person, with login "System" and password "Hopex"

    ☛ *The "Administrator" user cannot be deleted. It has no profile (it has all rights).*

  - **MEGA Agent**, with login "SysMA"

    ☛ *The "MEGA Agent" user cannot be deleted. The "MEGA Agent" user is used by the system to manage workflows. It has no profile (it has all rights).*

- a person given as example:
  - **Mega**, with login "Mega" and password "Hopex"

    ☛ *The "Mega" user can be deleted (not recommended).*

    The "Mega" user has the "Hopex Administrator" profile, which allows to create a first user with the "Hopex Administrator" profile to manage repositories and users.

User: Definition

For each environment, a user has:

- personal characteristics defined by his/her **Person**.

  ☛ *see Viewing the Characteristics of a Person.*

- a **login** which defines his/her connection identifier, status, and authentication **Hopex** mode. The login can also restrict the accessible products.

  ☛ *see Login Properties (Person).*

- a **user code** which enables naming of user associated files, for example the work repository.

  ☛ *see Login Properties (Person).*

- at least one assigned **profile**, which determines the products (restricted by the products defined for the user login), applications, desktops, and repositories to which the user has access as well the access rights to UIs (permissions).
  By default the user does not have an assigned profile.

  ☛ *see Profile Properties.*

  ☛ *see Assigning a Profile to a Person.*

- **options**

  ☛ *see Options.*

Only a user with an Administrator profile (Administration Profiles Provided or profiles with equivalent rights) can configure and modify user properties.

  ☛ *see Administration Profiles Provided.*

Person Properties

☛ *To consult the properties of a person, see Viewing the Characteristics of a Person.*

☛ *To define the properties of a person, see Defining a Person.*

Personal characteristics
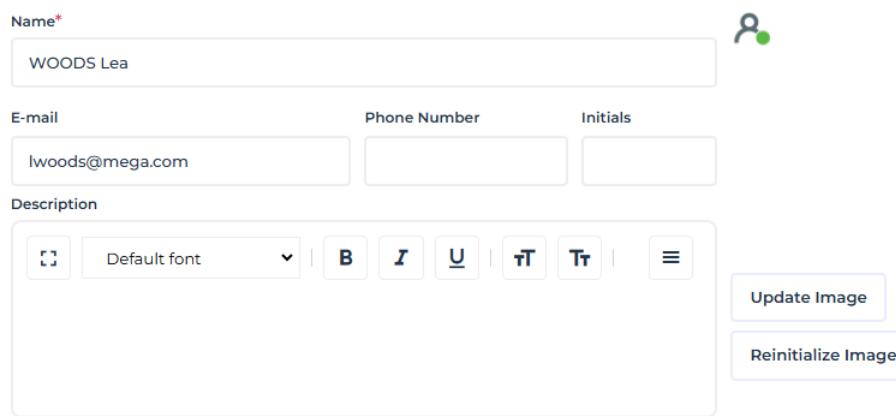
Name*

WOODS Lea

E-mail | Phone Number | Initials

lwoods@mega.com

Description

Update Image

Reinitialize Image

Name

The name of the person can include name and first name. It can comprise letters, figures and/or special characters. Format of the name of the person is free. It is recommended that the same format be used for all persons.

E.g.: DURAND Pierre

Image

You can download an image in .ico, .bmp, .gif or .png format up to a size of 30 MB.

E-mail

The e-mail address of the person is required, for example, for the user to define his/her password, for distributing documents, receiving notifications and questionnaires, or when a user loses his/her password.

Example: pdurand@mega.com

Phone number and initials

The phone number and initials of the person are optional.

E.g.: +33102030405 / DP

Description

This text field is free and optional.

Application Access

The user access to the application is defined by his/her **Login**.

If the user connects as a group, his/her access is defined by the information of the login of the group.

Belongs to a Person Group

A person can:

- belong to a group

  ☞ *See Creating a Person Group.*

- have the **Belongs to a person group** attribute selected
  When the person has the "Belongs to a person group" attribute selected, the person belongs to a dynamic group (SSO group).

  ☞ *See Defining a dynamic person group (SSO).*

  When the person has the "Belongs to a person group" attribute selected, but the person is not listed in a person group, this means that the person is not directly connected to a group or does not belong to a dynamic group (SSO group): the person belongs to the default group.

  ☞ *See Default connection group.*

  When you select the **Belongs to a person group** attribute, the person can connect to the application with one of the profiles defined for the group or with one of the profiles assigned to him/her.

Login

☞ *See Login Properties (Person).*

It is defined by the following parameters:

- **User code**
- **Command Line**
- **Status (Login)**
- **Last Connection Date**
- **Authentication Mode** (case of authentication managed within Hopex)

Data access

Data Language

The **Data Language** attribute of the person enables to define a specific data language for this user. It is the language in which data names are displayed by default, in case several languages are available.

> ☛ *By default, the data language is defined at installation in the environment options for all users (**Options>Installation>Languages**) with the **Data language** option.*

Default library

The **Default Library** attribute enables attachment of objects created by the person in a library, when the creation context does not permit this.

Person reading access area and reading access area at creation

> ☛ *Information related to the reading access area is only visible when the **Activate reading access diagram** option is selected in the **Environment Options** (**Compatibility > Windows Front-End > Administration**).*

Certain objects or modeling projects may be confidential or contain data (costs, risks, controls) that should be visible only to authorized users.

The **Hopex** administrator can hide objects corresponding to this confidential data.

To implement a data confidentiality policy, objects must be organized in distinct sets. Each set of objects constitutes a *reading access area*.

Each user is associated with a reading access area that determines objects the user can see. A user can only see objects located in his/her own reading access area or in the lower reading access areas.

Writing access area and writing access area at creation

> ☛ *Writing access management is available with the **Hopex Power Supervisor** technical module.*

A writing access area is assigned to an object to protect it from inadvertent modifications. At creation, an object takes the writing access area of the user that creates it.

By default, a new user is connected to the only writing access area: "Administrator".

There is a hierarchical link between writing access areas: a user can only modify an object when he/she has the same writing access level as this object or a higher writing access area level.

Person Groups

A person can belong to one or more person groups. The person can thus connect to the application as a group with one of the profiles assigned to the group.

The groups to which the person belong are listed here.

Assignments - Profile Assignments

To connect to **Hopex**, a person must have at least one profile assigned. The profile determines:

- the objects and tools the person can access
- the desktops the person can access
- the repository access
- the product access

☞ See *Profile Description*.

☞ See *Assigning a Profile to a Person* and *Assigning a Profile to a Person Group*.

Login Properties (Person)

To:
- create the login of a person, see Creating a User or Creating the Login of a Person.
- view the login characteristics, see Viewing the Characteristics of a Login.
- configure the login of a person, see or Defining the Login of a Person.

User code

The **User Code** is the short identifier of the user that serves as the basis for private workspace naming.

This code is automatically defined on user creation (upper case, 16 alphanumerical characters). To ensure data consistency, it should not be modified.

```
E.g.: D312DF9467BD6312
```

Login holder

The **Login Holder** is the person associated with the login.

```
E.g.: WOODS Laura
```

Status (Login)

Login **status** can be used to make a user inactive (value: Inactive). The user no longer has access to repositories, but trace of his/her actions is retained. The user can be easily reactivated (value: Active).

💣 **When you delete a user from the repository, the commands connected to this user become orphans and you lose part of the history saved in logs. With Inactive status, the user no longer has access to repositories, but the history of commands connected to the user is kept in logs.**

Last connection date

The **last connection date** indicates the last time the user accessed Hopex.

Products accessible on the license (Command Line)

The **Command Line** field enables restriction of access of a user or profile to available products.

☞ *For more details, see Products accessible on the license (Command Line).*

💣 **If a user is connected to a profile, and both the user and profile have access to products restricted by the Command Line attribute, the products accessible to the user are the intersection of the values of the Command Line attribute of the user and profile.**

Authentication mode (case of authentication managed within Hopex)

☞ *See Choosing an Authentication Mode.*

The user authentication is performed by checking the user password. Authentication modes managed within Hopex are:

- **MEGA** (default value)
  The Hopex authentication service checks that the password entered matches the (hashed and encrypted) password stored in Hopex repository.

- **HAS UAS**
  Password management is delegated to the UAS application of HAS. In this configuration the user cannot connect to Hopex (Windows Front-End).

INTRODUCTION TO PERSON GROUP MANAGEMENT

☞ *Only a user with Administrator type profile has administration rights. In particular, he/she is the only user who can modify user characteristics.*

Person group management involves the following concepts:

- *users:*

  📖 *A user is a person with a login.*

  - *persons*

    📖 *A person is defined by his/her name and e-mail.*

  - *person groups*

    📖 *A person group groups persons in a group. These persons share the same connection characteristics.*

  - *logins*

    📖 *A Login uniquely defines a user or user group. It can be assigned to only one Person or Person Group.*

- *profiles*

  📖 *A profile defines what a person can see or not see and do or not do in the tools, and how the person sees the tools and can use them. The profile defines options, access rights to repositories and products, read/write and read-only rights on objects.*

The following points are covered here:

- introduction:
  - Managing Person Groups Rather than Persons
  - Belonging to a Person Group
- properties:
  - Person Group Properties
  - Login Properties (Person Group)

See also:

- access:
  - Accessing the User Management Pages
- characteristics:
  - Viewing the Characteristics of a Person Group
  - Viewing the Characteristics of a Login

Managing Person Groups Rather than Persons

To facilitate person management, instead of managing persons individually, you can manage them by person group.

        Example: the group of auditors.

Configuration does not take place at the person level but at the group level.

Persons belonging to a group:
- depend on the same environment.
- share the same connection characteristics defined by the **profile** of the group and its assignment.

    ☛ *see Before Defining a User: Profile and Person Group Concepts.*

    ☛ *see Profile Description.*

- connect to the application with their **login**.
- share the assignments defined for the group.

    ☛ *See Assigning a Profile to a Person Group.*

- share the characteristics defined for the group (e.g.: access rights, data language).

    ☛ *see Person Group Properties.*

    ☛ *see Login Properties (Person Group).*

    ✹ **When a person belongs to a person group, the person cumulates the profiles assigned to him/her to the profiles assigned to the person groups she/he belongs to. The person connects as a group or via his/her own profile assignments (defined on his/her person).**

A person can belong to one or more groups.

You can:
- connect a person to a person group, individually, directly at creation of the person.

    ☛ *See Creating a User.*

- connect multiple persons to a person group simultaneously:

    ☛ *See Adding persons to a static person group.*

Belonging to a Person Group

A person can:
- belong to a group

    ☛ *See Creating a User.*

    ☛ *See Creating a Person Group.*

    ☛ *See Adding persons to a static person group.*

- have the **Belongs to a person group** attribute selected

    ☛ *See Belongs to a Person Group.*

    When the person has the "Belongs to a person group" attribute selected, the person belongs to a dynamic group (SSO group).

    ☛ *See Defining a dynamic person group (SSO).*

    When the person has the "Belongs to a person group" attribute selected, but the person is not listed in a person group, this means that the person is not directly connected to a group or does not belong to a dynamic group (SSO group): the person belongs to the default group.

    ☛ *See Default connection group.*

A person who belongs to a person group or who has the **Belongs to a person group** attribute selected, can connect to the application through the group, with one of the profiles assigned to the group.

> ☛ *The person cumulates the profiles assigned to him/her to the profiles assigned to the person group he/she belongs to.*

Person Group Properties

> ☛ *For information on a person group, see:*
>
> *Managing Person Groups Rather than Persons,*
> *Viewing the Characteristics of a Person Group, and*
> *Modifying a Person Group Login.*

Personal characteristics

Name

The name of the person group can comprise letters, figures and/or special characters.

        E.g.: HR Department

Description

This text field is free and optional.

Application access

Authentication Group

A person can belong to:

- a static group
  Persons are explicitly connected to the group.

  > ☛ *See Defining a Person Group.*

- a dynamic group
  The group computes the persons of the group on the fly.

  > ☛ *See Connection request and user created on the fly.*

  E.g.: SSO type groups (SSO authentication case) are characterized by claims.

  > ☛ *See Defining a dynamic person group (SSO).*

Default connection group

When the **Default connection group** attribute is selected, any person who has not a direct link with a specific group but with the "Belongs to a person group" attribute selected, belongs to the default connection group.

> ☛ *Use of this attribute in read-only mode is recommended.*

> ☛ *See Defining a default connection group.*

Login

The login of a person group is a unique character string uniquely identifying the person group. It enables to make the group inactive.

☛ *See Login Properties (Person Group).*

💣 **A person belonging to a group connects to the application with his/her own login.**

It is defined by the following parameters:

- **User Code**
- **Command Line**
- **Status (Login)**
- **Authentication Mode** (case of authentication managed within Hopex)

Data access

Data Language

The **Data language** attribute of the person group is used to define a specific data language for this user group.

☛ *By default, the data language is defined at installation in the environment options for all users (**Options>Installation>Languages**) with the **Data language** option.*

Person group writing access area and writing access area at creation

☛ *Writing access management is available only with the **Hopex Power Supervisor** technical module.*

A writing access area is a tag attached to an object to protect it from unwanted modifications. At creation, an object takes the writing access area of the group to which the user creating it belongs.

There is a hierarchical link between writing access areas: a user can only modify an object when he/she has the same writing access level as this object or a higher writing access area level.

Person group reading access area and reading access area at creation

☛ *Information related to the reading access area is only visible when the **Activate reading access diagram** option is selected in the **Environment Options** (**Compatibility > Windows Front-End > Administration**).*

Certain objects or modeling projects may be confidential or contain data (costs, risks, controls) that should be visible only to authorized users.

The **Hopex** administrator can hide objects corresponding to this confidential data.

To implement a data confidentiality policy, objects must be organized in distinct sets. Each set of objects constitutes a *reading access area*.

Each person group is associated with a reading access area that determines the objects the person group can see. A user can only see objects located in the reading access area of the group or in the lower reading access areas.

Persons

A person group is defined by a list of persons belonging to the same group.

Profile assignments

💣 **To be able to connect to Hopex the user must have at least one profile.**

By default, no profile is assigned to the person group; you must assign at least one profile to the person group.

The profile determines the following for the person group:

- the desktops accessible
- access to repositories
- the products accessible
- the objects and tools accessible

☛ *See Profile Description.*

The profile assignment defines:

- the repository concerned by the assignment
- the access rights to the repositories with this profile assignment
- (optional) the validity period of the assignment

☛ *See Assigning a Profile to a Person Group.*

Login Properties (Person Group)

The login of a person group is automatically created at creation of the person group.

To:

- create a person group, see Creating a Person Group.
- view login characteristics, see Viewing the Characteristics of a Login.
- define the login of a person group, see Modifying a Person Group Login.

User code

The **User Code** is the short identifier (upper case, maximum length 6 characters) of the person group.

This code is automatically defined at creation of the person group.

        E.g.: SUPPOR

Login Holder

The **Login Holder** is the person group associated with the login.

        E.g.: Support France

Inactive person group (Status)

Login status can be used to make a person group inactive (value: Inactive). Users belonging to the person group can no longer have access to repositories through the person group, but trace of their actions are retained. The person group can be easily reactivated (value: Active).

💣 **When you delete a person group from the repository, the commands connected to the users belonging to the person group are kept as long as the users are not deleted.**

Command line

The **Command Line** field is of no use for a person group.

ACCESS TO USER MANAGEMENT

See:

- • Accessing the User Management Pages.
- • Viewing the Characteristics of a Person.
- • Viewing the Characteristics of a Person Group.
- • Viewing the Characteristics of a Login.

Accessing the User Management Pages

To manage users:

1. Connect to the **Hopex Administration** desktop.

   ☞ *See Accessing Web Administration Desktop.*

2. Click the **Users** navigation menu.
   The user management submenus appear.
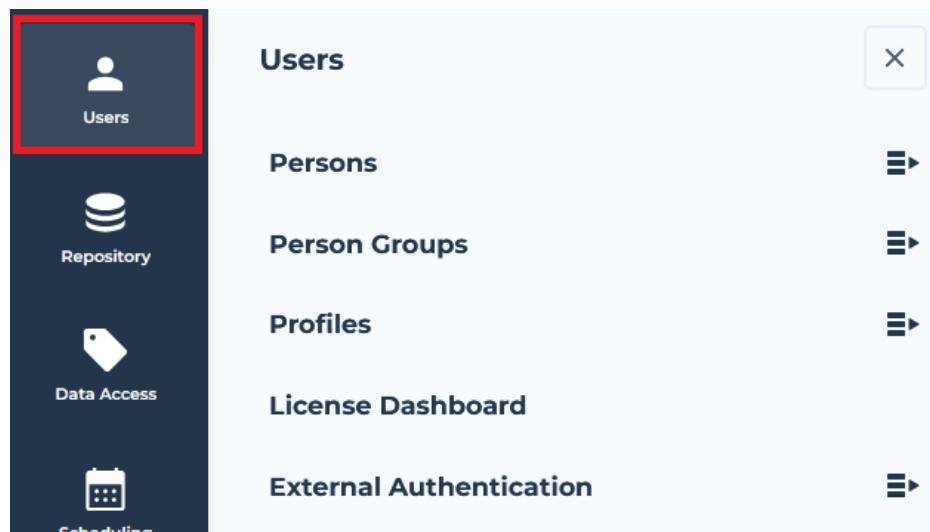
3. For a direct access, click:
- **Persons** to manage persons and logins
  - ☛ *See Actions performed in the Persons management page.*
  - ☺ *Direct access from the homepage: in **Inventory**, click **Persons** indicator.*
- **Person Groups** to manage the persons belonging to the same person group
  - ☛ *See Actions performed in the Person Group page.*
  - ☺ *Direct access from the homepage: in **Inventory**, click **Person Groups** indicator.*
- **Profiles** to access profiles
  - ☛ *See Profile Properties.*
  - ☛ *To manage profiles, see Managing Profiles.*
  - ☺ *Direct access from the homepage: in **Inventory**, click **Profiles** indicator.*
- **External Authentication** to manage authentication (e.g.: authentication groups and parameters).
  - ☛ *See Configuring SSO Authentication.*
  - ☺ *Direct access from the homepage: in **Inventory**, click **Authentication Groups** or **Authentication Parameters** indicator.*
- **API Keys** to manage user API keys
  - ☛ *See Managing API Keys.*
  - ☺ *Direct access from the homepage: in **Inventory**, click **API Keys** indicator.*

The management page selected appears.

See:
- Managing persons with identical characteristic
- Managing a person group with a specific characteristic
- Actions performed in the Persons management page
- Actions performed in the Person Group page

Managing persons with identical characteristic

To manage persons who have an identical characteristic, see:
- Accessing the list of persons who have a specific profile assigned
- Accessing the list of persons belonging to a specific group
- Accessing the list of persons with or without login

with the **Hopex Power Supervisor** technical module:
- Accessing the list of persons connected to a specific writing access area
- Accessing the list of persons connected to a specific reading access area

Managing a person group with a specific characteristic

To manage persons who have a specific characteristic, see:
- Accessing a person group with a specific profile

with the **Hopex Power Supervisor** technical module

- Accessing the list of person groups connected to a specific writing access area
- Accessing the list of person groups connected to a specific reading access area

Actions performed in the Persons management page

The **Persons** management page enables to:

- *configure a user*
  - Creating a User
  - Defining a Person
  - Creating the Login of a Person
  - Defining the Login of a Person
  - Modifying options at user level
  - Connecting a Person to a Writing Access Area
  - Connecting a Person to a Reading Access Area
  - Checking the Configuration of Users
- *manage users*
  - Managing the Password of a Web User
  - Deleting a User
  - Modifying the Properties of a User
- *manage person profile assignments*
  - Assigning a profile to a person
  - Performing a mass profile assignment to persons
  - Transferring Responsibilities to a Person
  - Duplicating Responsibilities of a Person
- *manage user licenses*
  - Managing Named Licenses

Tips to access persons:

- access a person by his/her name

  ☛ *Accessing a person using his/her name*

- filter the person list

  ☛ *See Accessing the list of persons with or without login or Accessing a person using his/her name.*

Actions performed in the Person Group page
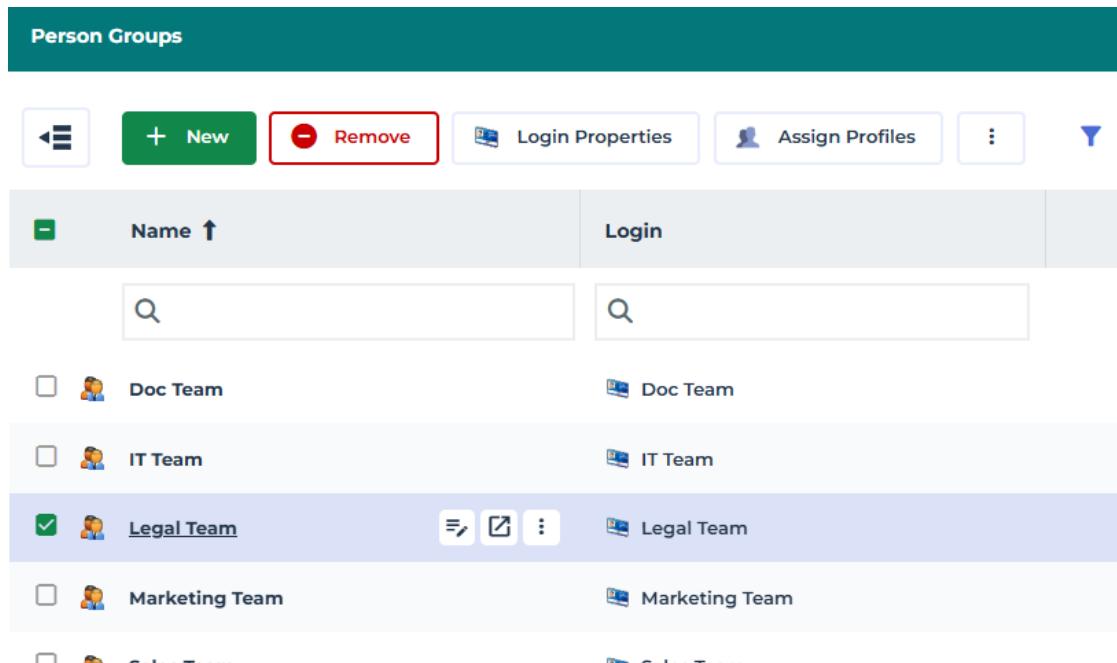
In the **Person Groups** management page you can:

- create user groups

  ☞ *See Creating a Person Group.*

- define the characteristics of a person group

  ☞ *See Defining a Person Group.*

- configure the characteristics of a login

  ☞ *See Modifying a Person Group Login.*

- assign a profile to a person group

  ☞ *See Assigning a Profile to a Person Group.*

- connect a person group to a writing access area

  ☞ *See Connecting a Person Group to a Writing Access Area.*

- connect a person group to a reading area access

  ☞ *See Connecting a Person Group to a Reading Access Area.*

- delete a person group

  ☞ *See Deleting a Person Group.*

- modify a user group properties

  ☞ *See Modifying a User Group Properties.*

Accessing the list of persons who have a specific profile assigned

You can list and manage all persons who have the same profile assigned.

To access the list of persons who have a specific profile assigned:

1. Access the **User** management pages.

    ☞ *See Accessing the User Management Pages.*

2. Click **Persons** ▤▸ then select **By Profile**.
3. (To display the persons only) In the tree, click the ➕ of the profile.
    The persons to whom the profile is assigned are displayed.
4. (To display the persons as a list) Select the profile.
    In the edit area, in the **Characteristics** page, the **Assignments** section lists the person groups (and persons) to which the selected profile is assigned.

Accessing the list of persons belonging to a specific group

You can list and manage all persons belonging to a same group.

To access the list of persons belonging to a specific group:

1. Access the **User** management pages.

    ☞ *See Accessing the User Management Pages.*

2. Click **Persons** ▤▸ then select **By Group**.
3. In the tree, click the ➕ of the group.
    The persons belonging to this group are displayed.

4. (To display the persons as a list) Select the group.
In the edit area, in the **Characteristics** page, the **Persons** section lists the persons belonging to this group.

In case of SSO groups, the list of persons may be long. Click **Calculated** to display, in the **Persons** section, the list of persons belonging to this group.

Accessing the list of persons connected to a specific writing access area

☛ *With the **Hopex Power Supervisor** technical module.*

When several writing access areas are defined, you can list and manage all the members (persons and person groups) of a specific writing access area.

To access the list of members of a specific writing access area:

1. Access the **User** management pages.

☛ *See Accessing the User Management Pages.*

2. Click **Persons** ⊟▸ then select **By writing access area**.
3. (To display the persons only) In the tree, click the ⊞ of the writing access area selected.
The persons connected to the writing access area are displayed.
4. Select the writing access area.
In the edit area, in the **Characteristics** page, the **Access area members** section lists all the persons and person groups connected to the writing access area selected.

Accessing the list of persons connected to a specific reading access area

☛ *With the **Hopex Power Supervisor** technical module.*

When management of reading access areas is activated, you can list and manage all the members (persons and person groups) of a specific reading access area.

To access the list of members of a specific reading access area:

1. Access the **Users** management pages.

☛ *See Accessing the User Management Pages.*

2. Click **Persons** ⊟▸ then select **By reading access area**.
3. (To display the persons only) In the tree, click the ⊞ of the reading access area concerned.
The persons connected to the reading access area are displayed.
4. Select the reading access area.
In the edit area, in the **Characteristics** page, the **Access area members** section lists all the persons and person groups connected to the reading access area selected.

Accessing the list of persons with or without login

You can filter persons according to their login.

To display the persons with or without login:

1. Access the **Persons** management pages.

    ☛ *See Accessing the User Management Pages.*

2. In the **Login** column field, click the filtering operator then select:

    - **Show non empty values only** ●
    The persons who have a login are listed.

    - **Show empty values only** ○
    The persons who do not have a login are listed.

    ☛ *See Actions performed in the Persons management page.*

Accessing a person using his/her name

You can filter the persons according to their name:

- in the edit area
- in the browse area

To find a person by name (edit area):

1. Access the **Users** management pages.

    ☛ *See Accessing the User Management Pages.*

2. In the **Name** column field, enter the name of the person.
    The list of persons narrows down as you enter characters.

    ☛ *See Actions performed in the Persons management page.*

To find a person by name (browse area):

1. Access the **Users** management pages.

    ☛ *See Accessing the User Management Pages.*

2. Click **Persons** ▤▶.
3. In the search field, enter the name of the person.
    The list of persons narrows down as you enter characters.

Accessing a person group with a specific profile

To access a group of persons connected to a specific profile:

1. Access the **Users** management pages.

    ☛ *See Accessing the User Management Pages.*

2. Click **Person Groups** ▤▶ then select **By Profile**.
3. (To display the person groups only) In the tree, click the ➕ of the profile.
    The person groups to which the profile is assigned are displayed.
4. (To display the person groups as a list) Select the profile.
    In the edit area, in the **Characteristics** page, the **Assignments** section lists the person groups (and persons) to which the selected profile is assigned.

Accessing the list of person groups connected to a specific writing access area

☛ *With the **Hopex Power Supervisor** technical module.*

When several writing access areas are defined, you can list and manage the members (persons and person groups) of a specific writing access area.

To access the person groups of a specific writing access area:

1. Access the **Users** management pages.

    ☛ *See Accessing the User Management Pages.*

2. Click **Person Groups** then select **By writing access area**.

3. (To display the person groups only) In the tree, click the of the writing access area selected.
    The person groups connected to the writing access area are displayed.

4. Select the writing access area.
    In the edit area, in the **Characteristics** page:

    *   the **Access area members** section lists all the persons and person groups connected to the writing access area selected.
    *   The **Objects** section lists all the objects connected to the writing access area selected.

Accessing the list of person groups connected to a specific reading access area

☛ *With the **Hopex Power Supervisor** technical module*

When management of reading access areas is activated, you can list and manage the members (persons and person groups) of a specific reading access area.

To access the person groups of a specific reading access area:

1. Access the **Users** management pages.

    ☛ *See Accessing the User Management Pages.*

2. Click **Person Groups** then select **By reading access area**.

3. (To display the person groups only) In the tree, click the of the reading access area selected.
    The person groups connected to the reading access area are displayed.

4. Select the reading access area.
    In the edit area, in the **Characteristics** page, the **Access area members** section lists all the persons and person groups connected to the reading access area selected.

Viewing the Characteristics of a Person

The icon of a person shows:

- when the person is created (name and writing access area defined) but does not have a login.

- when the person has a login but is not fully configured (e-mail or profile assignment is not defined).

- when the person is configure as a **Hopex** user:
  name, writing access area, login, and e-mail address are specified and a profile is assigned to the person.

> ☞ See *Defining a Person*, *Creating a User* and *Assigning a Profile to a Person*.

To view the characteristics of a person:

1. Access the **Persons** management pages.

> ☞ See *Accessing the User Management Pages*.

2. In the list of persons, click the name of the person.

☛ *Alternative: hover the cursor over of the person name then click* **Open in a new tab** ⬈ .

☺ *You can use the list filtering tool to help you find the person.*

The **Characteristics** property page of the person is displayed.

☛ *See Person Properties.*

☛ *See Defining a Person.*

3. To display:
- the activity on the person, display its **Activity Feed** property page.
- the history of actions performed on the person, in the property page menu bar, click ⋮ then select **Manage > History**.

Viewing the Characteristics of a Person Group

To view the characteristics of a person group:

1. Access the management pages of the **Person groups**.

> ☛ *See Accessing the User Management Pages.*

The list of person groups appears with for each group, where necessary, its associated SSO group, and its description.

> ☛ *You can sort or filter the display according to the columns.*

> ☛ *You can connect an SSO group to the group from this page (clicking in the corresponding field).*

2. In the list of person groups, click the name of the person group.

> ☛ *Alternative: hover the cursor over of the person group name then click* ***Open in a new tab*** ⬈ *.*

> ☺ *You can use the list filtering tool to help you find the person group.*

The **Characteristics** property page of the person group is displayed.

> ☛ *See Person Group Properties.*

> ☛ *See Defining a Person Group.*

3. To display:
   - the activity on the person group, display its **Activity Feed** property page.
   - the history of actions performed on the person group: in the property page menu bar, click ⋮ then select **Manage > History**.

Viewing the Characteristics of a Login

> ☛ *For detailed information on characteristics of a login, see Login Properties (Person).*

> ☛ *To configure a login, see Defining the Login of a Person.*

You can view the characteristics of a login:

- directly in the **Characteristics** property page of the login holder (person or person group), **Application Access** section (Application Access and Application access).

  ☺ See *Viewing the Characteristics of a Person* or *Viewing the Characteristics of a Person Group.*

- in the property pages of the login.

To view the characteristics of a login:

1. Access the **Users** management pages.

   ☛ See *Accessing the User Management Pages.*

2. Click **Persons** or **Person Groups**.

3. In the list toolbar, select the person (or person group) concerned.

4. In the list menu bar, click **Login** ☑ **> properties**.

CREATING AND MANAGING USERS

For an overview of actions to be performed to create and define a user see Big Picture: Actions to Define a User.

☛ *To manage person groups, see Managing Person Groups Rather than Persons and Creating and Managing a Person Group.*

The following points are covered here:

- configuration:
  - Creating a User
  - Defining a Person
  - Creating the Login of a Person
  - Defining the Login of a Person
  - Modifying the Properties of a User
  - Connecting a Person to a Writing Access Area
- management:
  - Checking the Configuration of Users
  - Connecting a Person to a Writing Access Area
  - Connecting a Person to a Reading Access Area
  - Preventing a User Connection
  - Deleting a User
  - Creating and Managing a Person Group
  - Managing User-Related Options
  - Transferring Responsibilities to a Person
  - Duplicating Responsibilities of a Person

Creating a User

📖 *Person represents a physical person or a system.*

☛ *Instead of creating users one by one, you can import a list of persons.*

A user depends on an environment. To create a user, you must connect to the environment to which the user will be attached.

A user is a person with a login. To create a user, you must create a person with its login, or create the login of a person already created.

☛ *For detailed information on characteristics of:*

- a person, see Person Properties,

- a login, see Login Properties (Person).

Once the user is created, he/she automatically receives an Hopex account activation e-mail to define his/her connection password.

☛ *This e-mail is sent only when Hopex SMTP settings are configured (see Configuring SMTP Settings). Otherwise, the Password field is available at user creation. You must then define this temporary password, that the user has to change at first connection.*

E-mail and password

The user defines his/her password on reception of his/her Hopex account activation e-mail. This e-mail includes a link valid for 48 hours.

☞ *To resend the account activation e-mail, see Initializing a User Web Account.*

If needed (e.g.: troubles with password or e-mail reception), the administrator can define a temporary password for the user.

☞ *See Defining a Temporary Password to a User.*

To create a user:

1. Access the **Persons** management pages.

☞ *See Accessing the User Management Pages.*

2. Click **New** ➕.
The **Creation of Person - Characteristics** window opens.

3. Enter the characteristics of a person:
- In the **Name** field, enter the name of the person.

  `E.g.: WOODS William`

    ☛ *Recommendation: the same format should be used for all persons.*

- In the **E-mail** field, enter the e-mail address of the person.
- In the **Login** field, enter a login.

  `E.g.: WWS`

    ☛ *If you do not enter the login, it automatically takes the value entered in the **Name** field.*

    ☛ *A **Login** is unique and can be assigned to only one Person or Person Group.*

    ☛ *A **Person** can have only one **Login**.*

Creation of Person (System) - Characteristics ↗ ⊠

Name*

WOODS Lea

E-mail*

lwood@mega.com

Login

LWS

⌃ **Data Access**

Writing access area*

Administrator ⌄

‹ Previous | Next › | OK | Cancel

    ☛ *If **Hopex** SMTP settings are not configured (See Configuring SMTP Settings) in the **Password** field, enter a temporary password.*

4. (with the **Hopex Power Supervisor** technical module) Use the **Reading Access Area** drop-down menu to select the reading access area value of the user.

    ☛ *The **Writing Access Area** field appears only if there are several writing access areas. By default at creation, the user is connected to the maximum writing access area: "Administrator".*

5. (If required, with the **Hopex Power Supervisor** technical module) In the **Reading Access Area** field, use the drop-down menu to select the reading access area value of the user.

    ☞ *By default at creation, the user is connected to "Standard" reading access area. This field only appears if reading access management has been activated.*

6. Click **Next**.
    The **Creation of Person - Profiles to be assigned** window pops up.

7. Assign a profile to the person:

    ☞ *You can perform this action later, see Assigning a Profile to a Person.*

    • In the **Repository** field, select the repository in which you want to assign the profile to the person.

        ☞ *You can select all the repositories.*

    • In the **Profiles** list, select the profile(s) you want to assign to the person.

    ### Creation of Person (System) - Profiles to be ...   ↗   ☒

    WOODS Lea

    Select the repository, accessible by the person, for the profiles assigned*

    DEMO   ⌄

    Select the profiles to be assigned to the person

⊟		Name ↑	Description	▼
☑	🧑	**Data Asset Manager**	The Data Scientist is responsible for brin...	
☐	👤	**Data Contributor**	The data contributor is involved in the d...	
☐	👤	**Data Designer**	A data designer is a professional who is ...	
☐	👥	**Data Functional Administra...**	The Data Functional Administrator is re...	

    < Previous   Next >   OK   Cancel

8. Click **OK**.
   The user is created and is added to the list of users.
   The user receives an email to define his/her password.

☛ *To check the configuration of the user, see Checking the Configuration of Users.*

☛ *To define the characteristics of the user, see Defining a Person.*

☛ *You must configure the login of the user, see Defining the Login of a Person.*

☛ *To check the configuration of the user, see Checking the Configuration of Users.*

☛ *To manage the licenses of the user, see Managing Named Licenses.*

Defining a Person

📖 ***Person*** *represents a physical person or a system.*

☛ *For more information on the properties of a person, see Person Properties.*

☛ *To assign a profile to a person (mandatory), see Assigning a Profile to a Person.*

In the property pages of a person, you can define:

Mandatory

- the name of the person
- the e-mail address of the person

    ☛ *The e-mail address is required, for example, for the user to define his/her password, for distributing documents, receiving notifications and questionnaires, or when a user loses his/her password.*

- the login of the person

Optional and also user-configurable

- the image of the person
- the default library to store the objects created by the person, if the creation context does not define one
- the data language of the Web user

> ☛ *If the field is not defined, by default the data language is the one defined in the environment options (**Options: Installation > Languages**: **Data Language**).*

> ☛ *See Managing Languages in Web Applications.*

Optional

- the phone number and initials of the person

If needed

- if the person belongs to a person group.

If data (writing or reading) access management is set up

- writing access area of the user

   For information regarding writing access management, see HOPEX Administration > Managing data writing access documentation

- reading access area of the user

> ☛ *Only if reading access management has been activated.*

   For information regarding reading access management, see HOPEX Administration > Managing data reading access documentation

To define a **Person**:

1. Access the properties of the person.

   > ☛ *See Viewing the Characteristics of a Person.*

2. (Optional) To add or update the image of the person, click **Update Image**, select the image then click **OK**.

   > ☛ *The image is stored in binary on an attribute of the person. To delete the image, click **Reinitialize Image**.*

   > *The person can update his/her image himself/herself.*

3. In the **E-mail** field, enter the e-mail address of the person.
4. (Optional) Enter the **Phone Number** and **Initials** of the person.
5. In the **Application Access** section:
   - so that the person can connect to **Hopex**, the person must have a **Login**.

     > ☛ *See Creating the Login of a Person.*

   - (optional, if necessary) select **Belongs to a Person Group**.
6. (Optional) In the **Data Access** section:
   - in the **Data Language** field, using the drop-down menu, you can define a specific data language for this user.
   - in the **Default Library** field, click the arrow then select the library in which objects created by the user are stored if the creation context does not define one.

     > ☛ *The person can modify these fields himself/herself.*

7. (With the **Hopex Power Supervisor** technical module) In the **Data Access** section, you can modify the access area values:

- the user writing access area, using the drop-down menu of the **Writing access area** field.

  ☛ *By default, a new user is connected to the only available writing access area: "Administrator".*

  ☛ *See also Mass Connecting Persons to a Writing Access Area.*

- the user writing access area at creation, using the drop-down menu of the **Writing access area at creation** field.

- the user reading access area, using the drop-down menu of the **Reading access area** field.

  ☛ *This field only appears if reading access management has been activated.*

  ☛ *See also Mass Connecting Persons to a Reading Access Area.*

- the user reading access area at creation, using the drop-down menu of the **Reading access area at creation** field.

  ☛ *This field only appears if reading access management has been activated.*

The person is configured.

Creating the Login of a Person

To access **Hopex**, a person must have a Login. When you create a person from:

- *Hopex administration desktop*, the login of the person is automatically created.
  This person can access **Hopex**.

- *other desktops*, (e.g.: with the GRC Functional Administrator) the login of this person is not created automatically.
  So that the person can connect to **Hopex**, you must create a login for the person.

  ☛ *See Login Properties (Person).*

To create the login of a person:

1. Access the properties of the person.

   ☛ *See Viewing the Characteristics of a Person.*

2. In the **Application Access** section, **Login** field, click the arrow then select **Create Login**.
   The **Creation of Login** window opens. The name of the login is already entered with the name of the login holder.

   ☺ *Alternative:*

   *Access the list of persons, then filter the list on the **Login** column "Show empty values only".*

   *Click in the **Login** field of the person, then click the arrow then select **Create Login**.*

3. (If needed) In the **Name** field, modify the login name.

> ☛ *A login is unique and can be assigned to only one Person or Person Group.*

> ☛ *A **Person** can have only one **Login**.*

`E.g.: WWS.`

4. In the **User Code** field, enter a user code associated with the login.

`E.g.: WWS.`

5. (If not filled) In the **E-mail** field, enter the e-mail address of the person.

> ☛ *If the **Hopex** SMTP settings are not configured (see Configuring SMTP Settings) the **E-mail** field is replaced by **Password**, enter a temporary password.*

6. Click **OK**.
The login of the user appears in the **Login** field.

Defining the Login of a Person

In the **Characteristics** property page of the login you can:

> ☛ *See Login Properties (Person).*

- define the login **Name**, the **User Code** associated with the login and the **Login Holder**

> 📖 *A **login** is unique and defined for a person or person group.*

> 📖 *The **User code** is an identifier (upper case) of the user. It serves as a basis for naming user files.*

- modify the user **status** (inactive)
- restrict the user access to certain products (**Command line**)
- (case of authentication managed within Hopex) modify the user **Authentication Mode**

To define the login of a person:

1. Display the **Characteristics** property page of the login of the person.

> ☛ *See Viewing the Characteristics of a Login.*

> ☺ *You can also display the **Characteristics** of the person, **Application Access** section, see Viewing the Characteristics of a Person.*

  - The login **Name** and **User Code** attributes are already created, but you can modify these if necessary.
  - The **Login Holder** is the person associated with the login.

2. (If needed) Modify the **Status (Login)** field value, which defines if the user is active or not.

> ☛ *See Status (Login).*

3. (If needed) In the **Command Line** field, define the products available to which the user has access.
To restrict the user access to products A and B, enter the command:
/RW'<accessible Product A code>;<accessible Product B code>;<...>'

`For example: You have licenses for products **Hopex Business Process Analysis, Hopex IT Portfolio Management** and other`

Hopex products. To authorize only the **Hopex Business Process Analysis** and **Hopex IT Portfolio Management** modules to a user, enter:

`/RW'HBPA;APM'`

☛ *To know the product code, see the online documentation: **Concepts > Products**.*

💣 **If a user is connected to a profile, and both the user and profile have access to products restricted by the Command Line attribute, the products accessible to the user are the intersection of the values of the Command Line attribute of the user (on his/her login) and profile.**

4. (If needed) In the **Authentication Mode** field, click the arrow and modify the authentication mode.

☛ *The default value is "MEGA", see Authentication mode (case of authentication managed within Hopex).*

Modifying the Properties of a User

For each user, you can modify:

- his/her personal characteristics:
  - name
  - image
  - E-mail address
  - phone number
  - initials
- data access
  - data language
  - default library
  - writing access area
  - reading access area
- the group to which the person belongs
- profile assignments

  ☛ See *Person Properties.*

  ☛ See *Viewing the Characteristics of a Person.*

  ☛ See *Defining a Person.*

- his/her application access defined by his/her login
  - name
  - user code

    💣 **To ensure consistent action history, the user code should not be modified.**

  - status
  - accessible products (Command Line)
  - authentication mode

    ☛ See *Login Properties (Person).*

    ☛ See *Viewing the Characteristics of a Login.*

    ☛ See *Defining the Login of a Person.*

Connecting a Person to a Writing Access Area

☛ *Managing writing access areas is only available with the **Hopex Power Supervisor** technical module.*

☛ *To connect a person to a writing access area, see also Defining a Person.*

To connect a person to a writing access area:

1. Access the properties of the person.

   ☛ See *Viewing the Characteristics of a Person.*

   ☺ *For a direct access to active persons without writing access area: in the homepage of the **Hopex Administration** desktop, **My scope > Person Statistics**, click **Active persons with no Writing Access Area** indicator.*

2. In the **Data Access** section, use the **Writing access area** drop-down menu to select the writing access area.

> ☛ *To find the writing access area with the search tool, click the arrow to the right of the **Writing access area** field then select **Connect Writing access area**. In the result list, select the writing access area then click **Connect**.*

The person is connected to the selected writing access area.

Mass Connecting Persons to a Writing Access Area

> ☛ *Managing writing access areas is only available with the **Hopex Power Supervisor** technical module.*
>
> ☛ *To connect a person to a writing access area, see Defining a Person.*

To mass connect persons to a writing access area:

1. In the **Hopex Administration** desktop, click the **Users** navigation menu, then **Persons** ▦▸ then select **By writing access area**.

2. In the tree, select the writing access area.
The **Characteristics** property page of the writing access area is displayed.

3. In the **Access area members** section, click **Connect** 🔗.

> ☛ *To add a person not yet created, click **New** ✚, see Creating a User.*

4. Use the search tool to select the persons in the result list.

> ☛ *You can select persons and/or person groups.*

5. Click **Connect**.
The selected persons are connected to the writing access area.

Connecting a Person to a Reading Access Area

> ☛ *Managing reading access areas is only available with the **Hopex Power Supervisor** technical module.*
>
> ☛ *To connect a person to a reading access area, see also Defining a Person.*

To connect a person to a reading access area:

1. Access the properties of the person.

> ☛ *See Viewing the Characteristics of a Person.*

2. In the **Data Access** section, use the **Reading access area** drop-down menu to select the reading access area.

> ☛ *To find the reading access area with the search tool: click the arrow to the right of the **Reading access area** field then select **Connect reading access area**. In the result list, select the reading access area then click **Connect**.*

The person is connected to the reading access area.

Mass Connecting Persons to a Reading Access Area

☞ *Managing reading access areas is only available with the **Hopex Power Supervisor** technical module.*

☞ *To connect a person to a reading access area, see also Defining a Person.*

To connect persons to a reading access area:

1. In the **Hopex Administration** desktop, click the **Users** navigation menu, then **Persons** ⇛ then select **By reading access area**.

2. In the tree, select the reading access area.
The **Characteristics** property page of the reading access area is displayed.

3. In the **Access area members** section, click **Connect** 🔗.

☞ *To add a person not yet created, click **New** ➕, see Creating a User.*

4. Use the search tool to select the persons in the result list.

☞ *You can select persons and/or person groups.*

5. Click **Connect**.
The selected persons are connected to the reading access area.

Preventing a User Connection

When you no longer want a user to connect to **Hopex**, but you want to retain trace of his/her actions, you must make the user inactive but not delete it from your repository.

To make a user inactive:

1. Access the **Characteristics** property page of the person.

☞ *See Viewing the Characteristics of a Person.*

2. In the **Application Access** section, in the **Status (Login)** field, select "Inactive".
The user can no longer connect to **Hopex**.
The user's named licenses, if any, are automatically revoked.

Mass Preventing User Connection

In a single action, you can prevent several users from connecting.

To make users inactive:

1. Access the **Persons** management pages.

☞ *See Accessing the User Management Pages.*

2. In the person list, select the persons concerned.

☺ *You can use the list filtering tool to help you select the persons.*

3. Click the **Status (Login)** cell of one of the selected persons then select "Inactive".
   The selected users can no longer connect to **Hopex**.

   Their respective named licenses, if any, are automatically revoked.

Deleting a User

💣 **When you delete a user from the repository, the commands connected to this user become orphans and you lose part of the history saved in logs. To remove a user but keep its history of commands, see Preventing a User Connection.**

To delete a user:
1. Access the **Persons** management pages.

   ☛ *See Accessing the User Management Pages.*

2. In the **Persons** list, select the person to be deleted then click **Remove** 🔴 .

   ☛ *You can select several persons.*

   The **Deleting** window pops up: the person and corresponding login and assignments are selected.

3. Click **Delete** to confirm the deletion.
   The person and corresponding login and assignments are deleted from the repository.

   💣 **All traces of user actions are lost.**

CREATING AND MANAGING A PERSON GROUP

For an overview of actions to be performed to create and define a user, see Big Picture: Actions to Define a User.

The following points are covered here:
- configuration:
  - Creating a Person Group
  - Defining a Person Group
  - Defining a default connection group
  - Connecting a Person Group to a Writing Access Area
  - Connecting a Person Group to a Reading Access Area
  - Modifying a Person Group Login
  - Modifying a User Group Properties
- management:
  - Preventing a User Group Connection
  - Deleting a Person Group

Creating a Person Group

A **Person Group** is a list of persons belonging to the same group. These persons share the same connection characteristics.

For detailed information on:
- connecting persons belonging to a group, see Managing Person Groups Rather than Persons:
- the types of person groups, see Authentication Group.
- the characteristics of a person group, see Person Group Properties.
- the characteristics of the login of a person group, see Login Properties (Person Group).

A person group depends on an environment. To create a person group, you must connect to the environment to which the persons are attached.

To create a person group:
1. Access the **Person groups** management page.

   ☛ See *Accessing the User Management Pages.*

2. Click **New** ➕.
   The **Creation of Person Group - Characteristics** window pops up.
3. In the **Name** field, enter the name of the person group.

   `Example: Marketing.`

4. (With the **Hopex Power Supervisor** technical module) In the **Writing access area** field, use the drop-down menu to select the value for the writing access area for the group.

   ☛ The **Writing Access Area** field appears only if there are several writing access areas.

5. (With the **Hopex Power Supervisor** technical module) In the **Reading access area** field, use the drop-down menu to select the value for the reading access area for the group.

☛ *By default, at creation, the group is connected to the "Standard" reading access area.*

☛ *This field only appears if reading access management has been activated.*

6. Click **OK**.
The person group is created and added to the list of person groups.

💣 **The login of the person group is automatically created and used for configuration purposes only. A person belonging to a group connects with his/her own login.**

☛ *See Modifying a Person Group Login.*

You must define this person group, see Defining a Person Group.

Defining a Person Group

A **Person Group** is a list of persons belonging to the same group.

☛ *See Managing Person Groups Rather than Persons.*

☛ *For detailed information on:*

- the characteristics of a person, see Person Properties.

- the characteristics of a person group, see Person Group Properties.

- the characteristics of a login, see Login Properties (Person Group).

- the person group types, see Authentication Group.

A person group can be created:

- statically

☛ *See Adding persons to a static person group.*

- dynamically

☛ *See Defining a dynamic person group (SSO).*

To configure a person group, you must:

- assign a profile to the person group

☛ *See Assigning a Profile to a Person Group.*

You can also:
- define a default connection group
  - ☞ See *Defining a default connection group.*
- connect the person group to a reading area
  - ☞ See *Connecting a Person Group to a Reading Access Area.*
- connect the person group to a writing area
  - ☞ See *Connecting a Person Group to a Writing Access Area.*
- define the data language of the person group
  - ☞ *Managing Languages.*
- modify the properties of the persons group
  - ☞ See *Modifying a User Group Properties.*

Adding persons to a static person group

Case of a person group created statically.

To add persons to a **Person Group**:

1. Access the **Characteristics** property page of the person group.
   - ☞ See *Viewing the Characteristics of a Person Group.*

2. In the **Persons** section, click **Connect** 🔗 .
   - ☞ *To add a person not yet created, click **New** ➕, see Creating a User.*

3. Use the search tool to select the persons in the result list.
   These persons must have a login to be able to connect.
   > 💣 **A person belonging to a group connects to the application with its login. A person without a login cannot connect to an application.**
   - ☞ *Use the [Ctrl] key to select more than one person at the same time.*

4. Click **Connect**.
   The person(s) are added to the person group.

Defining a dynamic person group (SSO)

📖 *A **Person Group** is a list of persons belonging to the same group. These persons share the same connection characteristics.*

📖 *A dynamic group is a group that computes the users of a group on the fly (see Connection request and user created on the fly).*

☞ *For information on person group types, see Authentication Group.*

In the case of a person group created dynamically, the **Authentication group** attribute enables to define the authentication group (SSO) that defines this person group. The persons belonging to this group (SSO) use the configuration defined on the person group.

Prerequisite: the SSO authentication group is already created.

☞ See *Defining an SSO authentication group.*

To define a dynamic **Person group** (SSO):

1. Access the **Characteristics** property page of the person group.

☞ *See Viewing the Characteristics of a Person Group.*

2. In the **Authentication Group** field, click the arrow and connect the required authentication group.

3. Click **OK**.
The dynamic person group is configured with SSO.

Defining a default connection group

□ *A **Person Group** is a list of persons belonging to the same group. These persons share the same connection characteristics.*

☞ *For information on person group types, see Authentication Group.*

A default person group is required for persons with the "Belongs to a person group" attribute selected, but who are not listed in any group.

☞ *No person group is provided at Hopex installation. See Creating a Person Group.*

To define a default connection group:

1. Access the property pages of the person group.

☞ *See Viewing the Characteristics of a Person Group.*

2. Select **Characteristics**.

3. Select **Default connection group** option.

Connecting a Person Group to a Writing Access Area

☞ *Managing writing access areas is only available with the **Hopex Power Supervisor** technical module.*

To connect a person group to a writing access area:

1. In the **Hopex Administration** desktop, click the **Users** navigation menu, then **Person Groups** ≣▸ then select **By writing access area**.

2. Select the writing access area.
The **Characteristics** property page of the writing access area is displayed.

3. In the **Access area members** section, click **Connect** 🔗.

☞ *To add a person group not yet created, click **New** ➕, see Creating a Person Group.*

4. Use the search tool to select the person group in the result list.

☞ *You can select several person groups.*

5. Click **Connect**.
The selected person groups are connected to the writing access area.

Connecting a Person Group to a Reading Access Area

☛ *Managing reading access areas is only available with the **Hopex Power Supervisor** technical module.*

To connect a person group to a reading access area:

1. In the **Hopex Administration** desktop, click the **Users** navigation menu, then **Person Groups** ⊒▶ then select **By reading access area**.
2. Select the reading access area.
The **Characteristics** property page of the reading access area is displayed.
3. In the **Access area members** section, click **Connect** 🔗.

☛ *To add a person group not yet created, click **New** ➕, see Creating a Person Group.*

4. Use the search tool to select the person group in the result list.

☛ *You can select several person groups.*

5. Click **Connect**.
The selected person groups are connected to the reading access area selected.

Modifying a Person Group Login

When you create a person group, the login of the group is automatically created.

From the login property pages you can:

☛ *See Login Properties (Person Group).*

- modify the name of the login and the user code associated with the login
- modify the status of the person group (inactive)
- modify the authentication mode

To modify the login of a person group:

1. Access the property pages of the login.

☛ *See Login Properties (Person Group).*

2. Select **Characteristics**:
   - The login **Name** and **User Code** attributes are already created, but you can modify these if necessary.

📖 *A **login** is unique and defined for a person or person group.*

📖 *The **User code** is the short identifier (upper case) of the user. It is of no use in case of a person group.*

   - The **Login Holder** represents the person group associated with this login.
   - The value of the **Status (Login)** field defines if the person group is active or not.

Modifying a User Group Properties

You can modify the properties of a user group. For each user group, you can modify properties of:

- person group:
  - name
  - writing access area
  - reading access area
  - login
  - if it is the default connection group
  - group type (SSO group, person group computed by macro, or persons directly connected to group)
  - persons who are members of the group

    ☛ *See Person Group Properties.*

    ☛ *See Viewing the Characteristics of a Person Group.*

    ☛ *See Defining a Person Group.*

    ☛ *See Defining a dynamic person group (SSO).*

- login:
  - name and user code
  - status

    ☛ *See Login Properties (Person Group).*

    ☛ *See Viewing the Characteristics of a Login.*

    ☛ *See Modifying a Person Group Login.*

Preventing a User Group Connection

When you want to temporarily prevent the persons in a group from connecting in the name of the group, you must make the person group inactive, without deleting it from your repository.

To deactivate a person group:

1. Access the **Characteristics** property page of the person group.

    ☛ *See Viewing the Characteristics of a Person.*

2. In the **Application Access** section, in the **Status (Login)** field, select "Inactive".
   The persons can no longer connect to **Hopex** as this group.

Deleting a Person Group

When you delete a person group, only the group is deleted. The persons belonging to the group are not deleted.

To delete a person group:

1. Access the **Person groups** management pages.

> ☛ *See Accessing the User Management Pages.*

2. In the list, select the person group to be deleted.

> ☛ *You can select several person groups.*

3. In the list menu bar, click **Remove** ⊖ .
The **Deleting objects** window opens.

4. Click **Delete** to confirm deletion.
The person group and its login are deleted from the repository.

MANAGING PROFILES

Profiles are managed (customization, creation) in the **Hopex Studio** desktop with the **Hopex Customizer** profile (with *Hopex Power Studio* technical module).

☛ See **Studio > Profiles & Permissions > Managing Profiles** documentation.

📖 *A profile defines what a person can see or not see and do or not do in the tools, and how the person sees the tools and can use them. The profile defines options, access rights to repositories and products, read/ write and read-only rights on objects.*

The following points are detailed here:

- Viewing Profile Characteristics
- Configuring a Profile
- Checking Profile Compliance with Connection Regulation
- Assigning a Profile to a Person
- Assigning a Profile to a Person Group
- Removing a Profile Assignment

Viewing Profile Characteristics

☛ *The full characteristics of a profile are accessible for profile customization purpose only (Hopex Studio desktop, Hopex Customizer profile).*

For a complete description of profiles, see Hopex Studio > Managaging Profiles documentation.

To view the main characteristics of a profile:

   1. Access the **Profiles** pages.

       ☛ *See* *Accessing the User Management Pages.*
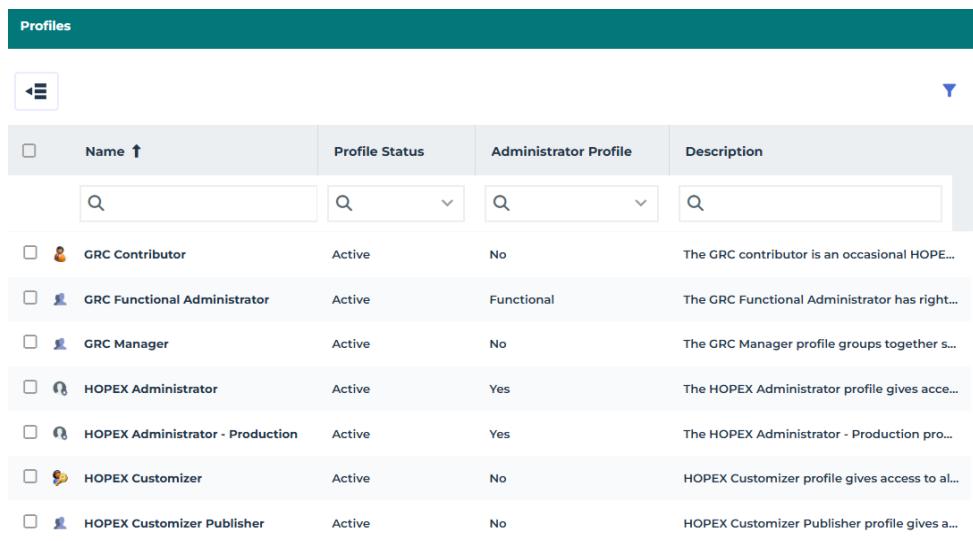
	Name ↑	Profile Status	Administrator Profile	Description
☐ 👤	GRC Contributor	Active	No	The GRC contributor is an occasional HOPE...
☐ 👤	GRC Functional Administrator	Active	Functional	The GRC Functional Administrator has right...
☐ 👤	GRC Manager	Active	No	The GRC Manager profile groups together s...
☐ 👤	HOPEX Administrator	Active	Yes	The HOPEX Administrator profile gives acce...
☐ 👤	HOPEX Administrator - Production	Active	Yes	The HOPEX Administrator - Production pro...
☐ 👤	HOPEX Customizer	Active	No	HOPEX Customizer profile gives access to al...
☐ 👤	HOPEX Customizer Publisher	Active	No	HOPEX Customizer Publisher profile gives a...

2. In the profile list, click the profile name.
   The profile **Properties** window displays its main **Characteristics**:
   - its **Status**
   - its **Command Line**
   - its **Description**
   - the persons and person groups to whom it is assigned (**Assignments** section)

☛ See *Configuring a Profile.*

Configuring a Profile

A profile creation and customization is restricted to Hopex Customizer profile.

☛ See ***Hopex Studio > Profiles & Permissions > Managing Profiles*** *documentation.*

In the **Characteristics** property page of the profile you can specify whether the profile is:

☛ *See Profile Properties.*

- an administrator profile or not (action restricted to **Hopex Administrator**)
- active or not

You can also:

- perform a mass profile assignment to persons

  ☛ *See Performing a mass profile assignment to persons or Performing of mass profile assignment to person groups.*

- check that the profile complies with the connection regulation

  ☛ *See Checking Profile Compliance with Connection Regulation.*

To configure a profile characteristics:

1. Access the properties of the profile.

   ☛ *See Viewing Profile Characteristics.*

2. (If needed) In the **Administrator Profile** field, modify the attribute value.

   ☛ *By default, the profile is not an administrator profile (value: No).*

   ☛ *See Administrator profile.*

3. (If needed) In the **Profile Status** field, modify the attribute value.

   ☛ *By default, the profile is active.*

Checking Profile Compliance with Connection Regulation

A profile must comply with modeling regulation.

To check that a profile complies with the connection regulation:

1. Access the **Profiles** pages.

   ☛ *See Accessing the User Management Pages.*

2. In the **Profiles** list, right-click the profile concerned then select **Manage > Check > Regulation with propagation**.
3. Select **Connection regulation**.
4. Click **OK**.
   The connection regulation report for the selected profile is displayed.

Assigning a Profile to a Person

☛ *A person may have several profiles.*

💣 **A user must have at least one profile assigned to be able to connect to Hopex.**

Assigning a profile to a person defines:
- the profile assigned
- the repository concerned by the assignment
- (optional) the validity period of the assignment
- (optional, with read-only access to the repository) the connection repository snapshot

  Repository Snapshot:

  📕 *A repository snapshot defines repository state at a given moment.*

  The connection repository snapshot defines the state of the repository to which the users of a profile connect.

  To define a repository snapshot, a repository snapshot must have been previously created.

  ☛ *See Managing Repository Snapshots.*

Restrictions:
- The **Administrator profile** attribute of a profile allows to assign an administrator type profile.

  ☛ *See Administrator profile.*

  Only administration dedicated profiles (Hopex Administrator, Hopex Administrator - SaaS) allow to assign any profile (including administration dedicated profiles) to persons.
- A functional administrator of a Solution, can only assign profiles related to this Solution.

  ```
  E.g.: the GRC Functional Administrator profile allows to
  assign the GRC specific profiles(e.g.: Audit Director, GRC
  Contributor) except GRC Functional Administrator profile.
  ```

See:
- Assigning a profile to a person
- Performing a mass profile assignment to persons

Assigning a profile to a person

☛ *To assign one or more profiles to one or more persons at a time, see Performing a mass profile assignment to persons*

To assign a profile to a person:
1. Access the properties of the person.

   ☛ *See Viewing the Characteristics of a Person.*

   ☺ *In the homepage, click the **Active Persons with no Writing Access Area** indicator.*

2. In the **Profile Assignments** section, click **New** ➕.
3. In the **Profile assigned** field, click the drop-down menu then select the profile you want to assign to the person.

   ☛ *To perform a search filtering the profiles, click the arrow then select **Connect profile**.*

4. (If needed) In the **Repository** field, click the drop-down menu then change the repository concerned by the assignment.

   ☛ *By default, the current repository is selected. You can select another repository or all the repositories.*

5. (Optional, with read-only data access) In the **Connection Snapshot** field, select a connection repository snapshot.
6. (optional, to define a validity date) Click **Valid for a limited period**.
   - (optional) In the **Validity start date** field, use the calendar to define the start date of profile assignment validity.
   - (optional) In the **Validity end date** field, use the calendar to define the end date of profile assignment validity.
7. Click **OK**.
   The profile is assigned to the person on the selected repository for the specified duration.

Performing a mass profile assignment to persons

You can perform a mass assignment of one or more profiles to persons.

To perform a mass assignment of profiles to persons:

1. Access the **Persons** management pages.

   ☛ See *Accessing the User Management Pages.*

   The list of persons displays in the edit area.
2. Select the persons to whom you want to assign one or more profiles.
3. In the list menu bar, click **Assignments > Assign Profiles**.
   The list of profiles appears.
4. In the **Repository** field, select the repository concerned by the assignment.

   ☛ *By default, the current repository is selected. You can select another repository or all the repositories.*
5. By default, assignments do not have a validity limit. If you must define a validity period for assignments, select **Define validity dates**.
   - In the **Validity start date** field, click the calendar then select a validity start date.
   - In the **Validity end date** field, click the calendar then select a validity end date.
6. Select the profiles you want to assign to the selected persons.
7. Click **OK**.
   The selected profiles are assigned to the selected persons, on the selected repository, for the defined period.

Assigning a Profile to a Person Group

For a user belonging to a person group to be able to connect to **Hopex** in the name of the group, you must assign a profile to the person group. If necessary, you can define a validity period for the profile assignment.

The profile assignment is specific to a repository.

   ☛ *A person group can have several profiles.*

See:
- Assigning a profile to a person group
- Performing of mass profile assignment to person groups

Assigning a profile to a person group

To assign a profile to a person group:

1. Access the properties of the person group.

    ☛ *See Viewing the Characteristics of a Person Group.*

    ☺ *In the homepage, click the **Active Person Groups with no assigned Profile** indicator.*

2. In the **Profile Assignments** section, click **New** ➕.

3. In the **Assigned profile** field, click the drop-down menu then select the profile you want to assign to the person group.

    ☛ *To perform a search filtering the profiles, click the arrow then select **Connect profile**.*

4. (If needed) In the **Repository** field, click the drop-down menu and change the repository concerned by the assignment.

    ☛ *By default, the current repository is selected. You can select another repository or all the repositories.*

5. (Optional, with read-only data access) In the **Connection Snapshot** field, select a connection repository snapshot.

6. (Optional) By default, assignments do not have a validity limit. If you need to define a validity period for assignments, select **Valid for a limited period**.

    • In the **Validity start date** field, click the calendar then select a validity start date.
    • In the **Validity end date** field, click the calendar then select a validity end date.

7. Click **OK**.
    The profile is assigned to the person group on the selected repository for the defined period.

Performing of mass profile assignment to person groups

To perform a mass assignment of profiles to a person group:

1. Access the **Person groups** management page.

    ☛ *See Accessing the User Management Pages.*

    The list of person groups displays in the edit area.

2. Select the person groups to which you want to assign one or more profiles.

3. In the list menu bar, click **Assign Profiles**.
    The list of profiles appears.

4. (If needed) In the **Repository** field, click the drop-down menu then change the repository concerned by the assignment.

    ☛ *By default, the current repository is selected, you can select another repository or all of them.*

5. By default, assignments do not have a validity limit. If you must define a validity period for assignments, select **Define validity dates**.

    • In the **Validity start date** field, click the calendar then select a validity start date.
    • In the **Validity end date** field, click the calendar then select a validity end date.

6. Select the profiles that you want to assign to the selected person groups.
7. Click **OK**.
    The selected profiles are assigned to the person groups selected for the defined period.

Removing a Profile Assignment

You can remove a profile assignment. This profile assignment can concern a person or a person group.

You can perform a mass removing of profile assignments.

To remove a profile assignment:

1. Access the properties of the person (or person group).

    ☛ *See Viewing the Characteristics of a Person.*

    ☛ *See Viewing the Characteristics of a Person Group.*

2. In the **Profile Assignments** section, select the profile concerned.

    ☛ *You can select more than one.*

3. Click **Remove** ⊖.
4. In the deleting window, click **Delete** to confirm your action.

    ☛ *If needed, you can clear some of the profile assignments selected.*

    ☛ *The corresponding named licenses, if any, are not automatically revoked. To assign only the required named licenses to the user, you can revoke and then assign licenses, see Managing Named Licenses.*

MANAGING NAMED LICENSES

Assigning Named Licenses

Assigning **named licenses** ensures that each user has exclusive access to Hopex products, unlike **floating licenses**, which may be temporarily unavailable when all are in use.

Licenses are assigned based on the products specified in the **Command Line** fields of the user's profile and login.

> ☛ See *Products accessible on the license (Command Line)* of the profile and *Products accessible on the license (Command Line)* of the person's login.

To assign named licenses:

1. Access the **Persons** management page.

   > ☛ See *Accessing the User Management Pages.*

2. Select the person concerned.

   > ☛ You can select several persons.

3. In list menu bar, click **Licenses** > **Assign Licenses**.
   Licenses are assigned according to the command line configuration.
   A warning message is displayed if any of the required licenses is unavailable.

Revoking Named Licenses

Revoking named licenses helps optimize license usage by making unused licenses available. Once released, they can be reassigned as needed.

All named licenses associated with the user are revoked simultaneously.

> ☞ *If a user has multiple profiles, the named licenses associated with all of their profiles are revoked.*

To revoke named licenses:

1. Access the **Persons** management pages.

   > ☞ See *Accessing the User Management Pages.*

2. Select the person concerned.

   > ☞ *You can select several persons.*

3. In list menu bar, click **Licenses** > **Revoke Licenses**.
   A confirmation of the license revocation appears.

   These licenses become available and can be reassigned to another person.

Viewing all Licenses

To support license management, the License Dashboard provides an overview of all assigned named licenses, as well as floating licenses (if applicable).

To view all licenses:

❭ Access the **License Dashboard**.

> ☞ See *Accessing the User Management Pages.*

Several reports appear based on the licenses subscribed.

Named licenses consumption

This report shows:
- the number of assigned named licenses
  - 🔵 the number of users currently logged in
  - 🟠 the number of users currently logged out
- 🟢 the number of available named licenses
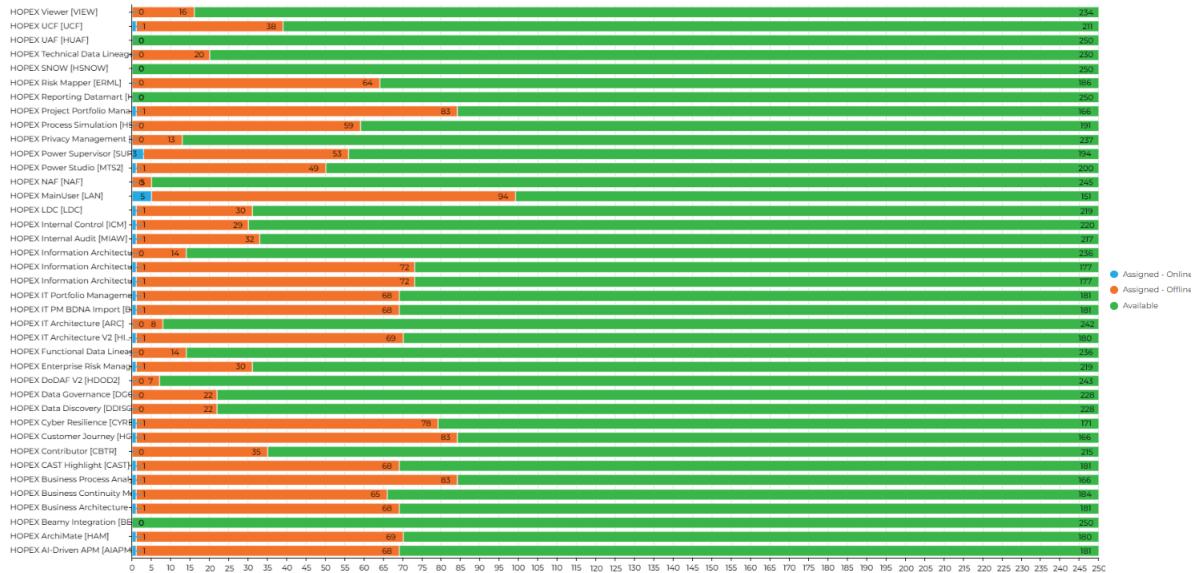
Floating licenses capacity

This report shows in real time the number of:

- ● used floating licenses
- ● available floating licenses

Floating license capacity
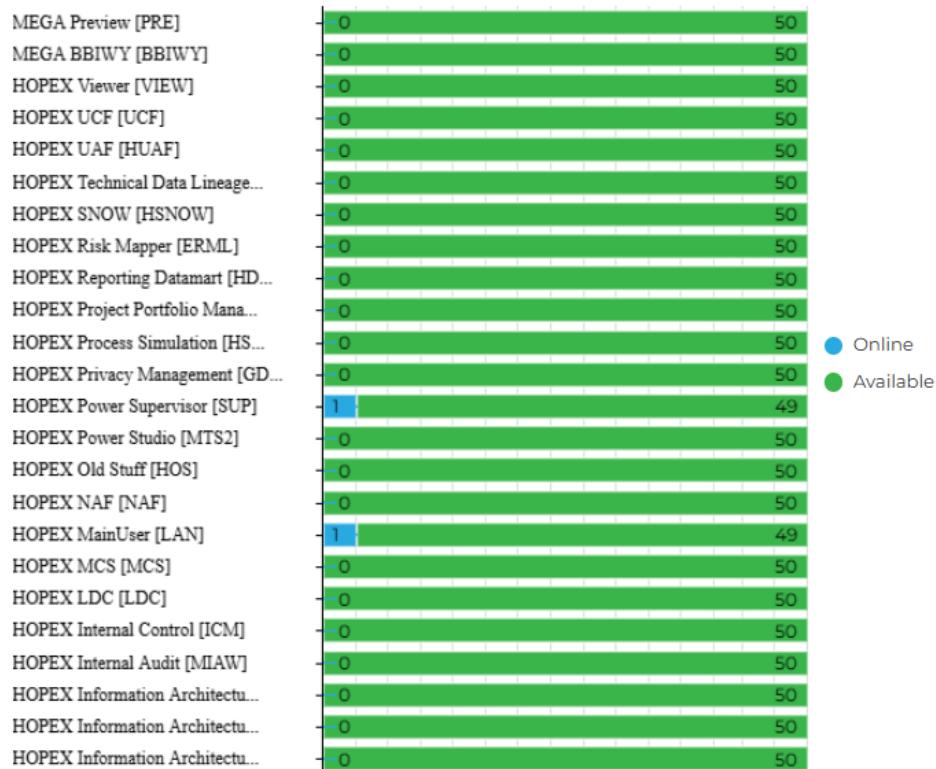
Assignements of named licenses

This report shows the named licenses assigned to each user.

- : the user is currently logged in.
- : the user is currently logged out.

The table lists users against HOPEX license columns:

User	HOPEX AI-Driven APM [AIAPM]	HOPEX ArchiMate [HAM]	HOPEX Bearry Integration [BEAM]	HOPEX Business Architecture & Strategic Plan	HOPEX Business Continuity Management [BCM]	HOPEX Business Process Analysis [HBPA]	HOPEX CAST Highlight [CAST]	HOPEX Contributor [CBTR]	HOPEX Customer Journey [HCJ]	HOPEX Cyber Resilience [CYRES]	HOPEX Data Discovery [DDISC]	HOPEX Data Governance [DGOV]	HOPEX DoDAF V2 [HDOD2]	HOPEX Enterprise Risk Management [ERMV]	HOPEX Functional Data Lineage [DLIN]	HOPEX IT Architecture V2 [HITA]	HOPEX IT Architecture [ARC]	HOPEX IT PM BDNA Import [BDNA]	HOPEX IT Portfolio Management [APM]	HOPEX Information Architecture Business L	HOPEX Information Architecture Logical Laye	HOPEX Information Architecture Phys	HOPEX Internal Audit [MIAW]	HOPEX Internal Co
Ernesto [Ernesto]				out				out				out								out	out	out	out	
FOUR Guillain [gfou@mega.com]	in	in		in	in	in	in		in	in			in		in		in	in	in	in		in	in	in
FOURIER Lionel [lfourier@mega.com]				out	out			out	out	out	out		out						out	out	out	out		
Frank [Frank]				out	out			out														out		
GAIER Pierre [pgaier@mega.com]	out	out		out	out	out	out		out	out			out		out		out	out	out	out		out	out	out
GANE Nabil [ngane@mega.com]	out	out		out	out	out	out	out	out	out			out		out		out	out	out	out			out	
GIBELIN Laura [lgibelin@mega.com]	out	out		out		out	out		out	out			out		out		out	out	out	out			out	
GIBERT Hervé [hgibert@mega.com]																							out	
GIOTTE Valérie [vgiotte@mega.com]	out	out		out	out	out	out	out	out	out		out	out	out	out		out	out	out	out	out	out	out	out
CLEVER Line [lclever@mega.com]	out	out		out	out	out	out		out	out			out		out		out	out	out	out		out	out	in

MANAGING USER-RELATED OPTIONS

For specific requirements, you can modify default values of certain **Options** (see Managing Options).

See:

- Authorizing deletion of a dispatched object
- Making the comment on dispatch mandatory
- Managing User Inactivity

See also:

- Modifying Password Security Settings

Private Workspace Specific Options

Authorizing deletion of a dispatched object

Users working in a public workspace can delete objects.

By default, users working in a private workspace are not authorized to delete dispatched objects, even if these have been created by the user wishing to delete.

The **Authorize dispatched object deletion from private workspace** option (**Options > Repository > Authorizations** folder) allows the user to delete dispatched objects from a private workspace, irrespective of the creator.

This authorization complements object deletion rights defined elsewhere for the profile or user.

Making the comment on dispatch mandatory

With the **Comment on dispatch** option (**Options > Repository > Data Saving** folder) users must enter information in the **Dispatch comment (report)** pane when they dispatch their work.

Managing User Inactivity

You can specify how long a user session can remain inactive before it is closed.

☺ *This option can be useful for example for security requirements, or to ensure that all sessions are closed before starting a batch program.*

By default, user inactivity management is not activated.

Activating/Deactivating user inactivity management

To activate/deactivate user inactivity management:

1. Access **Options** at environment level.

   ☞ See *Managing Options.*

2. In the **Options** tree, select **Workspace > Desktop**.
3. In the right pane:
   - to activate user inactivity management, select **Automatic Session Timeout**.
   - to deactivate user inactivity management, clear **Automatic Session Timeout**.

Managing user inactivity

Prerequisite: user inactivity management is taken into account if the **Inactivity Management** option is selected.

To manage user inactivity:

1. Access the **Environment Options**.

   ☞ See *Managing Options.*

2. In the **Options** tree, select **Workspace > Desktop**.
3. In the right pane, enter a value (in minutes) for the **Duration of inactivity before closing Hopex** option.

   💣 **If the Period of inactivity requiring authentication option is lower than the *Duration of inactivity before closing Hopex* value, thus the value taken into account for user disconnection is this latter.**

Once this duration is reached, the user is disconnected and **Hopex** closes without warning.

Managing User Account Inactivity

By default a user account is disabled after no connection for 90 days. The user receives a first notification by email, seven days before the deactivation date, then a reminder three days before the deactivation date.

The e-mail includes a link to connect to Hopex to reactivate the account.
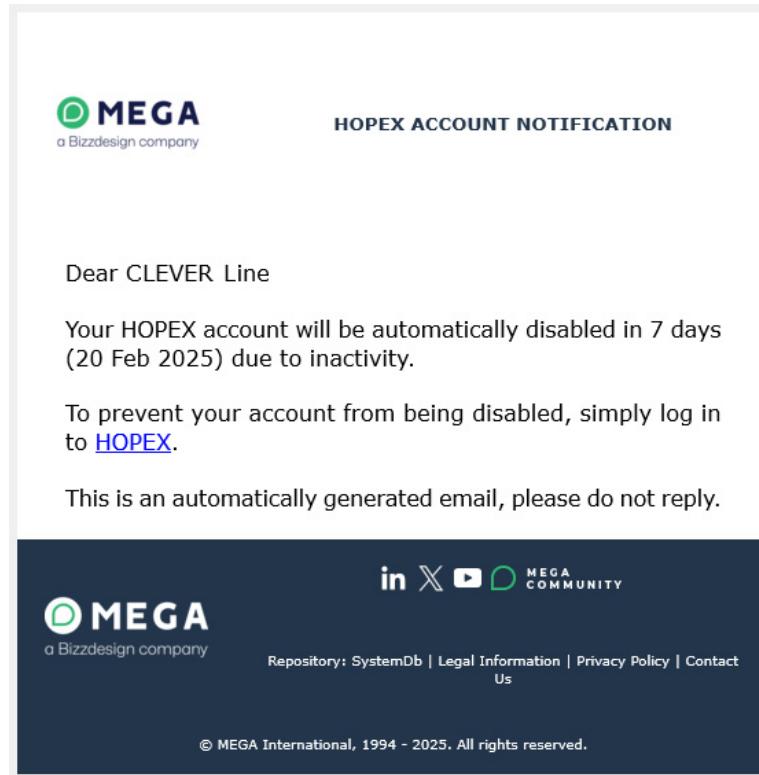
You can deactivate the option or modify the durations:

- **Number of days without login after which a user account is disabled**
  Value: 1 day or more (90 days by default).
  Value 0: the user account is never disabled.
- **Notification X days before deactivation**
  First notification: number between 0 and 21 days (7 by default).
  Value 0: no notification is sent.
- **Notification Y days before deactivation**
  Reminder: between 0 and 14 days (3 by default).
  Value 0: no notification or reminder is sent.

To manage inactive user accounts:

1. Access the **Environment Options**.

    ☛ *See Managing Options.*

2. In the **Options** tree, select **Installation > User Management > Authentication**.
3. In the right pane, modify the option values.
4. Click **OK**.

Modifying Data Import Authorization

The **Authorize import of Hopex data (MGR,MGL,XMG)** option defines which data a user or a profile is authorized to import into **Hopex**.

It can take the following values:
- "Prohibit"
- "Authorize XMG import in the data repository only"
- "Authorize XMG, MGR, MGL import in the data repository only"
  (By default for all the profiles, including the **Hopex Administrator - SaaS** and **Functional Administrators** profiles)
- "Authorize XMG, MGR, MGL import in the data repositories and SystemDb"
  (by default for **Hopex Administrator** profile only)

To change **Hopex** data import authorization:
1. Access **options** (level concerned).

   ☛ *See Managing Options.*

2. In the **Options** tree, select **Tools > Data Exchange > Import > MEGA Files: Generic Options**.
3. In the right pane, modify the **Authorize import of Hopex data (MGR,MGL,XMG...)** option value.

AUTHENTICATION IN HOPEX

Authentication process consists in verifying that a person corresponds to his or her declared identity. In IT networks, authentication is usually based on a connection name and a password.

By default, in **Hopex** (Web Front-End) authentication is managed by **Hopex Unified Authentication Service** (UAS).

> ☛ See ***Installation and Deployment > Hopex Unified Authentication Service*** *documentation.*

Unique authentication, known as Single Sign On (SSO) or Unified Login, is a software solution that enables company network users to access all authorized resources in total transparency, on the basis of unique authentication at initial network access.

In this way, a single password enables access to all company applications and systems.

This solution offers several advantages, including:

- greater security
  The user no longer has to remember several connection procedures, identifiers or passwords.
- improved administrator productivity
  Hopex integrates into enterprise directories, which reduces administrator workload regarding password management.

The Single Sign On system used in **Hopex** is based on standard security protocols natively integrated in Windows: Kerberos and SSO. In addition, **Hopex** Single Sign On complies with the following recognized standards:

- Windows Security Services
- C2-Level Security of the American Defense Department
- Kerberos
- NTLM Authentication

> ☛ *For more details on single sign-on, see "Single Sign-On in Windows 2000 networks" document at the following Web address:*
> *http://technet.microsoft.com/fr-fr/library/bb742456.aspx*

See:

- Authentication and Mapping Principle
- Choosing an Authentication Mode
- Modifying the Hopex Authentication Mode for a User
- Managing an SSO Authentication Group
- Configuring SSO Authentication

Authentication and Mapping Principle

The connection to **Hopex** includes the following phases:

- *Phase 1: Authentication*
  The authentication phase consists in checking that the person connecting to Hopex exists and that his/her identification is valid. This authentication can be independent of the Hopex repository.

  Once validated, this authentication phase is not called later at the mapping phase.

- *Phase 2: Mapping*
  The mapping phase consists in defining the profile with which the authenticated person will connect to the application.

  Without a profile assigned the connection is refused to the user, even authenticated.

- *Phase 3: Connection and access to the repository*
  Once authentication and mapping phases are validated, the person can connect to the application and access the repository.

  The person selects the repository and the profile with which he/she wants to connect.
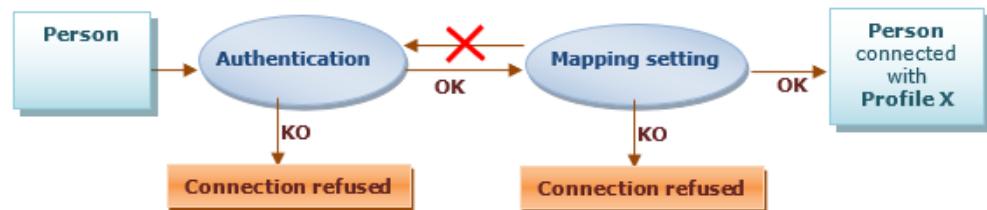
Choosing an Authentication Mode

In **Hopex** (Web Front-End) authentication is managed by **Hopex Unified Authentication Service** (UAS). UAS enables to define how the user authenticates.

☛ *For a detailed description, see **Installation and Deployment > Hopex Unified Authentication Service> UAS Configuration** documentation.*

To select your authentication mode, **Bizzdesign** recommends that you use authentication systems that comply with Standards (e.g.: SSO). You can choose an authentication managed:

- ***by an external module***
  If your enterprise has an external authentication or SSO module, it is preferable to use the delegated authentication system.

  ```
  Example: SAML2, OpenId.
  ```

  To define and configure your external authentication mode, see **Installation and Deployment > Hopex Unified Authentication Service documentation**.

- ***within the Hopex platform*** (by default)
  If you have no standard authentication system in your enterprise, you can use the authentication system managed within Hopex.

Modifying the Hopex Authentication Mode for a User

User authentication mode is defined on the login by the **Authentication Mode** parameter.

Hopex (Web Front-End) provides the **MEGA** authentication mode (by default): the Hopex authentication service checks that the password entered matches the password stored in Hopex repository.

To modify the authentication mode of a user, see Authentication mode (case of authentication managed within Hopex).

Managing an SSO Authentication Group

SSO authentication group

The SSO authentication process is characterized by claims. These claims include the groups or roles the user belongs to. These groups have a unique identifier that can be entered in the **Authentication identifier** attribute.

```
Example: the claim role "rCmp-WebAXDevRemoteRdpTier2@MEGA"
```

Defining an SSO authentication group

To define an authentication group:

1. Access the authentication group management pages.

   ☛ See *Accessing the User Management Pages.*

2. In the edit area, in the **Authentication groups** tab, click **New** ➕.
   The authentication group creation window appears.

3. In the **Name** field, enter a name for the authentication group.

4. In the **Authentication Identifier** field, enter the identifier of the claim with which you want to map the authentication group.

   ```
   Example: the claim role "rCmp-WebAXDevRemoteRdpTier2@MEGA"
   ```

5. Click **OK**.
6. Associate a Hopex person group with the authentication group: in the **Authentication Group** list, click in the **Person Groups** field then select the person group.

☛ *See also Associating a Hopex User Group with an Authenticated User Group.*

Configuring SSO Authentication

The SSO service includes information (claims), which enables to identify a user or a user group.

Claims

The claims are included in the SSO service.

```
Examples of claims: a name, a group, an email, a role.
```

These claims are used to map this information with the data included in **Hopex**.

To identify a person, you can for example map:

- the "displayname" claim with the **Name** attribute of the person in Hopex.
- the "email" claim with the **E-mail** attribute of the person in Hopex.

To identify a person group, your SSO service must include groups. These groups are listed under the claim "role".

☛ *To modify the claim used for mapping authentication groups, modify the **ClaimForRoles** of the identity provider (see **Installation and Deployment > Hopex Unified Authentication Service** documentation).*

To identify a person group, you can for example map:

- The claim role "rCmp-WebAXDevRemoteRdpTier2@MEGA" with a person group in Hopex.

Example of information included in an SSO service:

```
{
  "ValidateLifetime": true,
  "AccessTokenType": "Reference",
  "TokenHandle": "52c900bcfe54f2ef081b3fa704e19e11",
```
"Claims":{
"aud": "https://hopex/UAS/resources",

"iss": "https://hopex/UAS",

.....

"displayname": "Lou,Watts",

"name": "lws",

"email": "lwatts@mega.com",

"given_name": "",

"family_name": "Watts",

"groupsid": [

"S-1-5-21-0123456789-0123456789-513",

"S-1-1-0",

"S-1-5-32-544",

"S-1-5-32-545",

],

"role":[

"Domain Users@MEGA",

"Everyone",

"Administrators@BUILTIN",

"Users@BUILTIN",

"NETWORK@NT AUTHORITY",

"Authenticated Users@NT AUTHORITY",

"This Organization@NT AUTHORITY",

"rCmp-WebAXDevRemoteRdpTier2@MEGA",

"tNtfs-USTLVUCSD651DImagesRecorderModify@MEGA",

"tSvc-WebAX8AppXtenderRetentionFilingServiceFull@MEGA"

],

"lws": "1ae8ad551970e66e071536655b9542ad"

}

}

Configuring SSO Authentication

To configure SSO authentication:

1. Define the authentication parameters.

   For example: the name and e-mail of the person.

   ☞ *See [Defining an Authentication Parameter](#).*

2. If you manage person groups:
- Define the authentication groups.

  ☛ See *Defining an SSO authentication group.*

- Map the authentication groups with the person groups defined in Hopex.

  ☛ See *Associating a Hopex User Group with an Authenticated User Group.*

MAPPING

Mapping Diagram

The following diagram fully describes the process of mapping a user, whose login is authenticated, with a person in **Hopex**.
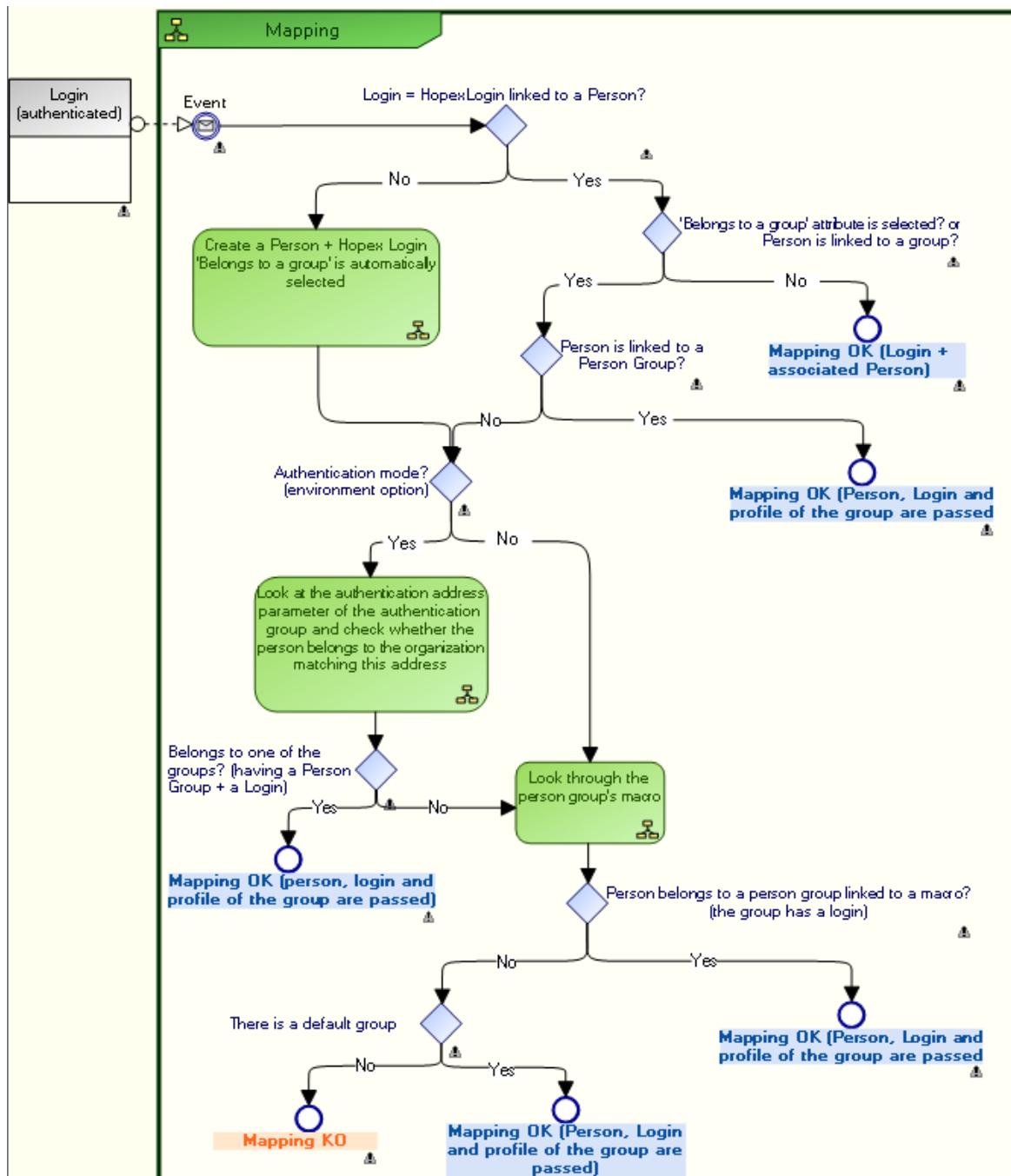
Principle

Once the mapping service is informed of the identifier of the person requesting connection, the service checks if this identifier is referenced in the repository:

> ☛ *This identifier is usually the login, but if an SSO authentication parameter is defined and that its "Is Index On Person" attribute is selected, then the service checks if the value of this attribute does not exist on a person, and in this case it is this identifier that is used to determine if the person exists in Hopex or not.*
>
> See *Defining an Authentication Parameter.*

- Case 1:
  The identifier is referenced in the repository and does not belong to a group.
- Case 2:
  The identifier is referenced in the repository and belongs to a group.
- Case 3:
  The identifier is not referenced in the repository and does not belong to a group.

When a default group is defined, any person not belonging to a specific group, but with the "Belongs to a person group" attribute selected, must belong to the default group.

> ☛ See *Creating and Managing a Person Group.*

Connection request and user created on the fly

In SSO authentication case, when an authenticated user requests connection to **Hopex**:

- If the login of the user is connected to the Login of a Person saved in Hopex and this person:
  - does not belong to a group, the mapping is validated and the user can choose to connect with one of his assigned profiles. The connection is made as the person.
  - belongs to one or several groups, the mapping is validated and the user can connect with one of the groups and choose one of the profiles assigned to the selected group. The connection is made as the group.
  - belongs to one or several groups and has one or several assigned profiles, the mapping is validated and the user choose to connect with one of his assigned profiles (the connection is made in the name of the person) or via one of the groups he belongs to (the connection is made in the name of the group).
- If the login of the user:
  - corresponds to the Login of a person saved in Hopex, that the "Belongs to a person group" attribute is selected, but the Person is not connected to a Person Group,

  or

  - does not correspond to the Login of a person saved in Hopex and authentication is SSO type, then the person is created on the fly with a

Login (the "Belongs to a person group" attribute is automatically selected).

☛ *The person is created on the fly only if it does not exist. If the person exists, only the login is created.*

☛ *The person (+ Login) is only created if it effectively belongs to a group (SSO, connected to a macro, or "default group" is defined).*

So if the person:

- belongs to an SSO group (with Person Group and Login) the mapping is validated and the connection is made in the name of the group (login and profile of the group are passed).

  `E.g.: Alexandre DUBOIS belongs to the Marketing group whose login is Marketing,`

- does not belong to an SSO group, but belongs to a group linked to a macro: the mapping is validated and the connection is made as the group (login and profile of the group are passed).
- does not belong to an SSO group, neither to a group linked to a macro, but a default group is defined: the mapping is validated and the connection is made as the group (login and profile of the group are passed).
- does not belong to an SSO group, neither to a group linked to a macro, and a default group is not defined: the mapping is rejected.

When the person belongs to a group, the service returns two pieces of information:

- The person created on the fly (Assignable Element) from the SSO server. The aim of creating a person on the fly is to keep a record of actions. The user acts in his/her name and not in the name of the group.

- The list of the person groups he/she belongs to (and his/her assignments, if he/she has profiles assigned).
  A profile is associated with the group. This indicates with which profile the person created on the fly will connect to the application.

  ☛ *At the next connection of this person, the service returns the same user created on the fly (same information/attributes). The service creates a user on the fly per person and saves his/her information.*

Associating a Hopex User Group with an Authenticated User Group

Once the authentication group is created, you must associate it with a Hopex user group.

So that when a person of the Hopex person group connects to Hopex, he/she is authenticated thanks to the user group authenticated to the SSO service.

☛ *If a default person group is defined, any person in Hopex with the* **Belongs to a person group** *attribute selected (see Person Properties) automatically belongs to the group defined by default (see Defining a default connection group).*

Prerequisite: the Hopex person group and the authenticated user group are created.

> ☞ *See:*
>
> *Creating a Person Group*
> *Defining an SSO authentication group*
> *Defining a dynamic person group (SSO).*

To associate a Hopex user group with an authenticated user group:

1. Access the properties of:
   - the authentication group

   or

   - the person group.

   > ☞ See *Accessing the User Management Pages.*

2. Display the **Characteristics** page.
3. Click the arrow of:
   - the **Person group** field and connect the Hopex person group to be associated with the authenticated user group.

   or

   - The **Authentication group** field and connect the authenticated user group to be associated with the person group.

   The authentication Group query wizard appears.

   > ☺ *Use the [Ctrl] key to select several authentication groups at the same time.*

   The Hopex person group is associated with the authenticated user group.

Defining an Authentication Parameter

An authentication parameter is a parameter that exists in the SSO service and that is associated uniquely with a **Hopex** attribute.

Configuring an authentication parameter is useful when importing persons from an SSO service.

Authentication parameters enable to:

- identify a person from the authentication server.
- predefine the characteristics of a person created in **Hopex**, using the mapping between the authentication parameter values (stored in the SSO service) and the Hopex MetaAttributes.

  ```
  Example: the "E-mail" MetaAttribute of the person is
  initialized with the "email" claim of the person in the SSO
  service (if mapping has been carried out).
  ```

To configure an authentication parameter:

1. Access the authentication management pages.

   > ☞ See *Accessing the User Management Pages.*

2. Select **Authentication parameters**.

3. Click **New** ➕.

> ☛ *The authentication parameter enables pre-completion of characteristics of a person corresponding to the authentication parameters.*

4. Enter a **Name** for the authentication parameter then click **Properties** 💬 .

    `Examples: E-mail, Name (person).`

5. (Optional, "expert" metamodel access) Select **Index on Persons**, so that the parameter value enables unique identification of a person. If a person in **Hopex** has the same e-mail as a person defined in the SSO service, this person is reused (instead of creating a new person and risking duplicating the same person).

6. (Optional, "expert" metamodel access) Select **Is available for search** so that an e-mail can be entered in the import entry area.

    `Example: if you enter ctodd@mega.com, you should find Clara TODD.`

7. In the **Authentication identifier** field, enter the claim associated with the SSO service.

    `E.g.: email`

8. In the **Mapped MetaAttribute** field, click the arrow then select **Connect MetaAttribute**.

9. Perform the search then select the Hopex MetaAttribute you want to associate with the SSO authentication identifier defined step 7.

    `Examples: E-mail, Name (person).`

10. Click **Connect**.
11. Click **OK**.

MANAGING THE PASSWORD OF A WEB USER

With MEGA authentication mode, to allow a Web user to define their password and security question, you must initialize their Web account.

The following points are detailed here:

- Initializing a User Web Account
- Modifying the Lifetime of the First Connection Link
- Modifying Password Security Settings
- Defining a Temporary Password to a User

Initializing a User Web Account

As soon as you enter the e-mail of the user, an e-mail for his/her Hopex account activation is automatically sent to the user. This e-mail includes a link with a lifetime of 48 hours.

In case the user did not receive his/her account activation e-mail, or if the link validity is exceeded, you can initialize his/her account.

Prerequisites:

Before initializing the Web account of a user:

- ensure the e-mail of the person is specified and correct.

    ☛ *See Viewing the Characteristics of a Person.*

- check that the SMTP settings is configured.

    ☛ *See Configuring SMTP Settings.*

To initialize the Web account of a user:

1. Access the **Persons** management pages.

    ☛ *See Accessing the User Management Pages.*

2. In the list of persons, select the person concerned.
3. In the menu bar, select **Login > Initialize Account**.
    An e-mail is sent to the person concerned with a limited life link (48 hours by default), allowing the person to define a password and the reply to a security question.

    💣 **In the characteristics of the person, if the e-mail address is not specified, the person cannot receive the message.**

    ☛ *To modify the lifetime of the first connection link, see Modifying the Lifetime of the First Connection Link.*

Modifying the Lifetime of the First Connection Link

To modify the lifetime of the first connection link:

1. Access the environment options.

☛ *See Modifying options at environment level.*

2. In the Options tree, expand the **Installation** folder then select **User Management**.

3. In the right pane, modify the value of the **Life of first connection link** option.

Modifying Password Security Settings

You can modify:

- the number of password entry tries allowed to users before their account is blocked and must be unblocked by the administrator
- the number of tries allowed to users to answer to their security question (defined at first connection)
- the number of days before users should change their passwords
- the number of last non-reusable passwords, among those defined by the user
- the strength level of users' password
  Each level is associated with a color (Low: red, Medium: yellow, High: green). As users enter their passwords, the progress bar color changes with the password strength (complexity).
- the number of times the user is allowed to modify his/her password per day
- password requirements:
  - at least one uppercase
  - at least one lowercase
  - at least one special character
  - at least one digit

To modify the settings related to password security:

1. Access environment options.

☛ *See Modifying options at environment level.*

2. In the Options tree, select the **Installation > Security > Password** folder.

3. In the right pane, you can modify the default settings of options:
   - **Number of tries before password invalidation**
     - ☛ *Default value: 3.*
   - **Nb. of tries before password invalidation in response to security question**
     - ☛ *Default value: 3.*
   - **Password expiry**
     - ☛ *Default value: 40 days.*
   - **Number of last non-reusable passwords**
     - ☛ *Default value: 5.*
   - **Password strength**
     - ☛ *Default value: High.*
   - **Maximum number of password changes (per day)**
     - ☛ *Default value: 2.*
   - **Require the use of a digit in the password**
     - ☛ *Default value: option selected.*
   - **Require the use of a lowercase in the password**
     - ☛ *Default value: option selected.*
   - **Require the use of an uppercase in the password**
     - ☛ *Default value: option selected.*
   - **Require the use of a special character in the password**
     - ☛ *Default value: option selected.*

Defining a Temporary Password to a User

☛ ***This action is only available to Hopex Administrator and Hopex Administrator - SaaS profiles.***

This feature is useful for a user whose e-mail is not set. Without email, a user cannot define his/her password via the e-mail sent at account initialization.

☛ *See Creating a User and Initializing a User Web Account.*

You must define this user a temporary password. At first connection to **Hopex**, the user must change this password.

To define a temporary password to a user:

1. Access the **Persons** management pages.

   ☛ *See Accessing the User Management Pages.*

   The list of persons displays in the edit area.

2. Select the person for whom you want to set a temporary password.

   ☛ *You can select multiple users. They will all have the same temporary password.*

3. In the list menu bar, click **Login** 🖼 **> Set Password** 🔑.
4. In the **Password** field, enter the temporary password you want to set for the user.

5. Click **OK**.
   The user's temporary password is saved.

   At first connection to **Hopex**, the user must enter this temporary password. Once connected he/she is prompted to define his/her password.

MANAGING API KEYS

API keys are used to securely establish sessions with Hopex, for example when working with GraphQL, ServiceNow Integration or Teams Integration.

Accessing the List of API Keys

The API key list details for each API key:

- its name
- its associated person and profile
- its expiration date, if any
- its session mode ("Multi Session" or "Single Session")
- its connection mode ("Read Write" or "Read Only")

To access the list of API keys:

1. Access the **Users** management pages.

    ☞ See *Accessing the User Management Pages*.

2. Click **API Keys**.
   The list of API keys is displayed.

	Name	Person (System) ↑	Profile	Expiration Date	Session Mode	Connection Mode
☐	SN API Key	Alan	Process Manager	12/17/2025	Multi Session	Read Write
☑	BT API Key	Antoine	Enterprise Architect	10/12/2025	Single Session	Read Write
☐	Msft API Key	Francesca	Control and Risk Architect		Multi Session	Read Write

Generating an API Key

To generate an API key:

1. Access the list of API keys.

    ☞ See *Accessing the List of API Keys*.

2. In the list menu bar, click **Generate**.
   The API Key generation wizard opens.
3. Enter the **Name** of the API key.
4. Select the **Person** and the **Profile** concerned.

5. Choose a **Session Mode**:
    - Multi Session (recommended): optimized for the use of GraphQL queries, Microsoft Teams Integration and ServiceNow Integration.
    - Single Session: less efficient, memory-intensive, and may slow down other users.
6. Select a **Connection Mode**.
    - Read Write
    - Read Only
7. Select the languages:
    - **Data Language**: display language for repository data.
    - **GUI Language**: display language for interface elements, including error messages and internal or external tabular values.
8. (Optional) Select an expiration date for the API key.
9. (Optional) Enter a description.

10. Click **OK**.
    The API key is generated and can be copied.

API Key : Alexander for Teams   ⊠

Copy the API key and paste it wherever it is required.

3D5bWX9cEeuYiDhH1HY5q8EDW7F3fHb4cwy3yAQvhny4JPfiPftRHSEPvLPHBcVjXaUQs
7KhfA8gZVerG3MLUk11

OK
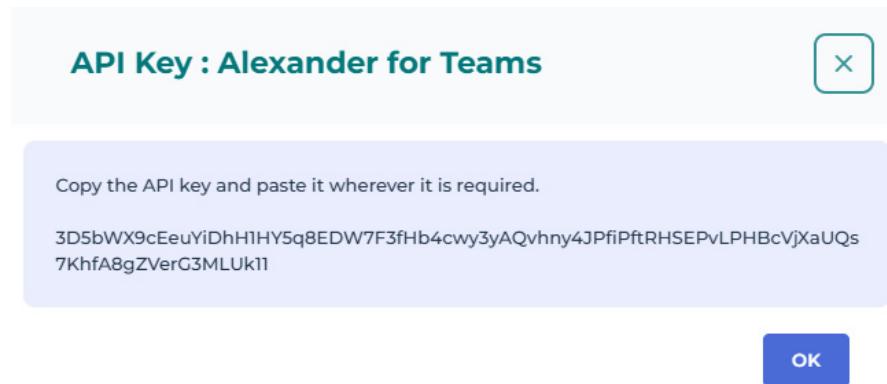
It is added to the list of API keys.
You can view the API key value later again.

Viewing an API Key value

You can view the secret value of an API key value.

To view the secret value of an API key:
1. Access the list of API keys.

    ☛ See *Accessing the List of API Keys.*
2. Select the API key concerned.

    ☺ *You can use the list filtering tool to help find the API key.*

3. In the list menu bar, click **View** 👁 .
    The API key is displayed and can be copied.

Revoking an API Key

For organizational or security reasons, you may need to revoke an API key.

To revoke an API key:
1. Access the list of API keys.

    ☛ See *Accessing the List of API Keys.*
2. Select the API key concerned.

    ☺ *You can use the list filtering tool to help find the API key.*

3. In the list menu bar, click **Revoke** ✖ .
    The API key is deleted and can no longer be used.

Renewing an API Key

You can renew only API keys with an expiration date configured.

To renew an API key:
1. Access the list of API keys.

   ☛ See *Accessing the List of API Keys.*
2. Select the API key concerned.

   ☺ *You can use the list filtering tool (e.g.: **Expiration date**) to help find the API key.*

3. In the list menu bar, click **Renew** .

   The API key generation wizard opens.
4. Enter or modify the required information.
5. Click **OK**.

   A new key is created and appears in the list of API keys.

   💣 **It is important to revoke the old key to prevent any unauthorized use and to update the new key in all applications or services that use it.**

MANAGING LANGUAGES

Managing the Data Language

The data language defines the language in which repository data is displayed to the user at first connection. If the user changes his/her data language (see Modifying your Data Language) in the interface, this is kept for the next connection.

By default, the data language is defined in the environment options.

If needed, you can define the data language for each user or for a user group.

> 💣 **The data language defined at user or user group level takes priority over the language defined in the environment options.**

To modify the data language at environment level:

❱   See Modifying the Data Language at Environment Level.

To specify for a user or user group a data language different from that inherited and defined in environment options:

❱   Modify the **Data Language** parameter in the user or user group properties (page **Characteristics > Data Language**).

☛   *See Defining a Person.*

☛   *See Viewing the Characteristics of a Person Group.*

Managing the User Interface Language

Hopex User Interface (UI) is available in six languages: German, English, Spanish, French, Italian, and Portuguese.

The interface language is defined at environment level for all the users.

To modify the interface language for all the users:

❱   See Modifying the Interface Language at Environment Level.

Each user can modify the language of his/her interface:

❱   See Modifying your User Interface Language.

MANAGING RESPONSIBILITIES

In an **Administration** desktop, you can manage users' responsibilities.

You can transfer or duplicate:
- profile assignments from a user to one or multiple users
  and/or
- object assignments from a user to one or multiple users

  ☛ *In case of object assignment transfer to multiple persons, only objects that can be assigned to multiple persons are available.*

See:
- Transferring Responsibilities to a Person
- Duplicating Responsibilities of a Person

Transferring Responsibilities to a Person

In the **Administration** desktop, you can transfer all or part of responsibilities from a user to one or more users.

The responsibilities transferred are deleted from the source user. To keep the responsibilities you can duplicate the responsibilities of the source user.

☛ *See Duplicating Responsibilities of a Person.*

To transfer the responsibilities from a person to another one:

1. Access the **Persons** management pages.

   ☛ *See Accessing the User Management Pages.*

2. In the list of persons, select the person from whom you want to transfer the responsibilities, then in the list menu bar, click **Assignments > Transfer Assignments**.

   ☛ *You can select multiple persons.*

   The assignment transfer wizard pops up.

3. Click **Next**.
   The window to add the persons to whom the assignments are transfered appears.

4. Click **Connect** 🔗.

5. Use the search tool to select the person to whom you want to transfer the assignments.

   ☛ *You can select multiple persons.*

   In that case, only objects that can be assigned to multiple persons are available.

6. Click **Connect**.
7. Click **Next**.

8. Select the assignments you want to transfer:
   - In the **Profile Assignment** pane, select the profiles you want to transfer to the target user (or to the selected persons).
   - In the **Object Assignments** pane, select the object assignments you want to transfer.
9. (optional) In the **Validity date of profile assignments** part, you can modify the validity dates defined for the source person. Select:
   - **Assignments always valid** for a permanent validity of assignments.
   - **Define validity dates** then select the validity start and end dates.
10. Click **OK**.
    The assignments selected are deleted from the source user (or source users) and transferred to the target user (or target users).

Duplicating Responsibilities of a Person

In the **Administration** desktop, you can duplicate the profile assignments and the object assignments (responsibilities) of a user to one or more users.

To duplicate the responsibilities of a person to another one:

1. Access the **Persons** management pages.

   ☛ *See Accessing the User Management Pages.*

2. In the list of persons, select the person from whom you want to duplicate the responsibilities, then in the list menu bar, click **Assignments > Duplicate Assignments**.

   ☛ *You can select multiple persons.*

   The Duplicate Assignments wizard pops up.

3. Click **Next**.
   The window to add the persons to whom the assignments are duplicated appears.

4. Click **Connect** 🔗.

5. Use the search tool to select the person to whom you want to duplicate the responsibilities.

   ☛ *You can select multiple persons.*

   In that case, only objects that can be assigned to several persons are available.

6. Click **Connect**.
7. Click **Next**.
8. In:
   - the **Profile Assignments** pane, select the profiles that you want to assign (duplicate) to the target user (or to the selected persons).
   - the **Object Assignments** pane, select the object assignments that you want to assign (duplicate) to the target user (or to the selected persons).
9. Click **OK**.
   The selected assignments are assigned (duplicated) to the target user (or target users).

ACCESS

This chapter shows a big picture regarding product and object access management.

The following points are covered here:

✓ Big Picture: Access management
✓ Managing Product and Object Accesses

BIG PICTURE: ACCESS MANAGEMENT

Product Access

Product or data accesses are governed by:

- **the license file**, which details the available products and their access type (**RW**: Read-Write or **RO**: Read Only)

  ☛ *To access the license file, see* Consulting your Licenses.

  Information

  HOPEX Power Studio [MTS2] (RW)
  HOPEX Power Supervisor [SUP] (RW)
  HOPEX Privacy Management [GDPR] (RW)
  HOPEX Process Simulation [HSIM] (RW)
  HOPEX Project Portfolio Management [PPM] (RW)
  HOPEX Risk Mapper [ERML] (RW)
  HOPEX SNOW [HSNOW] (RW)
  HOPEX Technical Data Lineage [HTDL] (RW)
  HOPEX UAF [HUAF] (RW)

  Close

- **the environment options** for the UI

  ☛ *To access the environment options, see* Modifying options at environment level.
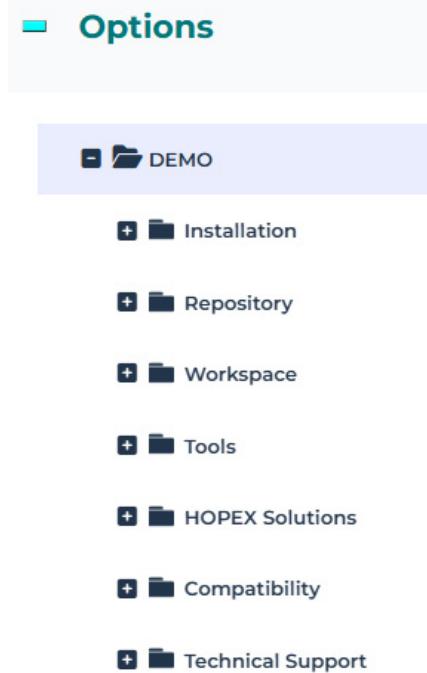
Access Restrictions

User accesses to products, UI, or objects can be restricted by:
- the profile used at connection
- the user
- the group used at connection

Profile level

The profile defines the Hopex desktop (one or several) that the user can access.
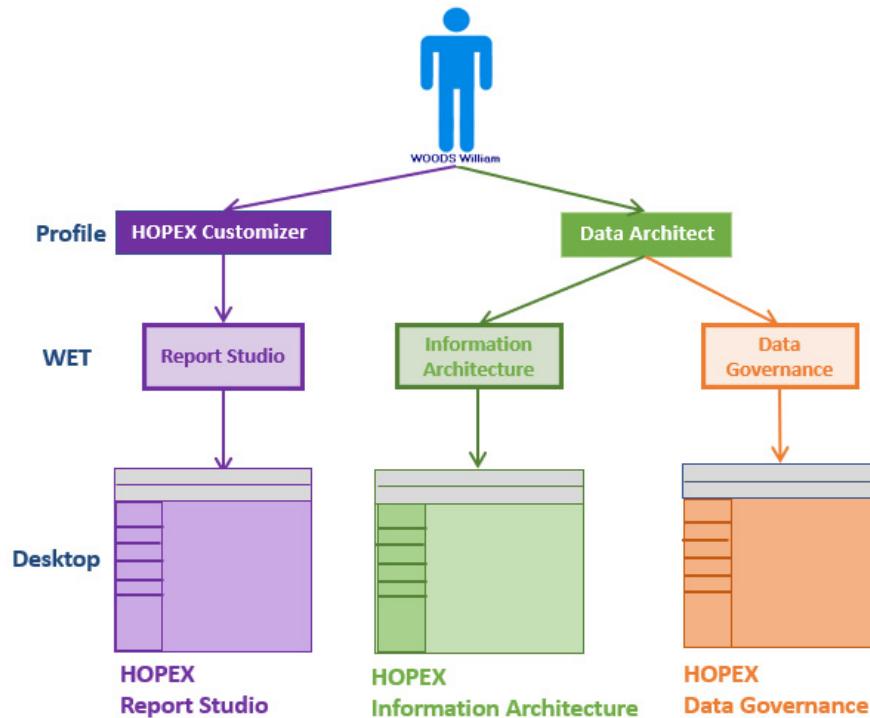
The profile restricts:

- specific product writing or reading access (via its **Command Line**)
- *object UI access (via **Permissions** on Create, Reade, Modify, Delete, Search) that is sufficient to the profile*
- *general UI access (via **availability**) that is sufficient to the profile*
- *metamodel or feature access (via **Options**) that is sufficient to the profile*
- (optional) dynamic data reading or writing access (via **Data access rules** related to the profile)

User level

The user properties restrict:

- writing or reading access to specific products (via the user login **Command Line** if any)
- *metamodel or feature access (via the user **options**)*
- static data writing access (via **Writing access diagram**): the person can modify the objects belonging to his/her writing access area
- (Optional) static data reading access (via **Reading access diagram**): the person has access to the objects belonging to his/her reading access area

Group Level (used at connection)

The group properties restrict:

- specific product writing or reading access (via the person group login **Command Line**, if any)
- static data writing access (via the **Writing access diagram**): the person can modify the objects belonging to the group writing access area
- (Optional) static data reading access (via the **Reading access diagram**): the person has access to the objects belonging to the group reading access area

Rules

Command line rule

The **Command Line** field is available at both profile and user levels.

If both the profile and the user have access to products restricted by the **Command Line** attribute, products accessible to the user are at the intersection of the values of the **Command Line** attribute of the user and profile.

Option rule

Options are governed by an inheritance mechanism **Environment > Profile > User**.

- the *profile* inherits the option values defined at environment level
- the *user* inherits the option values defined at connection profile level

An *Hopex administrator* profile can modify or lock an option at environment level, or even at a specific user level.

> ☛ See *Modifying Options*.

> ☛ In the Administration (Windows Front-End) application the *Hopex administrator* profile can also lock an option at environment level.

A *Hopex Customizer* profile can modify an option at a specific profile level.

> ☛ To modify the profile options, see *Modifying options for a profile*.

A *user* can modify his/her own options (**Main menu > Settings > Options**), for example to modify his/her metamodel access or feature visibility.

> ☛ See *Options* and *Extending the Visibility (Metamodel or Advanced Features)*.

Customization rule

Customizations performed at user level (e.g.: data language change) are of highest priority, followed in order of priority by those performed at profile and environment levels.

MANAGING PRODUCT AND OBJECT ACCESSES

Restricting Product Accesses for a Profile (Command Line)

The **Command Line** field of a profile properties enables to restrict the profile access to available products.

Format of the command is:

```
/RW'<Product Code A>;<Product Code B>;<...>' RO'<Product
Code C>;<...>'
```

RW (or HC): reading and writing access

RO (or HV): reading access only

To restrict the profile accesses to products, see Products accessible on the license (Command Line).

Examples:

User licenses: Products A, B, C and D.

Profile 1 gives reading and writing access to Product A and read only access to product D.

With Profile 1 the user has access to objects A with the permissions defined on the **Set of UI access rights** of Profile 1, and has read only access to objects D.

Profile 2 gives reading and writing access to Product A, B, and D.

With Profile 2 the user has access to objects A, B, and D with the permissions defined on the **Set of UI access rights** of Profile 1.
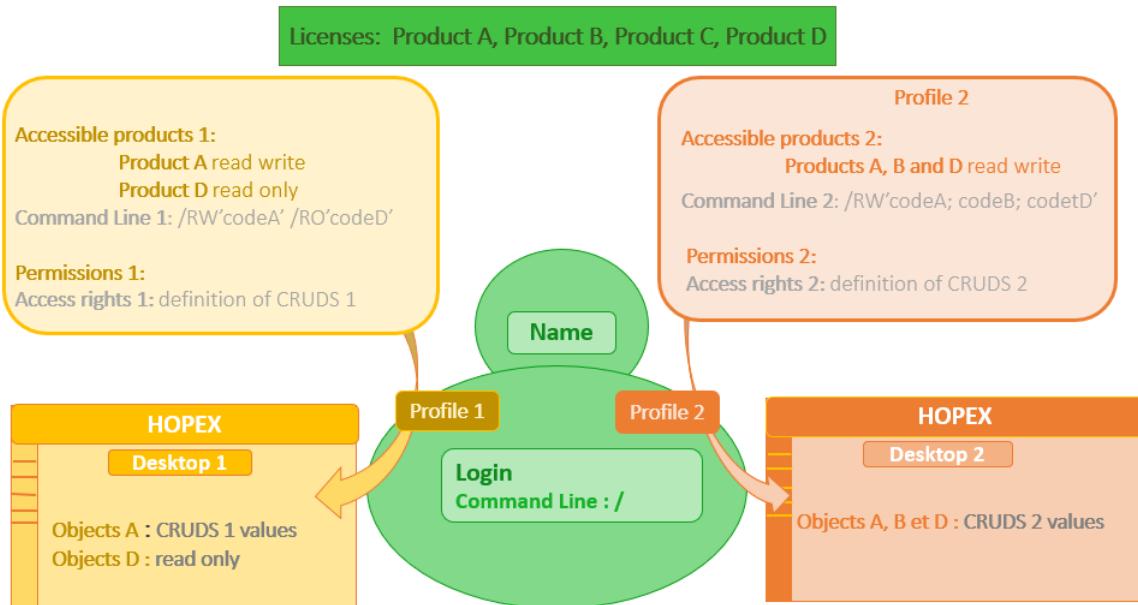
Restricting Product Access for a User (Command Line)

The **Command Line** field of the login properties of a person enables to restrict the user access to available products.

Format of the command is:

```
/RW'<Product Code A>;<...>' /RO'<Product Code B>;<Product
Code C>;<...>'
```

RW (or HC): reading and writing access

RO (or HV): reading access only

> 💣 **If both a user and his/her profile have access to products restricted by the Command Line attribute, the products accessible to the user are at the intersection of the values of the Command Line attribute of the user and profile.**

To restrict a user accesses to product, see Products accessible on the license (Command Line).

Examples:

User licenses: Products A, B, C and D.

Profile 1 gives reading and writing access to Product A and read only access to product D.

Profile 2 gives reading and writing access to Product A, B, and D.

The user has reading and writing access to product A only.

With Profile 1, the user has only access to objects A with the permissions defined on the **Set of UI access rights** of Profile 1.

With Profile 2, the user has only access to objects A with the permissions defined on the **Set of UI access rights** of Profile 2.
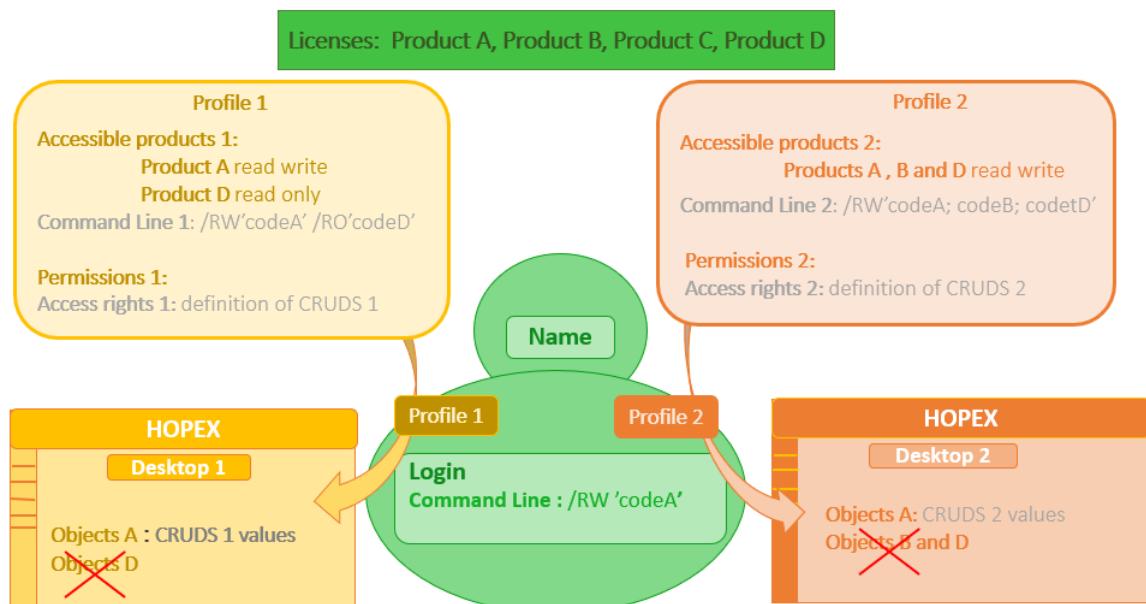
Restricting Product Accesses for a Person Group (Command Line)

The **Command Line** field of the login properties of a person group enables to restrict the product access to users belonging to the group.

Users belonging to a person group and connecting via the group inherits of the profile assignments and access rights of the person group (whatever their own assignments and access rights).

Format of the command is:

```
/RW'<Product Code A>;<...>' /RO'<Product Code B>;<Product
Code C>;<...>'
```

RW (or HC): reading and writing access

RO (or HV): reading access only

💣 **If both a person group and a profile have access to products restricted by the Command Line attribute, the products accessible to the users belonging to the group are at the intersection of the values of the Command Line attribute of the person group and profile.**

To restrict a person group accesses to product, see Command line.

Examples:

User licenses: Products A, B, C and D.

Profile 1 gives reading and writing access to Product A and read only access to product D.

Profile 2 gives reading and writing access to Product A, B, and D.

The person group has reading and writing access to product A only and is assigned Profiles 1 and 2.

Users connecting via the group with Profile 1 have only access to objects A with the permissions defined on the **Set of UI access rights** of Profile 1.

Users connecting via the group with Profile 2 have only access to objects A with the permissions defined on the **Set of UI access rights** of Profile 2.
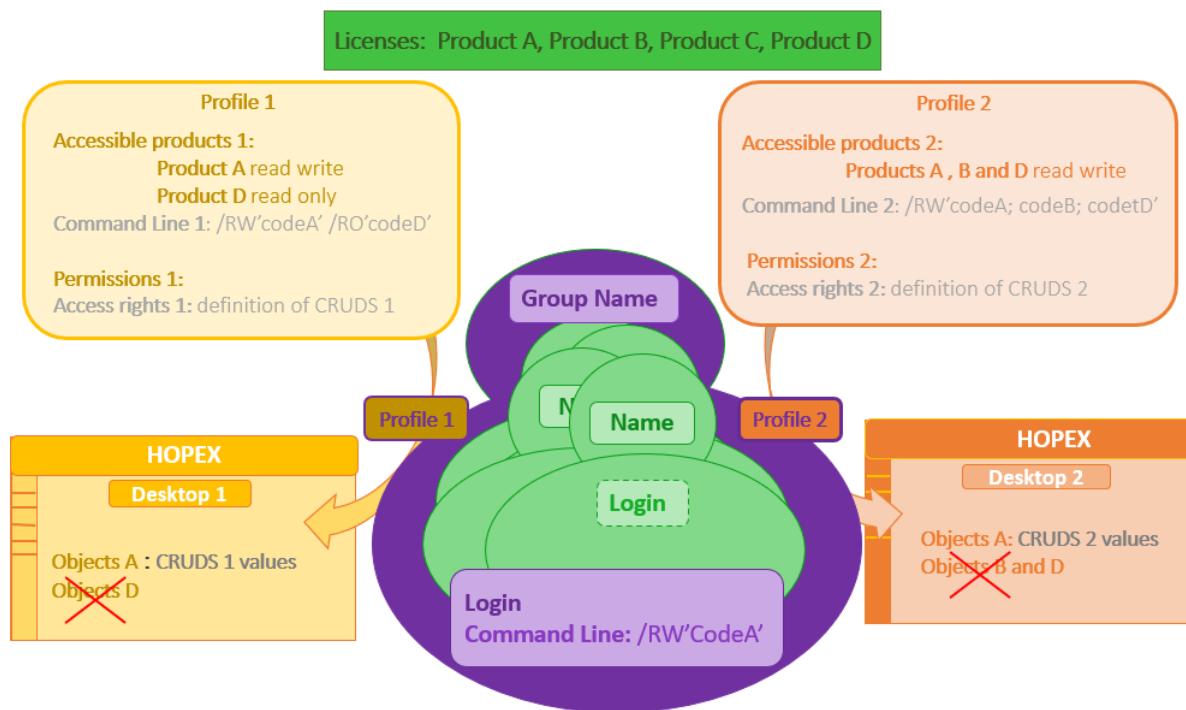
Restricting Object UI Accesses for a Profile (Permission)

Object UI access of a profile are defined by its associated **Set of UI access rights**.

To manage object UI access, see **Hopex Studio > Managing Permissions on Object UI** documentation.

> Example: the **Application Viewer** profile gives reading and searching access to applications (the **Permission** for **Application** MetaClass is: "RS"). This profile does not allow application creation, modification, or deletion.

Restricting General UI Accesses for a Profile (Permission)

General UI accesses are managed for a profile. General UIs are classified by category, like:

- desktop
- command category
- command group
- general command
- property page
- tree
- Working Environment Template (WET)

To manage the general UI accesses, see **Hopex Studio > Managing Permissions on Object UI** documentation.

> Example: the **Administration** navigation menu dedicated to GRC **(Working Environment Template > GRC > GRC –**

Administration) is not available for the **GRC Manager** profile.

Restricting Data Accesses Dynamically (macro)

The profile can be linked to a data access dynamic rule (reading or writing).

You can define dynamic rules for reading or writing data access.

Dynamic rule:
- applies to an object for given profiles
- is defined by a macro

To manage data access dynamically, see Managing Data Access Dynamically.

Restricting Data Accesses Statically

Writing access diagram (authorization) and reading access diagram (confidentiality) define data accesses statically.

A person sees objects belonging to his/her reading access area, and can modify objects belonging to his/her writing access area.

A person belonging to a person group and connecting via the group sees objects belonging to the group reading access area, and can modify objects belonging to the group writing access area.

To manage data accesses statically, see Data Writing Access and Data Reading Access.

Data writing access (authorization management)

Each user (or user group) is connected to a writing access area. It is the person (or person group) that carries the writing access area.

Each object is connected to a writing access area.

> ☛ *At creation, the object inherits the writing access area of the person who created it.*

MEGA delivers by default the "Administrator" writing access area, which is the highest writing access area level.

All other writing access areas depend on at least one writing access area.

Writing access areas are interconnected by hierarchical links. This is a strict hierarchy, with no circular dependencies: a writing access area cannot be declared at a higher level than the writing access area on which it depends, either directly or via a succession of dependencies.

A user can modify an object connected to his/her writing access area or to a hierarchically lower writing access area.

The writing access area of an object can be modified by the administrator:

- by specifically changing the object writing access area
- when modifying the writing access area of another object (project, process, diagram, etc.) if the propagation option is enabled.

Data reading access (confidentiality management)

Information related to the reading access area is only visible when the **Activate reading access diagram** option is selected in the environment Options (Options: **Compatibility > Windows Front-End > Administration**).

Certain objects or modeling projects may be confidential or contain data (costs, risks, controls) that should be visible only to authorized users.

The Hopex administrator can mask objects corresponding to this confidential or sensitive data.

To implement a data confidentiality policy, objects must be organized in distinct sets. Each set of objects is a reading access area.

Each user (or user group) is associated with a reading access area that determines the objects the user (or user group) can see. A user can only see objects located in his/her own reading access area or in the lower reading access areas.

REPOSITORY AND WORKSPACES

Workspaces are managed by the administrator.

The following points are covered here:

- ✓ Introduction to Workspaces
- ✓ Working in a Private Workspace
- ✓ Workspace Administration
- ✓ Private Workspace Life: Example
- ✓ Repository Performance and Health Tests
- ✓ Managing Updates
- ✓ Managing locks
- ✓ Managing Repository Snapshots

INTRODUCTION TO WORKSPACES

Workspace Types

Hopex gives access either to:
- a public workspace
- a private workspace, or
- read-only workspace

☛ *See Working in Hopex.*

☛ *The workspace type is defined by the WET (Working Environment template) properties associated with the desktop.*

Public workspace

In most management applications, the user cannot control the opening duration of his/her workspace: the end of a data entry stands for a definitive save of his/her work.

Private workspace

With private workspaces the user controls management of his/her workspace: opening, closing, dispatch, refresh.

Private Workspace Principle
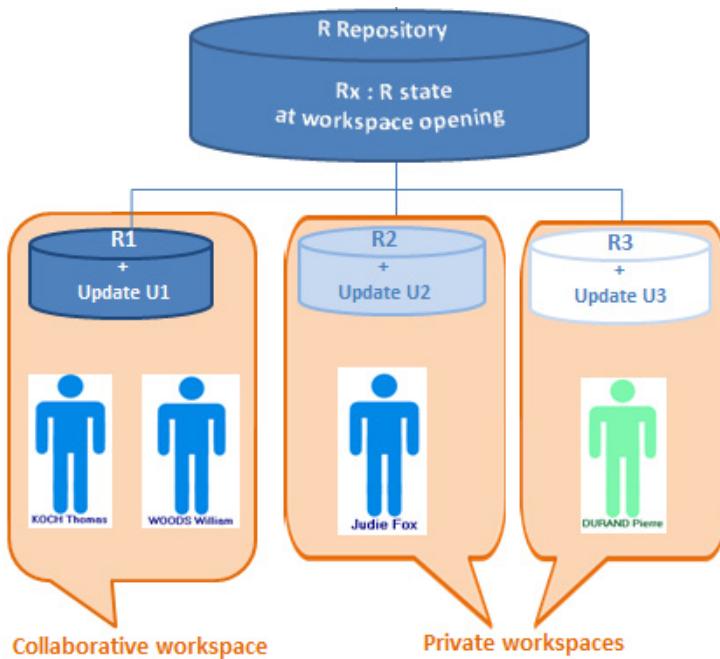
When a user connects to certain Web desktops, he/she opens a *private workspace*. This private workspace is a temporary view of the repository (repository snapshot) at the moment of user connection.

The user then sees:

- initial repository snapshot objects of his/her visibility scope
- updates he/she has executed on these objects.

The user decides when he/she wants to integrate his/her repository updates and make them visible to other users. To do this, he/she dispatches modifications.

> ☛ See *Dispatching Your Work*.

The user controls opening duration of his/her private workspace.

> ☛ *The private workspace is open for each user on both his/her repository and on the system repository. A private workspace always exists on system repository even if the user is not using any of the system repository objects.*

Several users can have private workspaces open in parallel. In his/her private workspace, the user is independent of updates carried out simultaneously by other users in their respective private workspaces.

> ☛ *Locks inform the user of objects modified by others. See Managing locks.*

The user can also update his/her private workspace with the updates of other users. To do this, the user refreshes his/her private workspace.

> ☛ See *Refreshing Data*.

Hopex allows several users to work at the same time.

WORKING IN A PRIVATE WORKSPACE

A private workspace is a temporary view of the work repository allocated to a user before the user dispatches his/her work. This view of the repository is only changed by modifications made by the workspace user, independently of concurrent modifications made by other users. This private workspace exists until it is refreshed, dispatched or discarded.

Note that a private workspace is kept when the user disconnects from the repository, unless the user indicates otherwise.

The following points are detailed here:

- Connecting to a Hopex Desktop
- Saving Sessions
- HOPEX Repository State Changes
- Dispatching Your Work
- Dispatch Conflicts
- Rejects When Dispatching
- Refreshing Data
- Conflicts When Refreshing
- Discarding Work
- Exiting a Session
- Workspace Administration
- Viewing Updates Dispatched in the Repository
- Managing locks

Connecting to a Hopex Desktop

When you connect to **Hopex**, you can:

- create a private workspace (if you do not already have one).

    ☛ *You can only have one private workspace open in the same environment.*

    ☛ *The private workspace is open for each user on both his/her repository and on the system repository. A private workspace always exists on system repository even if the user is not using any of the system repository objects.*

- resume work in your private workspace

To connect to a **Hopex** desktop:

1. Start the **Hopex** application from its HTTP address.

    ☛ *If you do not know this address, contact your administrator.*

    The connection page appears.
2. In the **Login** field, enter your identifier.
3. In the **Password** field, enter your password.

    ☛ *If you have lost your password, click **Forgot password**, see Resetting your Password.*

4. Click **Sign in**.
   When you have been authenticated, a new dialog box appears.

5. (If you belong to a person group) In the drop-down menu for groups, select the group with which you want to connect or "My assignments" to connect with one of your own assignments.

6. In the drop-down menu for repositories, select your work repository.

   ☞ *If you can access only one repository, this is automatically taken into account and the repository selection field does not appear.*

7. In the profile drop-down menu, select the profile with which you want to work.

8. Click **Enter**.
   A private workspace is created and your desktop opens.

   ☞ *If you already have a private workspace open, you should connect to it. If you want to change profile or repository, you must close the private workspace that is open.*

   ☞ *A user has up to one private workspace in progress in an environment.*

Saving Sessions

📖 *A session is the period during which a user is connected to a repository. A session begins when the user establishes connection and ends when he/she exits Hopex. Sessions and private workspaces can overlap. When you dispatch, refresh or discard a private workspace, a new private workspace is created in the same session. Conversely, a user can keep his/her private workspace when exiting a session.*

To save modifications you have made in your *session* since the last save:

1. In your **Hopex** desktop, click **Main Menu** 👤 .

2. Click **Save**.

   ☞ *These modifications are not saved in the repository. To save your modifications in the repository, you must dispatch these modifications, see Dispatching Your Work.*

Hopex Repository State Changes

The integrity of the repository is assured by successive changes in its state.

   ☞ *See example Private Workspace Life: Example.*

When repository updates are executed in a private workspace, they are only visible to other users when the user dispatches his/her work.

The repository changes from state N to state N+1 with memorization of new data related to the previous situation (state N).

If the user does not save updates, the changes made since the last valid state are forgotten. The repository remains in state N. Note that **Hopex** repository state changes are managed automatically.

A workspace opens on the latest states of the repository and system repository.

Dispatching Your Work

Dispatching consists in making public the updates carried out in a private workspace.
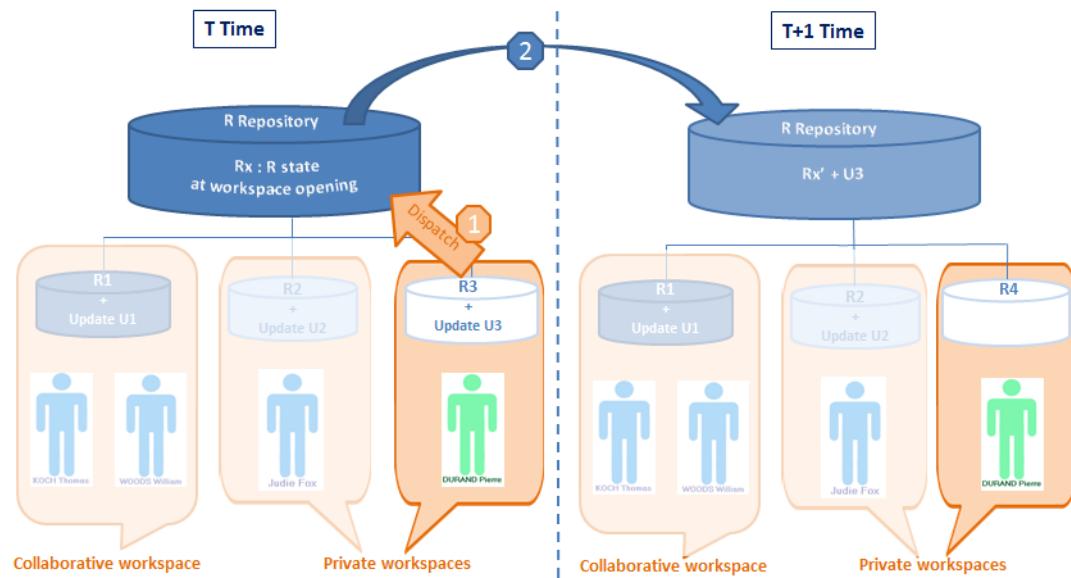
Dispatching allows:

- a user to make available to other users the modifications he/she has made to the repository.
- other users to have these updates available when they open a new workspace, whether this be after dispatch, refresh or discard of their current private workspace.

Dispatch:

- executes an update of the **Hopex** repository and the system repository.
- creates a new workspace for the user containing all updates since creation of his/her previous private workspace.

Note that only one user can dispatch at a time. When several users dispatch their work at the same time, a dialog box appears asking the user if he/she wants to queue his/her dispatch. This allows the user to exit **Hopex** without having to wait until the works from other queued private workspaces are dispatched.

☞ *See Dispatch Conflicts.*

From your Web desktop, to dispatch your work in the repository:

1. In your **Hopex** desktop, click **Main Menu** 👤 .
2. Click **Dispatch**.
   Your modifications are saved in the repository.

Dispatch Conflicts

The dispatch process automatically manages most conflicts that may arise when several users make updates.

Creation of duplicated objects

When duplicate objects are created, a prefix is added before the name of the second object.
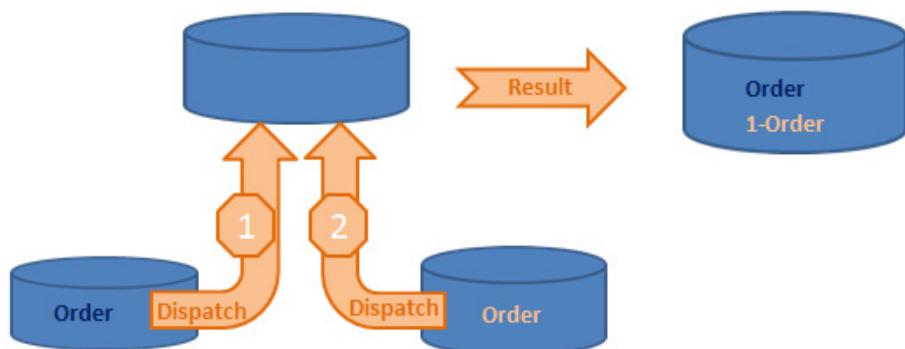

```
Two users create an object with the same name. The first to
dispatch his/her work actually creates the object. The
second user to dispatch his/her work creates an object with
a prefixed name.
```

This is indicated in the dispatch report.

The administrator or the users can then decide to rename one of these objects if they are actually different, or combine them into one object if they are in fact the same object.

Deletion of already deleted objects or links

As the deletion has already been performed, nothing happens. There is no mention of this in the dispatch report.

Modifying or linking a renamed object

This happens when a user modifies an object that in the interim has been renamed by another user, or tries to link something to this object. The new one is kept and the changes are executed normally. The object can be found using its *absolute identifier*. Note that this does not create a reject, but the dispatch report indicates that the object was renamed.

␇ *An absolute identifier is a string of characters associated with each object in the repository. This string is computed using the date and time the session was opened, the number of objects created since the session started, and the object creation date (in milliseconds). An absolute identifier provides a unique way to identify an object in the repository, so that even if the object is renamed, all the links to it are retained.*

Rejects When Dispatching

There are normally no rejects when dispatching work carried out in a private workspace. Most conflicts are managed automatically.

Rare cases of rejects are listed in the *rejects file*.

> 📖 *When updating a repository (importing, restoring, dispatching), a reject file is created in order to store rejected commands. Rejected commands are stored with the reason for which they were rejected. These are found in the "MegaCrd.txt" file located in the environment folder.*

Change in writing access values between opening and dispatching a private workspace

If you have access to the writing access management function, you can, for example, protect an object in the repository while a user is deleting it in his/her private workspace. When the user dispatches his/her work, he/she is no longer allowed to delete the object and the deletion is rejected.

Rename/create collisions

A user renames an object in his/her private workspace, for example, from "Customer" to "Customer*s*". Then another user dispatches his/her private workspace in which he/she created an object having the same name "Customer*s*".

When the first user dispatches his/her private workspace, since the "Customer*s*" object already exists, the object "Customer" cannot be renamed "Customer*s*". The rename command will therefore be rejected.

Verifying link uniqueness

A user creates a link for which there is a uniqueness check. For example, he/she indicates that the "Order" message is sent by the "Customer" org-unit. In the meantime, another user indicates in his/her private workspace that the "Order" message is sent by the "Customers" org-unit. When the second user dispatches his/her private workspace, the link is rejected if the uniqueness control imposes that a message can be sent by only one object.

> ☞ *See the **Hopex Power Studio - Imposing MetaAssociation Uniqueness** Technical Article for information on MetaAssociation uniqueness check.*

Attribute uniqueness (other than name)

Other attributes besides name may also be checked for uniqueness. If two users give two different objects the same value for this attribute, the second update will be rejected.

Updating a deleted object

If a user has made changes to an object in his/her private workspace and the object has been deleted by another user, the updates are rejected. The **Connect** and **Change** commands concerning this object are also rejected. All these rejects are listed in the private workspace report file.

Refreshing Data

A user can see modifications dispatched by other users of this repository without dispatching his/her own modifications. To do this, the user refreshes his/her data.

The system creates a new private workspace, into which the *private workspace log* of the user's previous modifications is automatically imported.

> 📖 *The private workspace log contains all modifications made by a user in his/her private workspace. It is applied to the repository at dispatch, then automatically reinitialized. This log is stored in the EMB private workspace file.*

Refreshing allows a user to incorporate repository and system repository changes made by other users, without dispatching current work.

Refreshing a private workspace:

- does not update repository or system repository state.
- does not unlock objects modified in the private workspace.

> ☞ see *Managing locks*.

When a user resumes work on his/her private space that has lasted longer than the limit set by the administrator (6 days by default), **Hopex** proposes that the user refreshes or dispatches his/her work.
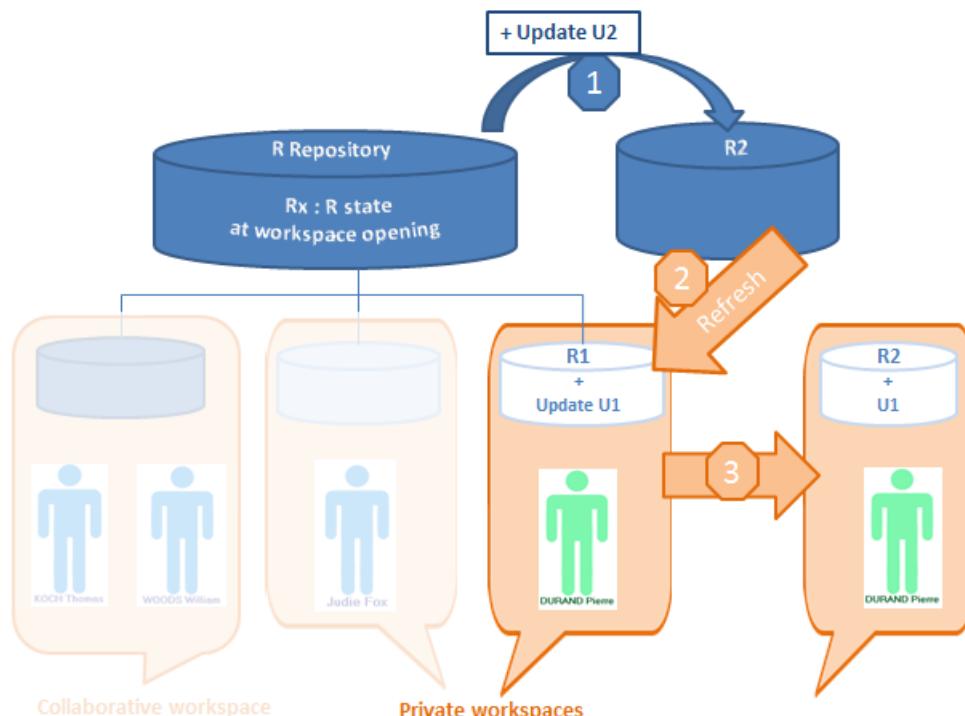
In your Web desktop, to update your workspace with data dispatched in the repository by the other users:

1. In your **Hopex** desktop, click **Main Menu** 😀 .

2. Click **Refresh**.

☞ *Your workspace is updated.*

Conflicts When Refreshing

Conflicts when refreshing are the same as when dispatching, but they apply to the private workspace only.

☞ *For more details on the main causes of rejects, see Dispatch Conflicts and Rejects When Dispatching.*
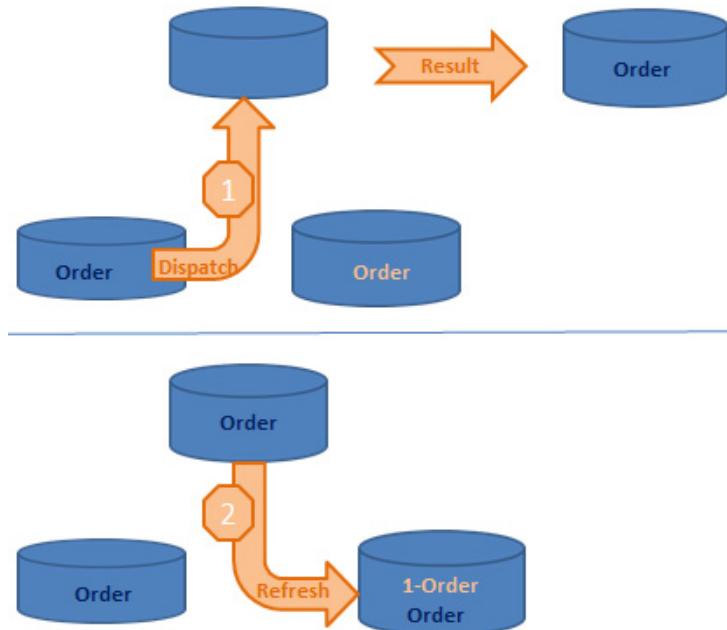
As is true in dispatching, if two objects are created with the same name, the second object name is prefixed:

```
The second "Order" object is renamed "1-Order".
```

Discarding Work

Discarding a workspace cancels all modifications made since the last dispatch. *Discarding* work causes loss of work carried out since opening of the private workspace, including modifications to the desktop. A warning message reminds the user of this. Use discard with care.

From your Web desktop, to discard your work:

1. (Optional) It is advisable to export the work performed in the private workspace before confirming the discard.

    ☛ *The administrator can export your private workspace log, see Exporting the Log .*

2. In the **Main Menu** 👤 , select **Discard**.

    ☛ *You can also discard your private workspace at disconnection, see Exiting a Session (choose not to dispatch modifications).*

Exiting a Session

When you exit **Hopex**, you close your session. You can:

*   save in the repository the modifications you have made in your private workspace
*   keep the modifications you have made in your private workspace

    ☛ *These modifications will remain awaiting validation, subsequent modification, or deletion.*

*   cancel modifications you have made.

From your Web desktop, to exit your work *session*:

1. From your **Hopex** desktop, click **Logout** 🔓.

    The **Hopex** exit dialog box appears.
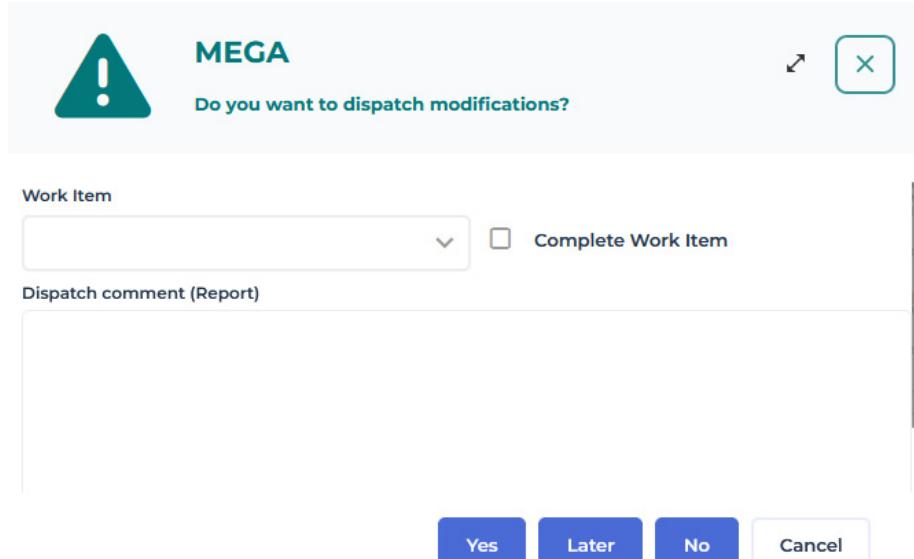
2. (Optional) In the **Dispatch comment (Report)** frame, enter a comment to remind you of modifications made in your private workspace.

3. Select your **Hopex** exit mode.

> ☛ *Click **Cancel** to not exit your private workspace.*

- **Yes**

Modifications you have made in your private workspace are saved in the repository.

> ☺ *In order to work effectively as a team, it is recommended that you dispatch frequently and regularly. Other users can update their own private workspace without dispatching their work (menu **File > Refresh**).*

> ☛ *This exit mode also allows the user to select a different repository the next time he/she logs in.*

- **No**

All modifications you made since your last dispatch will be lost. It is the recommended mode to exit without impacting the repository.

> ☛ *Modifications to your desktop are also lost.*

- **Later**

This option allows you to keep your changes without impacting the repository. You can open your session later and continue working but other users are not yet seeing the changes you have made.

> 💣 **You can have only one current private workspace. When you select the "Later" exit mode, any next session open in a private workspace re-opens the pending private workspace (the profile being the same or not). The private workspace exit mode is applied to all of the modifications you have made in this private workspace (desktops being the same or not).**

> ☛ ***When you switch the desktop (in private workspaces), if you want to keep your modifications in a desktop, it is recommended that you dispatch them.***

WORKSPACE ADMINISTRATION

You can view the list of current workspaces and their characteristics.
See:

- Accessing the Management Page for Workspaces
- Deleting a Workspace
- Exporting the Log
- Notifying Connected Users

Accessing the Management Page for Workspaces

To access the list of current workspaces in an environment:

1. Connect to the **Hopex Administration** desktop.

   ☞ *See Accessing Web Administration Desktop.*

2. Click the **Repository** navigation menu and select **Workspaces**.
   The management page for workspaces currently in progress in the environment appears.

Workspace Management

| ☑ Notify connected users | 🗃 Discard and Delete | 🗃 Publish and Delete | 🗃 Export logs | ⋮ |

☐	User	Type	Access Mode	Creation Date	Status	
☐	AIT AICHA Oth…	Public workspace (Micro)	Read/Write	5/12/2025 11:35:42 AM	Active	
☑	CORDEL Stéph…	Private workspace	Read/Write	5/7/2025 11:59:52 AM	Inactive	
☐	EL BABSIRI Ma…	Private workspace	Read/Write	5/8/2025 5:35:29 PM	Inactive	
☐	GLEVER Herve…	Public workspace (Micro)	Read/Write	5/12/2025 11:39:07 AM	Active	

« ‹ | Page 1 of 1 | › » | ↻ | Show 50 ⌃⌄ elements   Displaying 1 - 6 of 6

Persons who have accessed the workspace

Name	User ↑	Access Mo…	Duration (Days)	Session Start	Session End	Code	Status	▼
CORDEL S…	CORDEL …	Read/Write	5	5/7/2025 11:59:…	5/7/2025 12:35:…	SCL	Inactive	

The management page for workspaces currently in progress details the following for each workspace:

☛ *To sort workspaces according to a column, click the header of the corresponding column.*

☺ *You can also arrange columns in the order you want. To do this, click the header of the column to be moved and, holding down the mouse button, move it to the required position.*

- the **User** of the workspace
- the **Type** of workspace:
  - "Private Workspace":

    The user can modify data. His/her updates are kept in his/her private workspace until dispatched.
  - "Public Workspace (micro)":

    The user can modify data. As soon as he/she saves his/her updates, they are visible to other users.

    The user sees the updates of other users, as their updates progress.
- the **Access Mode** of the workspace, for example:
  - "Read/Write" when a session is open.
  - "Read-only" when the user is in consultation only.
  - no value, if the private workspace is passive (the user has saved his/her session but is not currently connected to **Hopex**).
  - no value if the user is in offline mode
- the **Creation date** of the workspace
- the **Status** of the workspace
  - active
  - inactive (for a private workspace)

The **Persons who have accessed the workspace** frame details:

- the **User** of the workspace
- the **Access Mode** of the workspace, for example:
- its **Duration** in days
- the start date and time of the last session
- the end date and time of the last session
- the user **Code**
- the user **Status**
  - active
  - inactive

Deleting a Workspace

The **Hopex** administrator can delete a private workspace when this is *inactive*.

To delete a workspace:

1. Access the workspace management page.

   ☛ *See Accessing the Management Page for Workspaces.*

2. Select the inactive workspace you want to delete and in the menu bar of the list, click:

> 💣 **When a workspace is deleted, the workspace in the work repository and that open on the system repository are deleted. Use private workspace deletion with care.**

- **Discard and Delete** 📇 if you want to delete the work performed in the workspace.

  > ☛ *The result is equivalent to discarding it.*

- **Export logs and Delete** 📇 if you want to export the workspace log (name: XXX_MM-DD-YYYY_hh.mm.ss) before discarding it and deleting it.

  `XXX: Login of the user who owns the deleted workspace`

  `MM-DD-YYYY: deletion date (month-day-year)`

  `hh.mm.ss: deletion time (hour.minute.second)`

  `E.g.: jwoods@mega.com_7-8-2024_5.56.58_PM.mgl`

  > ☛ *You, and the owner of the workspace, receive an e-mail with the deleted workspace log.*

- **Publish and Delete** 📇 if you want to keep the work performed in the workspace.

All users listed in the **Persons who have accessed the workspace** frame receive a notification e-mail concerning the deleted workspace.

Exporting the Log

The **Hopex** administrator can export a private workspace log when this is *inactive*.

The file is e-mailed, in .mgl format, to the administrator as well as as to the user concerned.

To export a private workspace log:

1. Access the workspace management page.

   > ☛ *See Accessing the Management Page for Workspaces.*

2. Select the inactive workspace you want to export.

   > ☛ *You can select several workspaces.*

3. In the menu bar of the list, click **Export logs** 📇 (name: XXX_MM-DD-YYYY_hh.mm.ss)

   `XXX: Login of the user who owns the exported workspace`

   `MM-DD-YYYY: exporting date (month-day-year)`

   `hh.mm.ss: exporting time (hour.minute.second)`

For each workspace concerned, an e-mail, including the exported data, is sent to the administrator and the user concerned.

Notifying Connected Users

The workspace management page shows the connected users (workspaces with "active" status)

You may need to notify these users (e.g.: to inform them about maintenance need).

To send an email to the connected users:

1. Access the workspace management page.

    ☛ See *Accessing the Management Page for Workspaces.*

2. In the menu bar of the list, click **Notify connected users**.
   An e-mail, with the users as recipients, appears.

3. Enter your message and send the e-mail.

PRIVATE WORKSPACE LIFE: EXAMPLE

To illustrate how private workspaces work, the following is an example of some steps in the work of several users:

Private workspace 1
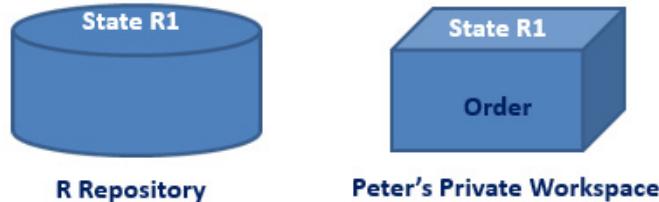
- Peter opens a private workspace, his repository view is state "n" (R1).
- He creates the "Order" message, which he links to the "Customer" org-unit.
- In parallel, Paul dispatches his private workspace...

Private workspace 2
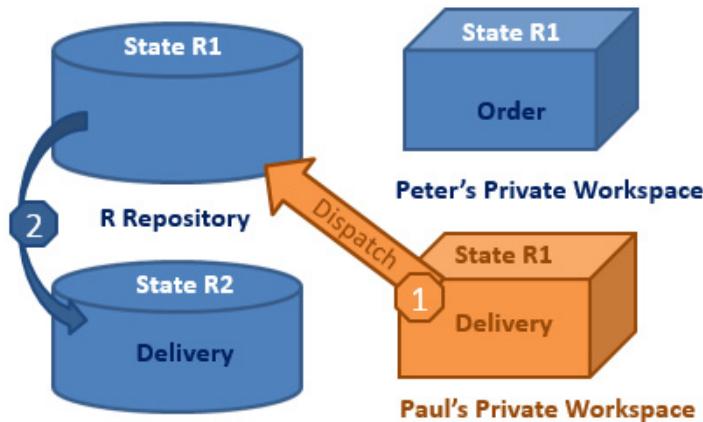
- The private workspace that Paul dispatched created the "Delivery" message, linked to the "Customer" org-unit.
- Paul's dispatch changes the repository to state "n+1" (R2).
- This new message is not seen from Peter's private workspace...

Private workspace 3
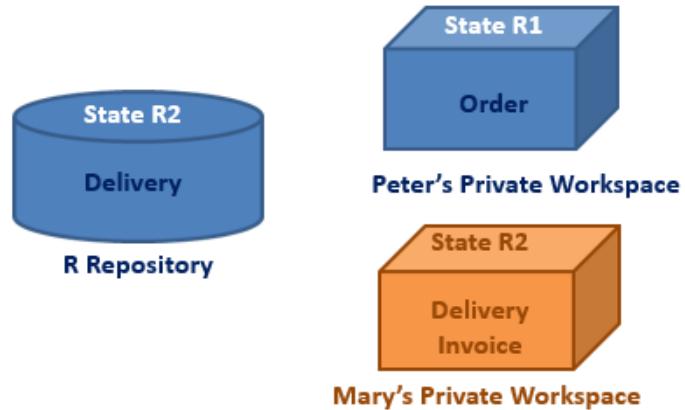
- Mary opens a new private workspace, her repository view is state "n+1" (R2).
- Mary creates the message "Invoice" connected to the "Customer" org-unit...

Private workspace 4
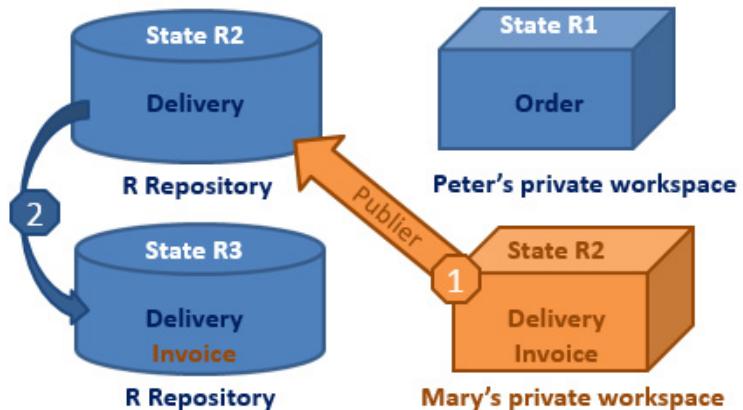
- Mary dispatches her private workspace.
- The repository moves to state "n+2" (R3).
- Peter's view is still in state "n" (R1).
- Peter refreshes his private workspace...

Private workspace 5
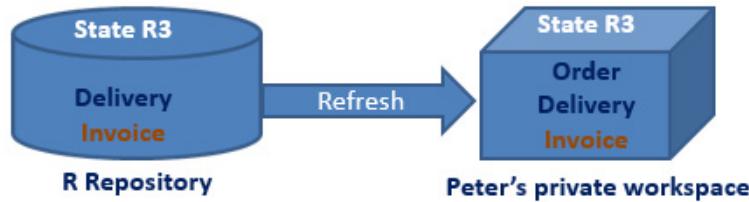
- Peter has refreshed his private workspace.
- His view now corresponds to state "n+2" (R3).
- He can now see the "Customer" org-unit with the additions made by Paul and Mary.
- Peter dispatches his private workspace...

Private workspace 6
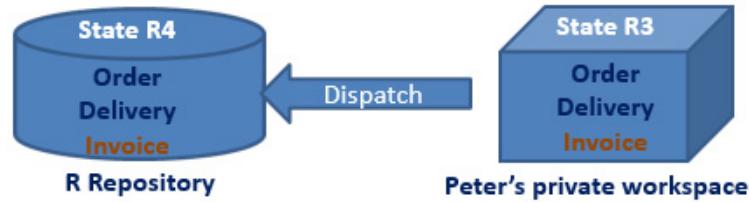
- When Peter, Paul, and Mary have dispatched their work, all the modifications they have made are visible in state "n+3" (R4) of the repository.

REPOSITORY PERFORMANCE AND HEALTH TESTS

With **Hopex** you can generate a daily repository health report. This report enables to detect:

- performance or usage anomalies that users can face daily.
- any significant change.

For this purpose, performance and health tests are run daily. Events are generated when anomalies are detected

☛ *See **HOPEX Administration > Technical Articles > Supervision Event Description >Repository Health***.

Test Description

Infrastructure performance test description

Hopex standard use scenarios are carried out every afternoon ("RepositoryHeath Daily Afternoon Trigger" job, 04:00 pm GMT):

- Reading of 1000 existing large objects (BLOB).
- Exploring an existing graph (1000 objects and 500 MetaAssociations).
- ERQL query on an existing graph (1000 objects and 500 MetaAssociations).
- Reading of 1000 large texts (BLOB).
- Creation of a graph including 1000 objects and 500 MetaAssociations.
- Deletion of a graph including 1000 objects and 500 MetaAssociations.
- ERQL query on a recently created graph (1000 objects and 500 MetaAssociations).

☛ *In a cluster-type configuration, performances are measured on all of the machines.*

Each scenario generates a result, which is stored in the repository. These results are analyzed daily in the evening ("RepositoryHeath Daily Evening Post Trigger" job, 11:05 pm GMT)

An history of 30 results are needed before generating an alert.

Repository health test description

It is essential to analyze certain usages to identify anything that might compromise data integrity, whether in the daily work or following a **Hopex** update.

For all of the repositories of all of the environments, the following checks are performed every evening ("RepositoryHeath Daily Evening Trigger" job, 11:00 pm):

- Administration
  - Compatibility checks between the SQL structure of the data and the server version.
  - table fragmentation
  - index fragmentation
  - SQL maintenance plan execution
- Customization
  - Hopex data modification
  - Hopex data volume
- Usage
  - workspace volume

> ☛ *In a cluster-type configuration, usage tests are performed randomly on a single machine only.*

Viewing the Hopex Health Reports

Accessing Hopex daily health reports

The **Administration** desktop gives access to Hopex daily health reports. Each report includes the anomalies detected on all the machines, in all the repositories. Reports are listed chronologically (the oldest first) in the following format:

```
HopexHealthFullReportYYYY-MM-DD_hh-mm-ss.html
```

with: YYYY: year, MM: month, DD: day, hh: hours, mm: minutes, and ss : seconds.

> ☛ *To access the content of the Repository navigation menu, you must be an advanced user. In Options > Workspace > Desktop, the **Display advanced UI** option must be selected.*

To view Hopex daily health reports:

1. Connect to the **Administration** desktop.

   > ☛ *See Accessing Web Administration Desktop.*

2. Click the **Repository** navigation menu and select **Repository Health Reports**.

3. In the report list, hover the cursor over the report of interest and click **Download report** ![download icon].

   ☞ *The last report is as the top of the list.*

The report is available in your downloads.

HOPEX Health Report Details

Deployment Health

Host: 1700-200-T6948 (-)

No alerts detected on this host.

Infrastructure Alerts (-)

Host: 1700-200-T6948 (-)

No abnormal performances detected on this host.

Data Alerts (-)

Environment: EnvTestsLab_1700_200_tst_6948 (-)

Repository: DEMO (-)

⚠ **SQL Maintenance Alert (+)**

Mitigation: With your DBA, schedule the SQL maintenance plan - at least - every week. If the problem persist, reduce the time frame between two maintenance plan executions.

Repository: EA (-)

No alerts detected on this repository.

Repository: SOHO (-)

⚠ **SQL Maintenance Alert (+)**

Mitigation: With your DBA, schedule the SQL maintenance plan - at least - every week. If the problem persist, reduce the time frame between two maintenance plan executions.

⚠ **Data Volume Alert (+)**

Exceeding the maximum number of recommended objects may rise usage/ergonomic problems.
Mitigation: Please call or email your MEGA contact to confirm users might not face issues using HOPEX.

Repository: SystemDb (-)

⚠ **Missing Compiled Data Alert (+)**

Keeping MetaModel and/or technical data not compiled may reduce performances of HOPEX.
Mitigation: Check - with Administration - why compiled data are missing and how to compile them.

⚠ **Customization Alert (+)**

Adding so many MetaAttributes is not recommended as it can generate regressions during updates/migrations.
Mitigation: Check with the responsible for the customization that the situation is under control.

4. Click (+)/(-) beside the name of the machine, environment, repository, or aler to display/hide its details.

Hopex Health report description

The Hopex health report includes a short description of the anomalies detected at performance or usage level. It shows alerts detected at:

- infrastructure level (**Infrastructure Alerts**)
- data level (**Data Alerts**) for each repository of each environment

> Example : detection of three alerts ("Query Execution Alert", "Macro Execution Alert" and "Data Volume Alert") at data level, on "Soho" repository.

MANAGING UPDATES

During their modeling work, users make additions to a **Hopex** repository within their workspace: for example they create objects, links between objects, diagrams.

Updates corresponding to user actions can be viewed in detail.

You can back up the modifications made to a repository: export each dispatch in the form of a command file.

The following points are detailed here:

- Viewing Updates Dispatched in the Repository
- Private Workspaces and Repository Size
- Managing locks

Viewing Updates Dispatched in the Repository

☛ *If you have created your own administration profile, to have access to the **Repository** navigation menu content, you must be an advanced user. In **Options > Workspace > Desktop**, the **Display advanced UI** option must be selected.*

You can view the activity on:

- the current data repository
- the SystemDb repository

For each repository, you can display its dispatches as:

- a list, which you can filter by user and/or date
  You can display the actions and access its code details.
- a tree, which sorts the dispatches by day, week, month
  You can directly display the actions in the tree.

To export the log, see Managing locks.

Viewing a dispatch (list)

To view the updates dispatched in the repository:

1. Connect to the **Administration** desktop.

   ☛ See *Accessing Web Administration Desktop.*

2. Click the **Repository** navigation menu and select **Repository Activity**.
   All the dispatches (private and public workspaces) performed on the data repository are displayed by date (the latest at the top).

3. (To display the SystemDb repository activity) Click **SystemDb Repository**.
   All the dispatches (private and public workspaces) performed on the SystemDb repository are displayed by date (the latest at the top).

4. In the list, click the dispatch.

☺ *You can use the list filtering tool to help you find the dispatch.*

The **Characteristics** property page of the dispatch displays, with the dispatch WI **Description** if any.

5. Display the **Updates** page.
The actions contained in the dispatch are detailed.
6. (If needed) Select a row to display the action details on the right.

Viewing a dispatch (tree by date)

To view a dispatch from a tree:

1. Connect to the **Administration** desktop.

2. Click the **Repository** navigation menu and select **Repository Activity**

 ▤▶.

All the dispatches (private and public workspaces) performed on the current and system repositories are sorted in folders by day, week, and month.

Repository Activity   ✕

⊟ ⊞   Search...   🔍

⊟ 🛢 DEMO

⊞ 📁 Today

⊞ 📁 Yesterday

⊞ 📁 This Week

⊞ 📁 Last Week

⊞ 📁 Two Weeks Ago

⊞ 📁 This Month

⊞ 📁 Last month

⊞ 📁 Before One Month

⊟ 🛢 SystemDb

⊞ 📁 Today

⊞ 📁 Yesterday

⊞ 📁 This week

3. In the repository folder concerned (**Data** or **SystemDb**) expand the folders (date and dispatch) to access the content of interest.

☺ *You can use the tree search tool to help you find the dispatch.*

The actions contained in the dispatch display.

4. If needed, hover the cursor over the dispatch and select **Properties** ⌫ or **Open in new tab** ⌫ to display the dispatch content as a list in the edit area.

☞ *See Viewing a dispatch (list).*

5. Display the **Updates** page.
The **Updates** page details the content of the dispatch as a list of actions displayed in chronological order.

6. (If needed) Select a row to display the action details on the right.

Private Workspaces and Repository Size

Private workspace life

A private workspace gives a user a frozen view of a repository.

When the repository is modified by other dispatched private workspaces, this private workspace keeps the view it had when created.

Since the data corresponding to these views is kept in the repository, its size grows, and may become disproportionate to the actual repository contents.

☞ See *Dispatching Your Work* and *Refreshing Data.*

Private workspace monitoring

More than one user can connect to a single repository via network share. The first time a user connects to the repository, he/she opens a private workspace. This private workspace ends only when the user dispatches, discards, or refreshes his/her modifications, and not when simply disconnecting from the **Hopex** repository.

☞ See *Refreshing Data* and *Discarding Work.*

Modifications made by the user are saved in a temporary space (data) in his/her private workspace dedicated to the data of his/her private workspace. The repository is updated only when the user dispatches these changes.

☞ See *Dispatching Your Work.*

All data accessed by a user is "frozen" for the duration of the private workspace.

Example:

```
If an object is renamed in the reference repository after
the private workspace is opened, the user sees the previous
name unless the private workspace is refreshed. However,
users connecting after the modification has been dispatched
```

> will have a view reflecting the latest state of the
> repository.
>
> If other users connected before you dispatch your updates,
> and are accessing the same data as you, they will have an
> obsolete view of the data until they refresh their private
> workspace. Note that when you dispatch your updates, your
> view is refreshed automatically.

This means that data being accessed by user A and modified at the same time by user B is duplicated. It is stored in its initial state for each user private workspace; if a user makes a change, the previous state is stored along with the new one.

When the updates are dispatched and all users accessing the updated data have refreshed their private workspaces, the previous state is no longer required.

Modifying the maximum duration of a private workspace

By default the maximum duration of a private workspace is 6 days

Once this duration has elapsed, at connection, a message prompts the user to dispatch or refresh his/her private workspace.

To modify the maximum duration of a private workspace:

1. Connect to the **Administration** desktop.

    ☛ See *Accessing Web Administration Desktop.*

2. Click the **Environment Options** navigation menu.
3. Access the **Installation > Advanced** options.
4. Modify the **Recommended open workspace duration** option value (in day).

MANAGING LOCKS

When several users are connected to the same repository simultaneously, there may be conflicts when they modify the same object in their different private workspaces.

See:

- Principle
- Managing Locks on Objects

Principle

With the network version, concurrent accesses to objects can be checked using *locks*.

Preventing conflicts

As soon as a user modifies an object, a lock is placed on this object. Another user can thus only view this object. This user cannot access a new update until the first user dispatches his/her private workspace, and he/she refreshes his/her private workspace. This prevents conflicts between the state of the object in the repository and the obsolete view of the second user.

Deleting a lock or unlocking an object

Lock management is automatic. You do not normally need to delete locks or unlock objects.

The few exceptions are due to abnormal operations, for example when a private workspace has been deleted from the private Workspace management window, or at desynchronization of clocks.

When a lock is deleted, another user can modify the object without dispatching or refreshing his/her private workspace.

> ☛ *A user can delete locks placed on his/her private workspace since its creation.*

When a user dispatches his/her work, the lock (his/she had placed on an object) is unlocked but not deleted. The lock is deleted only when all other private workspaces, which were created before the lock was unlocked, are closed. A private workspace is closed when it is dispatched, discarded, or refreshed.

Details on the operating method of the locks

Hopex only indicates that objects are locked when their attributes are modified (unlike links for example).

Warning on unlocking

If you attempted to use an object that was locked, a message alerts you as soon as the object is freed for you to use again.

Diagrams

There are two types of locking applied to diagrams

- **The diagram has simply been viewed and not modified**: as soon as the first user closes the diagram it can be opened by a second user.
- **The diagram has been modified**: as for classical locking, the second user must wait until the diagram has been dispatched by the first user and therefore unlocked.

Managing Locks on Objects

The **Lock Management** page of the **Administration** desktop provides access to:

- the **Locks** page, which details for each lock:
  - the **Name** of the object concerned
  - the **Type** of object concerned
  - the **User** who owns the lock
  - the dates and times (GMT0): **Lock Date** and, where appropriate, **Unlock Date**
  - The **Status** of the object concerned (protected or not)

    ☛ See *Viewing locks on objects.*

- the **Immutable Locks** page, which details the following for each immutable lock:
  - the **Name** of the object concerned
  - the **Type** of object concerned
  - the **User** who owns the lock
  - its **Lock Date** and time (GMT0).
  - The **Status** of the object concerned (protected or not)

    ☛ See *Managing immutable locks on objects.*

For each object locked with an immutable lock, you can:

- unlock the object to remove its immutability
- unlock the object and propagate, to remove its immutability and that of its child.

Viewing locks on objects

To view the locks:

1. Connect to the **Administration** desktop.

   ☛ See *Accessing Web Administration Desktop.*

2. Click the **Repository** navigation menu and select **Locks**.
   The **Lock Management** page appears and displays by default the **Locks** list.

3. (Optional) To sort locks according to column, click the column header.

☺ *You can also arrange columns in the order you want. To do this, click the header of the column to be moved and, holding down the mouse button, move it to the required position.*

	Name	Type	User	Lock Date	Unlock Date	Status
☐	Airport::* MEGA Airport::AA Titi Co	Term	NOURY ...	2025/05/09 14:25:02	2025/05/09 14:25:26	Not Locked
☐	Airport::* MEGA Airport::Concept	Term	NOURY ...	2025/05/09 14:24:53	2025/05/09 14:25:26	Not Locked
☐	Airport::Account Management (EN) Ebauche...	Sketch	SOULAI...	2025/05/07 14:59:47	2025/05/07 15:24:35	Not Locked
☐	Airport::Account Management (EN) Ebauche...	Sketching Item	SOULAI...	2025/05/07 15:00:24	2025/05/07 15:24:35	Not Locked
☐	Airport::Account Management (EN) Ebauche...	Sketching Item	SOULAI...	2025/05/07 15:00:17	2025/05/07 15:24:35	Not Locked
☐	Airport::Account Management (EN) Ebauche...	Sketching Item	SOULAI...	2025/05/07 15:00:24	2025/05/07 15:24:35	Not Locked

Lock Management — Locks | Immutable Locks

« ‹ | Page 1 of 5 | › » | ↻ | Show 50 elements — Displaying 1 - 50 of 232

Managing immutable locks on objects

To manage immutable locks:

1. Connect to the **Administration** desktop.

   ☛ *See Accessing Web Administration Desktop.*

2. Click the **Repository** navigation menu and select **Locks**.
   The list of locks is displayed.

3. Click **Immutable Locks**.

4. (Optional) To sort immutable locks according to column, click the column header.

   ☺ *You can also arrange columns in the order you want. To do this, click the header of the column to be moved and, holding down the mouse button, move it to the required position.*

5. Select the immutable lock (you can select more than one) and:

- click **Unlock** 🔓 to remove its immutability.
- click **Unlock and Propagate** 🔓 to remove its immutability and that of its child locks.

The immutable lock is deleted.

You, and the person who set the lock receive a notification e-mail.

MANAGING REPOSITORY SNAPSHOTS

To use repository snapshots, you must:

- check that the repository log is enabled (default value).
- set up a procedure for taking account of repository snapshots before deletion of historical data.
  A repository snapshot captures a historical state of the repository. When a historical state of the repository has been deleted, it is no longer possible to create a repository snapshot that captures this state.

  It is therefore important to take management of repository snapshots into account when deleting historical data (in Administration.exe, via the repository pop-up menu: **Administration RDBMS > Shrink unused repository historical data**).

  ☛ *For more details, see "Repository - RDBMS Installation Guide", "Hopex Historical Data Cleanup".*

Creating a Repository Snapshot

To create a repository snapshot:

1. Connect to the **Administration** desktop.

   ☛ *See Accessing Web Administration Desktop.*

2. Click the **Repository** navigation menu and select **Repository Snapshots**.

3. In the edit area, click **New** ✚.
   A creation wizard appears.

4. (Optional) In the **Name** field, enter the repository snapshot name.

5. Select the criterion to be used to find the state of the repository to be captured:
   - Task (design task)
   - Dispatch

6. Click **Next**.

7. Select the task or dispatch.

8. Click **OK**.

   ☛ *You can schedule repository snapshot creation with the scheduler. For more details, see Scheduling.*

Scheduling automatic repository snapshot creation

To schedule repository snapshot creation:

1. Connect to the **Administration** desktop.

   ☛ *See Accessing Web Administration Desktop.*

2. Click the **Repository** navigation menu and select **Repository Snapshots**.

3. Click **Automated snapshots** 📷.

4. Click **Activate**.

5. Configure the frequency.

☺ *For example, you can schedule the frequency of repository snapshot creation to once a week.*

☛ *See Defining a Trigger Scheduling.*

6. Click **OK**.

OBJECTS

The following points are covered here:

- ✓ Importing - Exporting a Command File
- ✓ Comparing and Aligning Objects Between Repositories
- ✓ Merging Objects

IMPORTING - EXPORTING A COMMAND FILE

Export of an object with propagation enables creation of a consistent set allowing transfer of part of the repository to another repository. For example, export of **Hopex** objects from a library includes objects present in the library and their dependent objects.

From your **Administration** Web desktop, you can import command files to a **Hopex** repository:

☛ *See Importing a Command File into Hopex.*

- in **text format** (.MG*).

☛ *For more details on .MG* file syntax, see Command File Syntax.*

- In **Bizzdesign XML format**. These files have .XMG extension and contain commands or data (objects and links).

☛ *For more details on MEGA XML data exchange format, see technical article MEGA Data Exchange XML Format EN.*

The following points are detailed here:

- Importing a Command File into Hopex
- Exporting Objects

Importing a Command File into Hopex

You can update a repository by importing a command file produced by the repository backup tool, an export file of an object, or any other means of command file production.

Data import authorization depends on the **Hopex data import (XMG, MGR, MGL)** option.

☛ *See Modifying Data Import Authorization.*

By default, you can update:

- authorized to all profiles:
  - the **Data** (most frequent case)
- restricted to *Hopex Administrator* profile:
  - the **Metamodel** (repository structure)
  - the **Technical Data** (*descriptions*, *queries*, as well as *users*).

To export a command file from the **Administration** desktop:

1. Connect to the **Administration** desktop.

☛ *See Accessing Web Administration Desktop.*

2. From the main menu, select **Import > Hopex Files**.
   The **Parameterization** window opens.

3. In the **Command File** field, click **Browse** to browse the folders and select the backup file.

☛ *The command file must not exceed 30 MB.*

4. (If needed) Select the types of **Processing** to be executed:
    - **Data**
    - **Metamodel**
    - **Technical Data**

    ☞ *If the file includes commands that do not match the type you have selected, these commands are ignored.*

5. (If needed) Modify **Save** frequency of the modifications.

    ☞ *Note that there is no optimal save frequency:*

    - ***Standard*** *frequency saves at each "Validate" command in the command file and at the end of the file. This type of frequency is useful when the command file has been written by a user.*
    - ***At end*** *is generally sufficient if the file is not very large.*
    - ***At end if no reject encountered*** *saves the changes only if no rejects were encountered.*
    - ***Never*** *is used to carry out tests before the effective update, for example for syntax checking.*

6. In the **Checks** pane, the checks to be carried out are selected automatically, based on the file extension:
    - **Check Absolute Identifiers** is not selected in the case of a command file that does not come from a **Hopex** repository.
    - **Control writing access areas** is selected when the **Hopex Power Supervisor** technical module is available on the site, ensuring that the user who executed the update has the corresponding writing access in the repository.

    ☞ *For command files with the **MGR** extension (repository backup), absolute identifiers are included in the imported objects and writing access levels are kept.*

    ☞ *For command files with the **MGL** extension (log extraction), the absolute identifiers are included in the imported objects. Writing access levels are kept if the updates are consistent with the writing access diagram for the environment.*

    ☞ *These controls are not carried out if the user level is "Administrator", this enables the data restorations.*

7. In the **Filters** pane, select the import behavior to be applied:
    - **Standard Reprocessing** changes creation of an already existing object into a modification, or into creation of an object of the same name preceded by a number if their absolute identifiers are different.
    - **Reassign User** ignores the writing accesses contained in the imported file. All elements in the imported file are given the same writing access level as the user executing the import. This is useful when you have the **Hopex Power Supervisor** technical module. The creator and modifier names are replaced with the name of the user executing the import.

    ☞ *It is recommended that you enable this option when the import file comes from an environment where the writing access diagram is not the same as the one for the environment where this file is being imported.*

    The options you select are controlled by the software, based on the file extension and the standard processing to be applied. If your choices are

not consistent with the file extension, a message box informs you of this fact and its possible consequences.

☞ *For more details on the main causes of rejects, see Dispatch Conflicts and Rejects When Dispatching.*
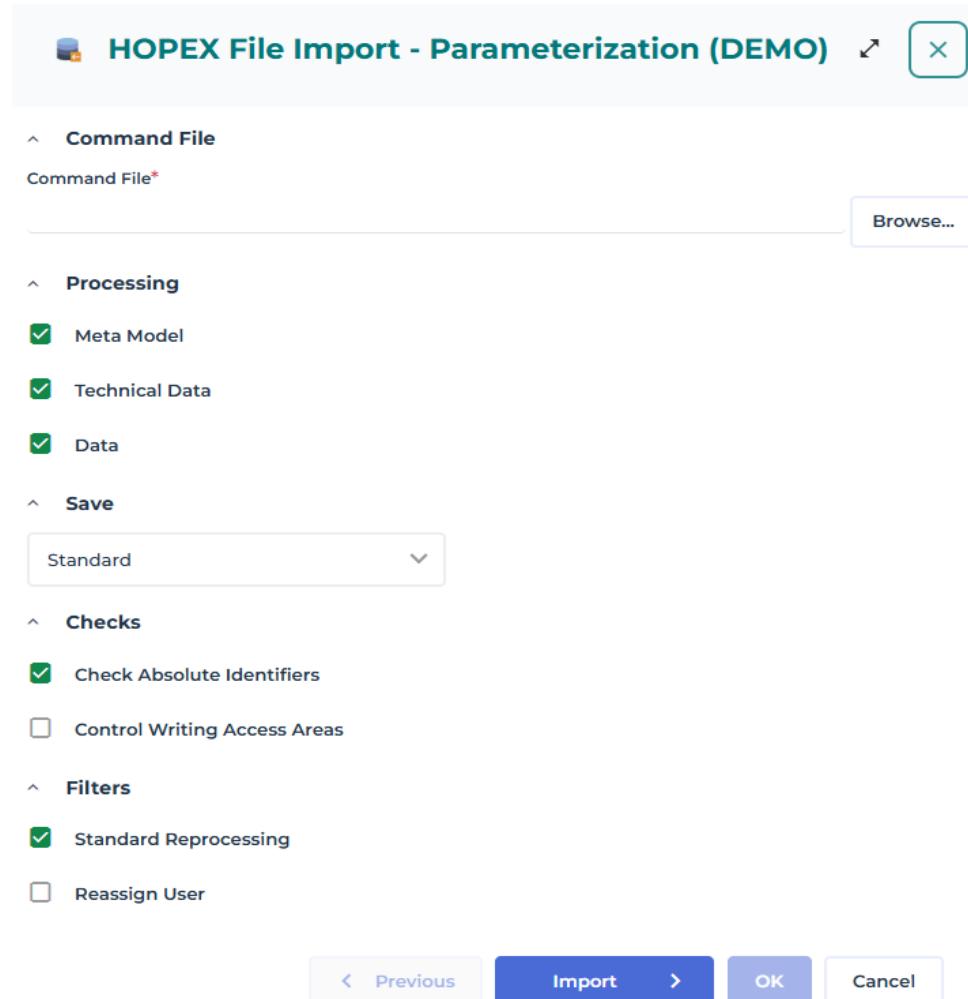
8. Click **Import**.
When the import contains errors, a reject report file is generated.

9. (If needed) To display the rejects (or errors) saved during the command file import, in the **Report** section, click the **Report File** field arrow and select **Open**.

☛ *The contents of the report file depend on import options. For more details on importing a command file, see* *Options*.

Case of a text file import (MGR, MGL): The report file appears and details all the rejects.

Example of rejects file at MGR file import

Exporting Objects

You can export **Hopex** objects from the **Administration** desktop:

You can export objects in the following formats:

- **Text** (by default)
  The exported file is in the form of an .MGR file.

    ☛ *For more details on .MGR file syntax, see Command File Syntax.*

- **Bizzdesign XML**
  The exported file is in the form of an *.XMG file containing commands or data (objects and links).

    ☛ *For more details on MEGA XML data exchange format, see technical article "MEGA Data Exchange XML Format".*

To export **Hopex** objects from the **Administration** desktop:

1. Connect to the **Administration** desktop.

    ☛ *See Accessing Web Administration Desktop.*

2. From the main menu, select **Export > Hopex Objects export**.
   The **Parameterization** window opens.

3. (If needed) In the **Destination** section, in the **Export File** field, modify:
   - the file format (text format by default)
   - the file name

     ```
     File name format: "OBJmmdd000.mgr"
     ```

     ```
     where "mmdd" stands for the month and day of the export, and "000" a 3-digit number.
     ```

4. In the **Options** section, by default, two export parameterization options are selected:
   - **Include Objects of Merging**: exports the technical objects resulting from the object merging (_TransferredObject).
   - **Propagate**: exports the objects listed together with their dependent objects.

5. In the **Objects to export** section, click **Add objects to list** .
   The query dialog box appears.

6. Launch the search and select the appropriate objects in the result window.

7. Click **OK**.
   The objects appear in the list of objects to be exported.

   You can carry out these steps several times, for example to export objects of different types.

    ☛ *In case of mistake, click **Remove objects from list** to delete an object from the list.*

8. When selection is complete, click **Export**.
   The export file is exported.

9. (Optional) If required, in the **Export File** field, click the arrow and select **Open** to read the contents of the export file.

10. Click **OK**.
    The exported file can then be imported into another repository.

    ☛ *See Importing a Command File into Hopex.*

COMPARING AND ALIGNING OBJECTS BETWEEN REPOSITORIES

Hopex enables comparison and alignment of:

- two complete repositories
- objects in different repositories
- objects of the public repository with those of the current private workspace.
- two archived states from current repository

☛ *The objects compared must not be in the same private workspace.*

See:

- Compare and Align Principle
- Compare and Align Warnings
- Compare and Align

Compare and Align Principle

The principle of comparing and aligning objects between repositories is as follows:

1. ***Extraction***

   The selected objects and any linked objects are extracted from the two repositories, browsing links according to **Hopex** principles of object extraction.

   Comparison

   The two sets of data are compared on the basis of *absolute identifiers* of the objects they contain.

2. ***Comparison result***

   A window displays the results of the comparison. You can also generate a report and a command file in this window.

   ☛ *The page showing differences displays a maximum of 1000 lines. If the list of differences is greater than 1000 lines, a message prompts you to either ignore this limit and display all the lines (in this case, the list may take some time to load) or not.*

3. ***Alignment***

   The upgrade command file is imported in the target repository.

Compare and Align Warnings

You must be aware of the following points before alignment and selection of the user executing alignment.

💣 **In case the compare and align includes a large amount of data, this action can take some time and slow down Hopex**

performance. Remember to perform this action when Hopex users are not connected.

Repository log

The repository log lists all modifications made in the repository. It gives users a better understanding of actions executed in a repository in private workspaces. Each time an action is executed, an occurrence of Change Item is created.

The repository log is not transferred from one repository to the other: a new log is created in the target repository. Object history is not therefore kept.

Users

The creator/modifier of an object in the target repository is the user executing the alignment.

The date of creation of an object is the date on which alignment was executed.

Reading (confidentiality) and writing access levels

Writing and reading access levels are taken into account during the comparison and during the alignment.

To perform a comparison and an alignment, you must have reading access (if reading access management is activated) and maximum reading access for all objects in the repository.

☛ *Reject files are generated on completion of alignment. To delete the files, in the environment options* **Options > Tools > Data Exchange > Import/Export Synchronization > MEGA**, *select the* **Delete files produced at compare/align on completion of processing** *option.*

Compare and Align

The Compare and Align feature is available in all the desktops (Administration, Functional Administration, and Solutions).

☛ *Before comparing and aligning, see* Compare and Align Warnings.

To compare and align:

1. Connect to Hopex with the profile concerned.

    ☛ *See* Accessing Web Administration Desktop *or* Logging in to Hopex.

2. In the edit area, right-click an object and select **Manage > Compare and Align**.
   The object comparison wizard opens.

3. Indicate if you want to compare:
   * two repositories
   * two current repository archived states

4. Click **Next**.

5. Select:
   - the **Source repository**
   - the **Target repository**, which is the repository to be updated.

     ☛ *It can be a private workspace of the repository.*

6. (Optional) If required, you can choose to **Compare all repository objects**. Select the option an go to step 10.

   ☛ ***Warning***: *processing of this option can be time-consuming.*

7. Click **Next**.
   The dialog box for selection of objects to be compared opens.

8. In the **Perimeter** field, select the perimeter type (by default **Standard for Comparison**)

   ☛ *For detailed information on perimeters, see the **Hopex Power Studio - Perimeters** technical article.*

9. In the **Elements to compare** pane, select:

   - **Add from source** ▶ to add objects from the source repository, or

   - **Add from target** ◀ to add objects from the target repository.

     ☛ *If you have opened the comparison wizard from an object, this object is automatically added in the list of objects to be compared.*

10. Click **Next**.
The **Comparison Progress** window opens. It presents the differences between compared objects and their modifications.

Comparison - Comparison Progress

Difference list

	Order ↑	Difference	Kind	Target	Object 1	Object 2
+	1	Created	Object	Application	* MEGA BANK Mobi...	
🔗	2	Connected	Link	(Application/Application...	* MEGA BANK Mobi...	Bank Mobile App - Back
+	986	Created	Object	Deployable Application ...	Bank Mobile App - ...	
🔗	3	Connected	Link	(Workflow Status/Work...	* MEGA BANK Mobi...	Validation in Progress
🔗	4	Connected	Link	Persona Right Reference	* MEGA BANK Mobi...	Access
🔗	5	Connected	Link	Class of IT Service Enabl...	* MEGA BANK Mobi...	Mobile SDK

« ‹ | Page 1 › ↻ | Show 50 elements Curr...

Generate a difference file

Export to CSV

‹ Previous   Next ›   OK   Cancel

The **Difference** column presents differences by update category:

- **Created**: objects not existing in the target repository.
- **Deleted**: objects existing in the target repository but not in the source repository.

    ☛ *Deletion commands of compare and align can be generated in a separate file. For this purpose, activate the corresponding option in*

Options > Tools > Data Exchange > Import/Export Synchronization > MEGA.

- **Modified**: objects of which characteristics, including name, have been modified.
- **Connected**: links, between two objects, that do not exist in the target repository.
- **Disconnected**: links existing in the target repository but not in the source repository.
- **Changed**: links for which a characteristic has been modified.

The **Type** column presents differences by type.

11. (Optional) Click:
    - **Generate a difference file** to generate a file (.mgr format) that contains the list of differences detected.
    - **Export to CSV** to generate a CSV file of the differences detected.

12. Click **Next**.

    Differences are imported in the target repository.

    The target repository is aligned with the source repository.

    > ☞ *An alignment file with the content of differences (align-YYYY-MM-DD-hh-mm_555.mgr) is automatically saved in folder <Environment Name>\Db\<Repository Name>\USER\<User Code>.*

    If the alignment contains rejects, click **Display rejects** to open and save the file of the alignment rejects (.mgr format).

    > *A rejects file is automatically saved in folder <Environment name>\Db\<Repository name>\USER\<User Code> (rejects file-reject-YYYY-MM-DD-hh-mm_555.mgr). This file is empty if alignment does not contain rejects.*

13. Click **OK** to dispatch the modifications.

    > ☞ *Click **Cancel** if you do not want to keep the modifications.*

MERGING OBJECTS

The object merge feature is available with the **Hopex Power Supervisor** technical module.

When you merge two objects of the same type, you get a single object by transferring the *characteristics* and *links* from the source object to the target object. The source object is deleted.

Choice of the objects to merge

The **Target** object is the reference object that will be merged with the **Source** object. By default:

- its characteristics are not modified
- merging proposes addition of source object links.

The **Source** object is the object of which:

- you want to reuse certain characteristics or certain links
- characteristics and links will be transferred to the **Target** object.

When the link is to be a unique link (e.g., for sub-typing where the type is unique), the link of the target object is kept by default.

💣 **When merging is completed, the source object is deleted.**

☺ *You can **Explore** objects using the corresponding command. It can also be used to explore their links.*

Merging Two Objects

The merging feature is available in the functional administration desktops and Solution desktops.

To merge two objects:

1. Connect to **Hopex** with the profile concerned.

    ☞ *See Logging in to Hopex.*

2. Access the source object.
3. Right-click the source object and select **Manage > Merge**.
   In the **Object selection** window, the object type and the source object are predefined.

    ☞ *(private workspace case) To have the right to merge two objects, you must have the right to delete objects.*

4. In the **Selected target object** field, click the arrow and **Select the target object**.

5. Use the search tool to select the target object and click **OK**.
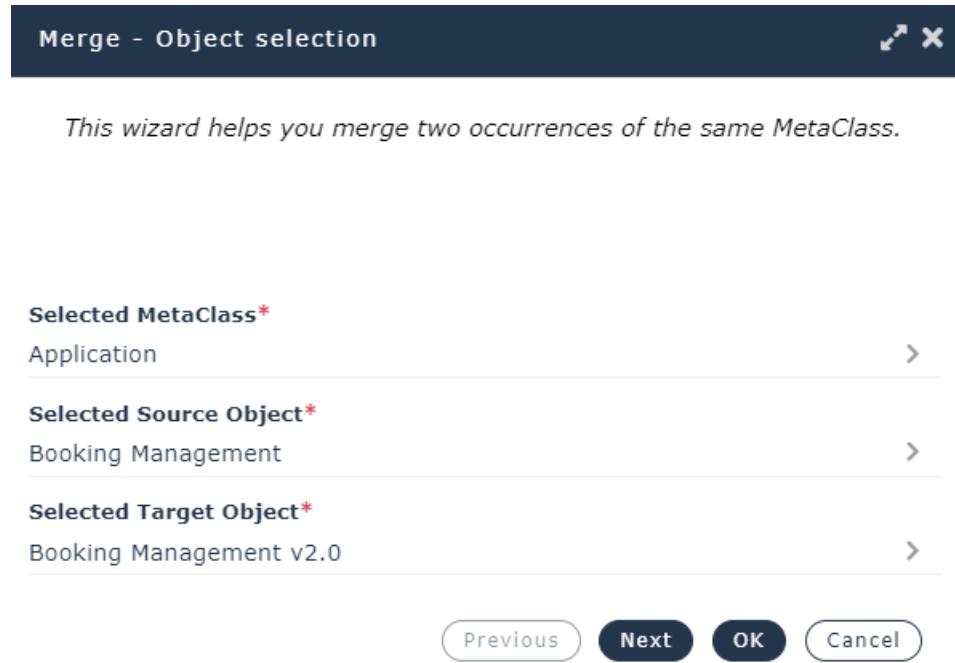
6. Click **Next**.
The **Properties to merge** window shows the differences found in the characteristic values of both objects.

7. In the **SourceValueSelected** column, select the source object characteristics you want to transfer to the target object. Characteristics that remain selected in the target object are kept.

Name ↑	SourceValueSelect...	Source Value Display	TargetValueSelect...	Target Value Display
Aggregation Type\APM	☐	Application	☑	Application
Application Code	☐	RESBOOK	☑	
Average Level of Vulnerability	☐	Medium	☑	
BackFired Function Points\CAST Hi...	☐	1505	☑	
Business Impact\Cast	☐	29.44	☑	
Cloud Computing	☐	On-Premises	☑	On-Premises
Cloud Ready Scan\CAST Highlight	☐	82	☑	
Cloud Ready Score\CAST Highlight	☐	52	☑	

Merge - Properties to merge

Select the properties to merge

Reorganize   Instant Report

« ‹ | Page 1 of 1 | › » | ⟳ | Show 50 ⌄ elements   Displaying 1 - 30 of 30

Previous   Next   OK   Cancel

8. Click **Next**.
The **Unique links to merge** window (links that can only exist once for a given object) appears only if the objects to be merged have unique links connecting them to different objects.

> Example: a message can have only one super-type.

9. Select the link to be transferred.

10. Click **Next**.
    The **Links to merge** window shows the links.

By defaut, when:

- the link does not exist for the target object, the target object is connected: "Connect" **Action** is selected. You can clear the action so as not to transfer the link.
- the link exists for both source and target objects, both links are kept: "Connect" **Action** is selected for the link from the source object, "Disconnect" **Action** is cleared for the link from the target object
You can keep existing links, or **Disconnect** them.

11. Click **OK** to start merging.
    When merging has been completed, the source object no longer exists and the selected *characteristics* and *links* have been transferred to the target object.

    ☛ *"_TransferredObject" temporary merge objects are created on this occasion. Merge objects of a repository can all be exported at export of **Hopex** objects.*

MANAGING DATA ACCESSES

The following points are covered here:

- ✓ Managing Data Writing Access
- ✓ Managing Data Reading Access

MANAGING DATA WRITING ACCESS

Full management of data writing access and opening of corresponding diagram is only available with **HOPEX Administration (Windows Front-End)**.

☛ *See Data Writing Access.*

The Web Administration desktop enables to:

- display writing access areas (as a list or a hierarchical tree)
- create writing access areas:
  - define their upper levels ("Administrator" by default)
  - define their lower levels
  - define their members
- compile the writing access diagram

Accessing Writing Access Areas (list)

To access the list of writing access areas (in Web):

1. Connect to the **Hopex Administration** desktop.

☛ *See Accessing Web Administration Desktop.*

2. Click the **Data Access > Writing Access areas** navigation menu.
   The list of writing access areas displays with, for each area, its corresponding **Upper** area.

Writing Access Areas

◄☰	**+ New**	🐸 Compile	▼

☐	**Name ↑**	**Upper**	
	🔍	🔍	
☐ 🐸	Administrator		
☐ 🐸	New Jersey	🐸 Administrator	
☐ 🐸	Singapore	🐸 Administrator	

☺ *To display the writing access areas as a hierarchical tree, in the list menu bar, click* ◄☰ *.*

Accessing Writing Access Areas (tree)

To access the hierarchical tree of writing access areas (in Web):

1. Connect to the **Hopex Administration** desktop.
   ☛ *See Accessing Web Administration Desktop.*
2. Click the **Data Access** navigation menu.

3. Click **Writing Access areas** ▤▸.
    The hierarchical tree of writing access areas displays.

Creating a Writing Access Area

To create a writing access area:
*   you must define its name
*   you can define its upper area ("Administrator" by default)

To create a writing access area:
1. Access the list of writing access areas.

    ☛ See *Accessing Writing Access Areas (list).*

2. In the list menu bar, click **New** ➕ .
3. Enter the writing access area name.

        E.g.: Hoboken

4. By default its upper area is "Administrator", to modify it:

    ☛ *You can modify the area later.*

    - Click the **Upper** field arrow and select **Connect Writing Access Area**.
    - Select the area.

        `E.g.: New Jersey`

    - Click **Connect**.
5. Click **OK**.

Writing Access Areas

	Name ↑	Upper	
□	🐾 Administrator		
☑	🐾 Hoboken	🐾 New Jersey	
□	🐾 New Jersey	🐾 Administrator	
□	🐾 Singapore	🐾 Administrator	

☺ *To display the writing access areas as a hierarchical tree, in the list menu bar, click ◀☰ .*

Creating a Writing Access Area with its Upper Area

To facilitate the hierarchical creation, you can create a writing access area directly under its upper access area.

To create a writing access area with its upper area predefined:

1. Access the tree of writing access areas.

    ☛ *See Accessing Writing Access Areas (tree).*

2. Hover the cursor over the name of the upper writing access area, then
click ✛ **New > Writing access area**.
The upper writing access area is predefined.

```
E.g.: New Jersey.
```

Creation of Writing access area

Name*

Writing access area-1

Upper*

New Jersey

OK   Cancel
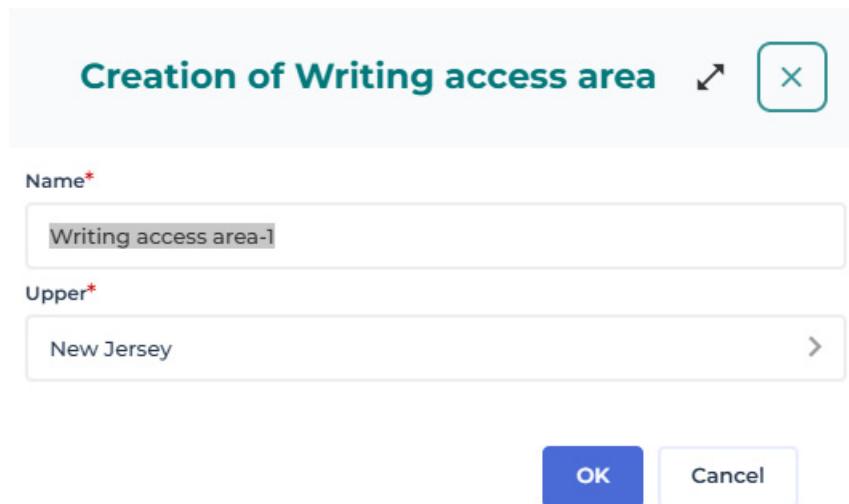
3. Enter the **Name** of the writing access area.

```
E.g.: Newark.
```

4. Click **OK**.

Defining Writing Access Area Members

A writing access area member can be a person or a person group.

☛ *Alternative: to modify the writing access area of a person, see*
Connecting a Person to a Writing Access Area.

☛ *Alternative: to modify the writing access area of multiple persons at*
once, see Mass Connecting Persons to a Writing Access Area.

To define the writing access area members:

1. Access the list of writing access areas.

☛ *See Accessing Writing Access Areas (list).*

2. Access the writing access area properties.
3. In the **Characteristics** page, expand the **Access area members**
section.
4. Click **Connect** 🔗 .
5. (If needed) To narrow down the target, click the **Access Area Member**
drop-down menu and select **Person** or **Person Group**.
6. (Optional, to refine your search) In the second field, enter the character
string you want to search for.

7. Click **Find** 🔍 .
8. In the result list, select the required members of the area and click
    Connect.
    The selected person and/or person groups are connected to the writing
    access area.

    ☛ *To remove a member from the area, select the member, then click*
    Remove 🔴 *. Confirm* **Remove***.*
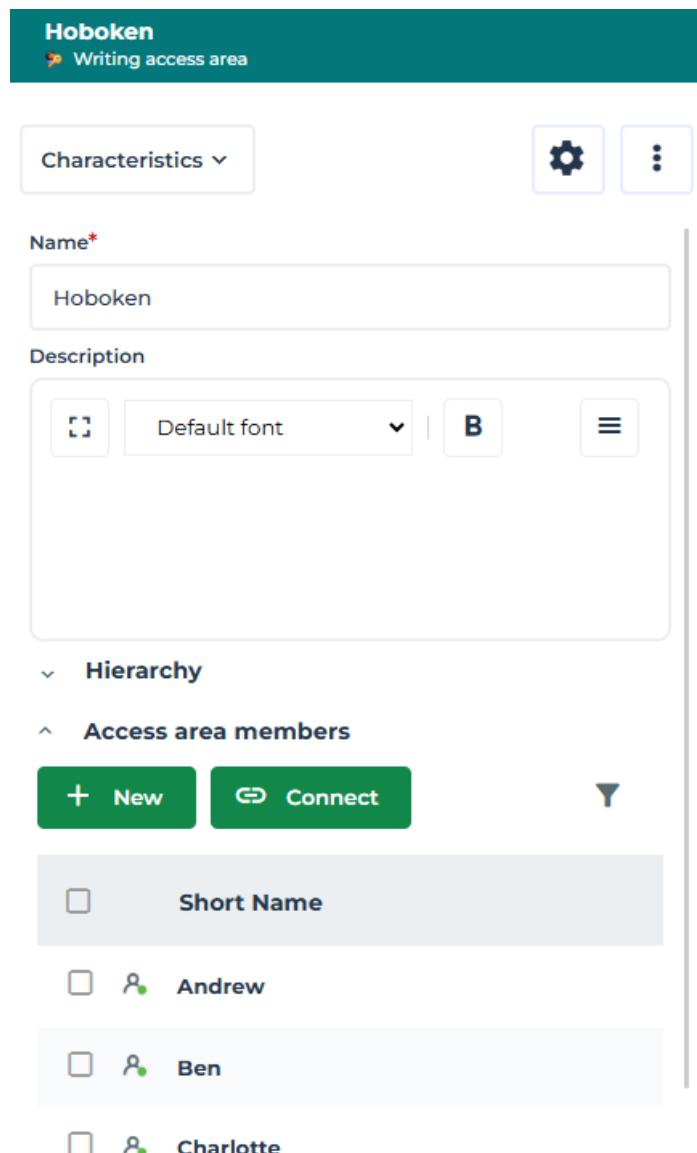
Hoboken
🗝 Writing access area

Characteristics ∨   ⚙   ⋮

Name*

Hoboken

Description

⛶   Default font   ∨ | **B**   ≡

∨   **Hierarchy**

∧   **Access area members**

\+ **New**   🔗 **Connect**   ▼

☐   **Short Name**

☐ 👤 **Andrew**

☐ 👤 **Ben**

☐ 👤 **Charlotte**

Defining a Lower Writing Access Area

A writing access area may have several lower writing access areas.

To define a lower writing access area:

1. Access the list of writing access areas.

   ☛ See *Accessing Writing Access Areas (list).*

2. Access the writing access area properties.
3. In the **Characteristics** page, expand the **Hierarchy** section.
4. In the **Lower** list, click **Connect** 🔗 .

   ☛ *To create an area, in the **Lower** list, click **New** ➕ and enter its **Name** and select its **Upper** area.*

5. In the **Possible Lower Writing Access Areas**, select the area and click **Connect**.

Defining an Upper Writing Access Area

A writing access area may have several upper writing access areas.

To define an upper writing access area:

1. Access the list of writing access areas.

   ☛ See *Accessing Writing Access Areas (list).*

2. Access the writing access area properties.
3. In the **Characteristics** page, expand the **Hierarchy** section.
4. In the **Upper** list, click **Connect** 🔗 .

5. To create an area: click **New** ➕ , then enter its **Name**, and select its **Upper** area.
6. In the **Possible Upper Writing Access Areas**, select the area and click **Connect**.

Deleting a Writing Access Area

You can delete a writing access area.

- The writing access areas dependent on the deleted writing access area are, after updating, no longer connected to the writing access area tree. It is therefore preferable to first change their link with the obsolete writing access area for a retained writing access area.
- A person must belong to a writing access area ("Administrator" by default).
  If you delete a writing access area that includes members, you must connect these persons to another writing access area.

  ☛ See *Defining Writing Access Area Members* and *Connecting a Person to a Writing Access Area.*

To delete a writing access area:

1. Access the list of writing access areas.

   ☛ *See Accessing Writing Access Areas (list).*

2. Select the writing access area.

   ☺ *You can use the filtering tool to help you find the area.*

3. In the list menu bar, click **Remove** 🔴 .

   If the removal has an impact, a warning is indicated in the **Status** column with its **Motive**.

4. Click **Delete** to confirm.

   ☺ *To access the list of persons with no writing access area, in the homepage, **Person Statistics**, click the **Active persons with no writing access area** indicator.*

   To connect multiple persons to the same writing access area, select the persons then click in a writing access area cell of the list to use the drop-down menu to select the area.

   ☛ *See also Defining Writing Access Area Members and Connecting a Person to a Writing Access Area.*

Compiling the Writing Access Diagram (Web)

Running writing access diagram compilation ensures consistency of **Hopex** behavior with declarations of the diagram.

💣 **If the diagram is not compiled, some users may be able to update objects that are normally protected.**

To compile the writing access diagram (Web):

1. Access the list of writing access areas.

   ☛ *See Accessing Writing Access Areas (list).*

2. In the list menu bar, click **Compile** 🐾 .

   When compilation is complete, a message indicates that the operation was successful, or, if applicable, that the diagram contains errors.

MANAGING DATA READING ACCESS

Full management of data reading access is only available in **HOPEX Administration (Windows Front-End)**.

Managing data reading access areas is only available after activating the data confidentiality management.

☛ *See Data Reading Access.*

The Web Administration desktop enables to:

- display reading access areas
- create reading access areas
  - define its upper level area
  - define its lower level area
  - define its reading access area type
  - define its members
- compile the reading access diagram

Accessing Reading Access Areas (Web)

To access reading access areas (Web):

1. Connect to the **Hopex Administration** desktop.

☛ *See Accessing Web Administration Desktop.*

2. Click the **Data Access > Reading Access areas** navigation menu.
The list of reading access areas displays with, for each area:

- its **Reading access area type**
- its **Upper** area
- its **Lower** area

Reading Access Areas

	Name ↑	Reading access area type	Upper	Lower
	Maximum reading access	General reading access area		MEGA Process
	MEGA Process	General reading access area	Maximum reading access	Standard
	MEGA Process BPMN	General reading access area	Maximum reading access	Standard
	Standard	General reading access area	MEGA Process	

Compiling the Reading Access Diagram (Web)

Running the reading access diagram compilation ensures consistency of **Hopex** behavior with declarations of the diagram.

> 💣 **If the diagram is not compiled, some users may be able to see objects that are normally hidden.**

To compile the reading access diagram (Web):

1. Access the list of reading access areas.

> ☞ See *Accessing Reading Access Areas (Web)*.

2. In the list menu bar, click **Compile**.
When compilation is complete, a message indicates that the operation was successful, or, if applicable, that the diagram contains errors.

SCHEDULING

The **Scheduler** of **Hopex** enables to create Triggers to schedule Job execution.

In your **Hopex** desktop, some profiles (Hopex Administrator, functional Administrator, Hopex Customizer) give access to the (Job) Trigger scheduling list.

The following points are covered here:

- ✓ Introduction to Scheduling
- ✓ Managing Triggers
- ✓ Defining a Trigger Scheduling

INTRODUCTION TO SCHEDULING

Concepts

The scheduler enables to execute jobs, provided or defined by a Hopex Administrator, at defined dates, times, and frequencies so as to avoid overloading **Hopex** at user working hours.

Job

A job is a process. It includes:
- a macro to be executed
- a context, which gives the information required to execute the macro: **Job Context** as a character string.

Scheduler

The Scheduler enables to schedule job execution:
- execution date and time
- frequency

Trigger

A Trigger is associated with a job to define the job execution date:
- the Trigger is based on a Trigger Definition. This definition consists of a job which includes the macro that the Trigger will execute.
- the Scheduler enables to define when (date and time) to execute the job and at which frequency.

Defining your Local Time

In the Scheduler, by default the time format is hh:mm:ss (UTC). To facilitate configuration, you can change this UTC format for a local time format (local time of the user or of the server launching the execution).

☛ See *Defining the Execution Time Zone.*

To define your user local time:
1. Access the site (or environment) level options.
2. Expand the **Installation** folder and select **Web Application**.

3. In the right pane, use the drop-down menu of the **Time zone** option to select your time zone.

```
E.g.: select "(UTC-05:00) Eastern Time (US & Canada)" to
define times in New-York local time.
```

Time zone

◆ (UTC-05:00) Eastern Time (US & Canada)   ⌄

When you configure your Triggers, the execution scheduling is defined in this time zone if you select the **User time zone**.

If you configure your Triggers in **UTC** or **Server time zone**, you can consult the conversion in this time zone.

☞ *For example, see Defining the Recurrence Time of a Trigger execution.*

MANAGING TRIGGERS

See:
- Accessing Triggers
- Managing a Trigger

Accessing Triggers

In the **Scheduling Management** window, the **Scheduling** page displays the Triggers:

- **Custom Triggers**
  Triggers defined by the Hopex administrator. These Triggers can be defined on a data repository or on the System repository.

- **WebSite Generation Triggers**
  Triggers for WebSite generation.

- **Predefined Triggers**
  Triggers provided with Hopex and available in all the installations. These Triggers are defined on the System repository.
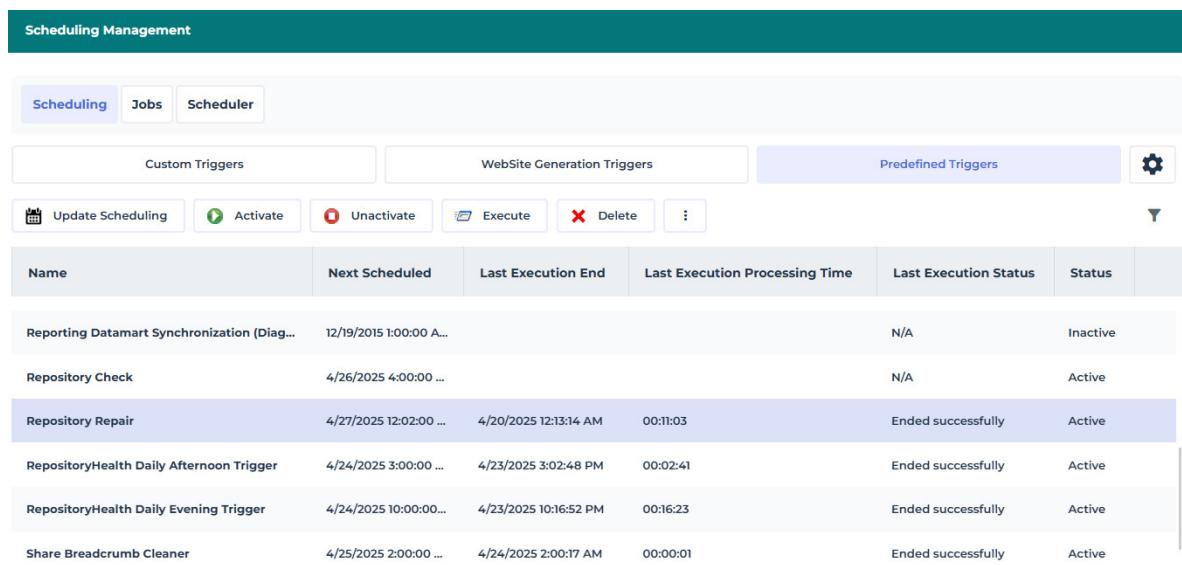
Scheduling Management

| Scheduling | Jobs | Scheduler |

| Custom Triggers | WebSite Generation Triggers | Predefined Triggers | ⚙ |

📅 Update Scheduling   ▶ Activate   ⬤ Unactivate   🗒 Execute   ✖ Delete   ⋮   ▽

Name	Next Scheduled	Last Execution End	Last Execution Processing Time	Last Execution Status	Status	
Reporting Datamart Synchronization (Diag...	12/19/2015 1:00:00 A...			N/A	Inactive	
Repository Check	4/26/2025 4:00:00 ...			N/A	Active	
Repository Repair	4/27/2025 12:02:00 ...	4/20/2025 12:13:14 AM	00:11:03	Ended successfully	Active	
RepositoryHealth Daily Afternoon Trigger	4/24/2025 3:00:00 ...	4/23/2025 3:02:48 PM	00:02:41	Ended successfully	Active	
RepositoryHealth Daily Evening Trigger	4/24/2025 10:00:00...	4/23/2025 10:16:52 PM	00:16:23	Ended successfully	Active	
Share Breadcrumb Cleaner	4/25/2025 2:00:00 ...	4/24/2025 2:00:17 AM	00:00:01	Ended successfully	Active	

For each scheduled Trigger, it indicates:
- its name
- its next execution date and time
- its last execution information:
  - start and end date and time
  - processing time (duration)
  - status
- its repeat number
- its status (enabled or disabled)
- if the trace of the trigger is kept after its deletion or not
- its retention period (in days)
- its deletion date

☞ *By default, some of the columns are hidden, you can display them.*

☑ Next Scheduled

☐ Last execution start

☑ Last Execution End

☑ Last Execution Processing Time

☑ Last Execution Status

☐ Repeat number

☑ Status

☐ Keep Execution History

☐ History Retention Period (in days)

☐ Keep after last execution

More...

To access the Triggers:
1. Connect to **Hopex** with one of the required profiles.

    E.g.: Hopex Administrator, <Solution name> Functional
    Administrator, Hopex Customizer.

2. Depending on the desktop:
   - **Administration Web** desktop: click the **Scheduling** navigation menu.
   - other desktops: select the navigation menu **Administration > Tools: Scheduling Management**.

Creating a Trigger

A Trigger is based on a Trigger Definition. This definition consists of a job which includes the macro that the Trigger will execute.

The Trigger is triggered on the objects defined in the associated job macro.

Prerequisite: the definition (**Trigger Definition**) on which is based the trigger is created.

To create a Trigger:

1. Access the **Scheduling** management pages.

   ☞ *See Accessing Triggers.*

2. In the **Scheduling > Custom Triggers** page, click **New** ➕.
3. Select the **Trigger Definition**.
4. Click **Next**.
   The Trigger definition window opens.
5. (If needed) Enter the Trigger **name**.
   If not entered, by default the Trigger name is the definition name selected.
6. In the **Job Context** pane define the job execution context, i.e. the objects on which the job applies.

   💣 **Do not add any break line in the character string.**

7. Click **OK**.
   The Trigger is created.

   By default the Trigger is active. You can execute the Trigger to test it before configuring its scheduling.

   ☞ *To test the Trigger, see Managing a Trigger.*

Managing a Trigger

You can:

- update the Trigger scheduling
  To modify the job execution dates, times, and frequencies, see Defining a Trigger Scheduling.

- activate/deactivate a Trigger
  By default a Trigger is active.
  To temporarily suspend the job execution, you can temporarily deactivate its Trigger.

- execute a Trigger
  To immediately execute the job associated with the Trigger (outside its scheduling).

  > For example, to test a job.

- delete a Trigger
  If you want to reuse the Trigger later, instead of deleting the Trigger you can deactivate it.

To manage a Trigger:

1. Access the **Scheduling** management pages.

   ☛ *See Accessing Triggers.*

2. Select the Trigger concerned.
3. In the list menu bar, click:

   - **Update Scheduling**

     ☛ *See Defining a Trigger Scheduling.*

   - **Activate** ▶ / **Deactivate** ⏹

   - **Execute** 🗇

     ☛ *The Trigger must be active to be executed.*

   - **Delete** ✖

DEFINING A TRIGGER SCHEDULING

Trigger Scheduling Definition

A Trigger scheduling is defined by:

- its execution **time zone** for all its scheduling time definitions

    ☛ *See Defining the Execution Time Zone.*

- its **recurrence**
  The execution can be unique or recurrent.

    ☛ *See Defining the Trigger Execution Frequency.*

  If the execution is recurrent:

  - the recurrence **pattern**, i.e. its execution recurrence (daily, weekly, monthly, weekly)

      ☛ *See Defining the Trigger Recurrence Pattern.*

  - the execution recurrence **time**, i.e. executing the trigger once or several times th days scheduled on a recurrence range.

      ☛ *See Defining the Recurrence Time of a Trigger execution.*

  - the execution recurrence **range**, i.e. defining the first and last Trigger execution dates.

      ☛ *See Defining the Recurrence Range of a Trigger Execution.*

Defining the Execution Time Zone

To facilitate scheduling time definition, you can modify the time zone in which you define the scheduling times:

- **UTC** (default), to define times in UTC format
- **User time zone**, to define times in the user time zone
- **Server time zone** (STZ), to define times in the time zone of the server executing the Trigger

    💣 **Attention: if you change the time zone a posteriori, times are not automatically converted.**

To define the execution time zone:

1. Access the Triggers.

    ☛ *See Accessing Triggers.*

2. Select the Trigger concerned and in the list menu bar, click **Update Scheduling**.
3. Expand the **Advanced** section, and in the **Time zone for all the scheduling time definitions**, select the time zone.
4. If you select **User time zone**, you must define your time zone.

    ☛ *See Defining your Local Time.*

Defining the Trigger Execution Frequency

A Trigger can be executed uniquely or on a regular basis.

To define the Trigger execution frequency:

1. Access the Triggers.

   ☛ *See Accessing Triggers.*

2. Select the Trigger concerned and in the list menu bar, click **Update Scheduling**.

3. In the **Frequency** section, define the frequency:
   - *unique execution*: select "Once"
   - *recurrence*: keep "Recurrent" and define the recurrence (pattern, moment, range).

     ☛ *See Defining the Trigger Recurrence Pattern, Defining the Recurrence Time of a Trigger execution, Defining the Recurrence Range of a Trigger Execution.*

4. If you selected "Once", define the date:
   - keep, "**As soon as possible**", the Trigger est executed as soon as possible, or
   - select" **At scheduled time**" and define the **Start Date** with the help of the calendar and the **Start time** with the the arrows.

     ☛ *Time is defined in the time zone defined (see Defining the Execution Time Zone) with the hh:mm:ss format.*

     ☛ *If you are in the UTC time zone, to facilitate the check of your settings, see Defining your Local Time.*

Defining the Trigger Recurrence Pattern

A Trigger can be executed uniquely or on a regular basis.

The recurrence pattern can be:

- ***daily***
  By default, the Trigger is executed every day at the time set for the first execution.
  You can execute the Trigger every N days (N to be defined)
- ***weekly***, you must define:
  - the frequency

    `E.g.: every two weeks (N=2)`
  - the day of the week

    `E.g.: Monday, Tuesday,..., Sunday`

    You can select several days.
- ***monthly***, you must define:
  - the day of the month, or the day of the week (day of the week and week of the month to be defined)

    `E.g.: 1,2,...,31, last day of the month`

    You can select several days.

    `E.g.: every Sunday of the last week of the month, i.e. the last Saturday of the month.`

    You can select several days and several weeks.
  - the frequency: every N months (N to be defined) or a specific month every year

    `E.g.: every 2 months (N=2) or in April every year.`

    You can select several months.

To define the Trigger recurrence pattern:

1. Access the Triggers.

    ☛ *See Accessing Triggers.*

2. Select the Trigger concerned and in the list menu bar, click **Update Scheduling**.
3. In the **Recurrence Pattern** section, select the frequency.

    `E.g.: Daily, Weekly, Monthly.`

4. Define the recurrence time.

Defining the Recurrence Time of a Trigger execution

In case the **Recurrence Pattern** is "Daily", "Weekly", or "Monthly", you must define the Trigger execution recurrence time:

- at a unique time each scheduled execution day
- recurrent on a time range each scheduled execution day

Times are defined in the time zone defined (see Defining the Execution Time Zone) with the hh:mm:ss format.

☛ *If you are in the UTC time zone, to facilitate the check of your settings, see Defining your Local Time.*

To define the recurrence time of a Trigger execution:

1. Access the Triggers.

   ☛ *See Accessing Triggers.*

2. Select the Trigger concerned and in the list menu bar, click **Update Scheduling**.

3. In the **Recurrence Time** section, for:

   • a *unique execution* each scheduled day: keep "*Scheduled time*" and in the **At** field set the execution time.

   `E.g.: 23:30:00`

   • a **multiple execution** each scheduled day: select "*Several times*" and define the recurrence according the pattern: **Every** <period> *from* <time 1> **to** <time2>.

   `E.g.: every 4 hours from 10 am to 6 pm (in the time zone defined)`

   `Every` `04:00:00` **`from`** `10:00:00` **`to`** `18:00:00`

4. Define the recurrence range.

Defining the Recurrence Range of a Trigger Execution

The Trigger execution range is defined by a start and end date in the **Scheduling Update** window **Recurrence Pattern** section.

The first date of Trigger execution can be:

   • as soon as possible
   • at scheduled time

   `E.g.: on the 08/18/2025 at 18:30:15.`

The end date of Trigger execution can be defined by:

   • a given date

   `E.g.: on the 08/30/2025 at 20:30:00.`

   • a given repeat number

   `E.g.: schedule the Trigger every 30 minutes from 6am to 10am.`

   • no end

Times are defined in the time zone defined (see Defining the Execution Time Zone) with the hh:mm:ss format.

   ☛ *If you are in the UTC time zone, to facilitate the check of your settings, see Defining your Local Time.*

To define the Trigger execution range:

1. Access the Triggers.

   ☛ *See Accessing Triggers.*

2. Select the Trigger concerned and in the list menu bar, click **Update Scheduling**.

3. In the **Recurrence Range**, define the first execution date.
   In **From**, select:

   - "As soon as possible" or
   - "At scheduled time"

4. (With "At scheduled time") Define the start date and time:

   - Use the calendar of the **Start date** field to select the first date of Trigger execution.

     Select **Today** if you want to define the current day.

   - In the **Start time** field, set the triggering time of the Trigger.

     By default the time is set to 00:00:00 (hh:mm:ss format) in the time zone defined (see Defining the Execution Time Zone).

     ☛ *If you are in the UTC time zone, to facilitate the check of your settings, see Defining your Local Time.*

5. In **To**, set the end execution date.

   E.g.: "End date", "Repeat N times", "No end".

   If you selected:

   "**End date**", set the end date and time:

   - Use the calendar of the **End date** field to select the last date of Trigger execution.
   - In the **End time** field, set the triggering time of the Trigger.

     By default the time is set to 00:00:00 (hh:mm:ss format) in the time zone defined (see Defining the Execution Time Zone).

     ☛ *If you are in the UTC time zone, to facilitate the check of your settings, see Defining your Local Time.*

   "**Repeat N times**", define the number of occurrences:

   - In the **End after** field, use the arrows to set the number of occurrences.

6. Click **OK**.

OPTIONS

This chapter presents the various tools and options used to configure and customize **Hopex**.

The following points are covered here:

- ✓ Introduction to Options
- ✓ Managing Options
- ✓ Option Groups
- ✓ Managing Languages in Web Applications
- ✓ Managing Date and Time Formats
- ✓ Managing Hopex Data Customization
- ✓ Hiding Errors to Users
- ✓ Configuring SMTP Settings

INTRODUCTION TO OPTIONS

Option Overview

In **Hopex**, options can be configured at the following levels:

- environment
- profile (restricted to **Hopex Customizer** profile)
- user

> ☛ *Site level options can be modified in the **Administration** (Windows Front-End) application.*

Option levels are governed by an inheritance mechanism.

> ☛ *See Option Inheritance.*

Customizations made at the user level are of highest priority, followed in order of priority by those made at the profile and the environment levels.

> 💣 **Having modified option values, it is recommended that you dispatch or save your work, close Hopex and then reopen it. Refresh issues can occur if these precautions are not taken.**

Options Window Description
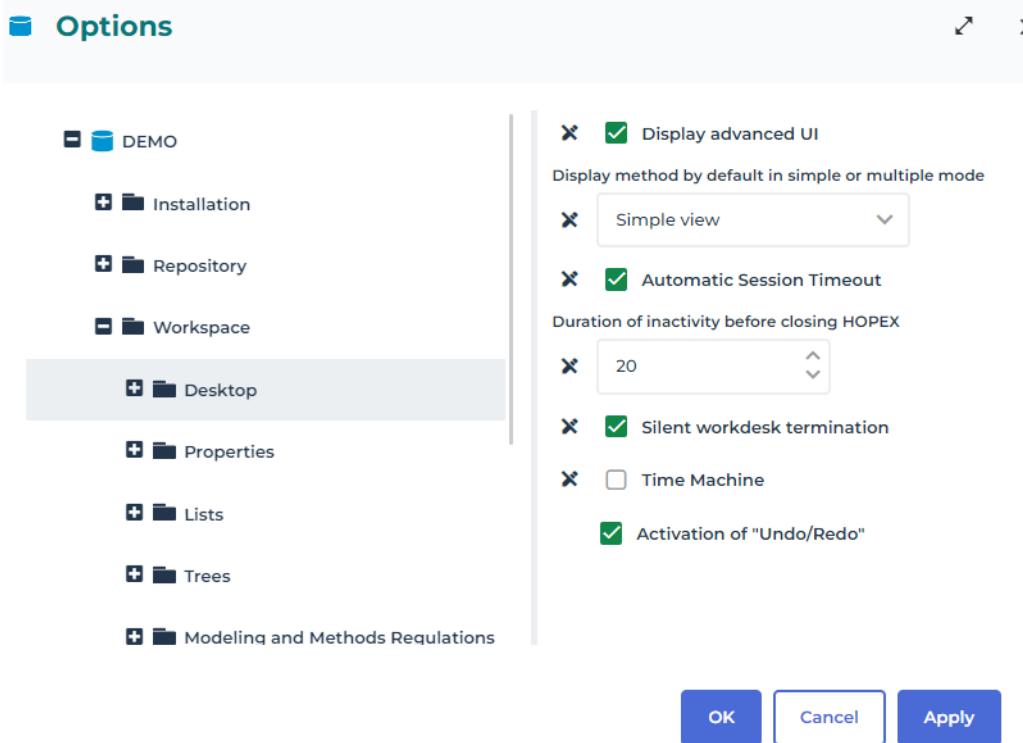
The left pane contains the option tree classified by group.

☞   See *Option Groups*.

The right pane enables configuration of the options corresponding to the group selected in the left pane.

Options vary depending on your available products.

For more details on an option:

❱   Hold the mouse over the option to display context-sensitive help.

When the user has a private workspace in progress, you cannot modify his/her options from the **Administration** desktop.

MANAGING OPTIONS

Modifying Options

In the **Administration** desktop, you can modify the options at the following levels:

- environment
- user

> 💣 **Having modified option values, it is recommended that you dispatch or save your work, close Hopex and then reopen it. Refresh issues can occur if these precautions are not taken.**

Modifying options at profile level is restricted to **Hopex Customizer** profile, see **Hopex Studio > Modifying options at profile level** documentation.

Modifying options at environment level

Storage: option values at environment level are stored in the MegaEnv.ini file. This file is accessible in the environment folder: **<HAS instance repository> > Repos > <environment name>**.

To modify options at environment level from the **Administration** desktop:

1. Connect to the **Hopex Administration** desktop.

   ☛ See *Accessing Web Administration Desktop*.

2. Click the **Environment Options** navigation menu.
   The environment options window opens.
3. Modify the option concerned.
4. Click:
   - **Apply** to validate your modifications and keep the **Options** window open.
   - **OK** to validate your modifications and close the **Options** window.
   Options are modified at environment level.

Modifying options at user level

A user can modify some of his/her options from his/her desktop main menu (**Settings > Options**).

If needed a Hopex administrator can modify an option at a user level.

To modify the options of a user from the **Administration** desktop:

1. Access the **Persons** management pages.

   ☛ See *Accessing the User Management Pages*.

   The list of persons displays in the edit area.
2. In the edit area, select the person concerned.
3. In the list menu bar:click **Options**.
   The person's options window opens.
4. Modify the option concerned.

5. Click:
   - **Apply** to validate your modifications and keep the **Options** window open.
   - **OK** to validate your modifications and close the **Options** window.
   The options are modified at user level.

Option Inheritance

Option levels are governed by an inheritance mechanism. An option inherits the value defined at higher level:

- A user inherits the option values defined at connection profile level.
- A profile inherits the option values defined at environment level.
- An environment inherits options defined at site level.

Customizations made at the user level are of highest priority, followed in order of priority by those made at the profile and the environment levels.

The icon located opposite the option indicates the inheritance, or not, from the higher level:

- ✖ indicates the inheritance from the higher level.

- ✏ indicates that the inherited option value has been modified. The value is no longer inherited from the higher level.

- options without icons indicate that the option value cannot be modified at this level.

   In this example of a Solution Desktop, the first option value is modified, the following two ones are inherited and the last one cannot be modified at this level.
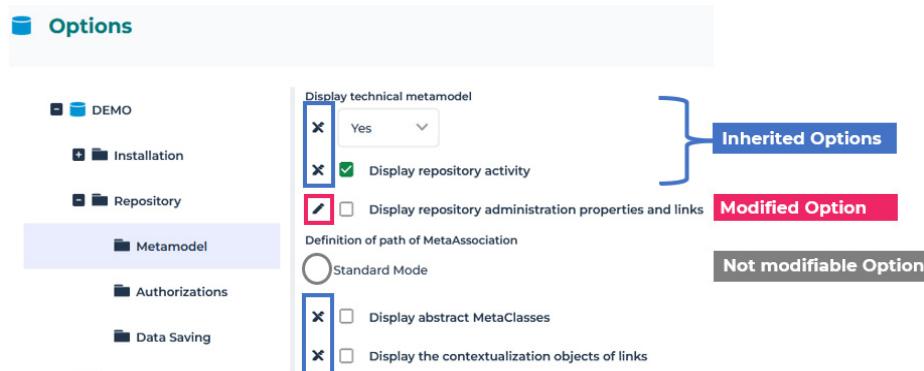
Modifying an option value

To modify the value of an option inherited from a higher level:

1. Access the Options page.

   ☞ See *Modifying Options*.

2. Modify the value of the option concerned.

The icon ✏ indicates that the option value is modified.

Resetting an option value

To reset the value of an option:
1. Access the options.

☞ *See Modifying Options.*

2. Click ✏.

The option value is reset and the icon changes to ✖.

Controlling the modification of options

With **HOPEX Administration**(Windows Front-End) you can prohibit modification of any option at a lower level than your current level.

```
Example: if you open options of the environment, you can
prohibit modification of all options at user level.
```

☞ *See Controlling Modification of Options.*

OPTION GROUPS

Only a Hopex administrator can access **Environment** level options.

Hopex Solutions option group contains important information for the functional administrator.

Installation

Options linked to installation:
- company information
- activated data languages
- user management
- Web user desktop (Web application)

Options available at environment level only:
- licenses
- documentation (URL)
- customizing
- machine Translation
- cache management (advanced)
- currency
- electronic mail
- security

Repository

Options linked to the repository:
- display of some advanced metamodel part
- authorizations
- data saving (dispatch)

Options available at environment level only:
- permissions
- log

Workspace

Options linked to the user workspace:
- desktop
- properties
- lists
- trees
- modeling and methods regulations
- dashboards

These options enable to display certain functionalities or not.

Tools

Options linked to **Data Exchange**:
- import
- export
- exchanges with third party tools

Options linked to the **Documentation** generated by Hopex:
- reports
- Web sites

Options linked to the **Diagrams**:
- display
- intellibar
- status indicators

Options linked to **Assessments**

Options linked to **Collaboration**:
- history management
- review note management
- notification and object follow-up management
- social
- workflows
- environment level only:
  - change management
  - workspace management

Options linked to the **Mapping Editor**

Options linked to **Explorer**

Options linked to **Query** (search)

Options linked to **Simulation** (Environment level only)

Hopex Solutions

Options linked to Solutions:
- Common Features
- IT Architecture
- IT Portfolio Management
- Privacy Management
- Business Process Analysis
- Data Management
- Loss Data Collection (Environment level only)

Compatibility

Compatibility options with deprecated or Windows Front-End specific features.

Technical Support

Options concerning Technical Support access.

Debugging

Options regarding debugging.

Available for Hopex administrator and functional administrator profiles.

MANAGING LANGUAGES IN WEB APPLICATIONS

In Web applications, you can modify:
- the interface language
- the data language

Each user can customize his/her desktop:
- modify his/her interface language

    ☛ *See Modifying your User Interface Language.*

- switch to another data language

    ☛ *See Modifying your Data Language.*

Modifying the Interface Language at Environment Level

The interface language defines the default language in which the Web application interface is displayed.

💣 **This modification requires restarting Hopex Core back-End module. Make sure to perform this action when users are not connected.**

☛ *The Web user can modify the interface language from his/her desktop, see Modifying your User Interface Language.*

To define the interface language in Web applications:

1. Access the environment options management window.

    ☛ *See Modifying options at environment level.*

2. In the Options tree, select **Installation > Web Application**.
3. In the right pane, use the drop-down menu to modify the value of the **GUI language** option.
4. In the **HAS console**, stop and start **Hopex Core Back-End** module.

    💣 **This action disconnects users.**

    ☛ *In the **HAS Console**: menu **Cluster** navigation menu, **Modules** tab **Hopex Core Back-End** module, click **Plus** ⋮ **> Stop**, then **Plus** ⋮ **> Start**.*

Modifying the Data Language at Environment Level

The data language is the language with which the user connects by default the first time. If the user changes his/her data language (Modifying your Data Language) in the interface, this is kept for the next connection.

By default, the data language is defined in the environment options.

If necessary you can define the data language for each user.

> ☛ *See Managing Languages.*

> 💣 **The data language defined at user level takes priority over the language defined in the environment options.**

To modify the data language at environment level:

1. Access the environment options management window.

   > ☛ *See Modifying options at environment level.*

2. In the tree, select **Installation > Languages**.
3. In the right pane, use the drop-down menu to modify the value of the **Data language** option.
   The default data language for any new created user is modified.

   > 💣 **Users already created keep their data language (defined at user creation or modified later at user level).**

MANAGING DATE AND TIME FORMATS

In **Hopex**,the date and time formats depend on the data language format.

These formats are defined for each language in the Windows parameters of **Hopex** installation server.

If needed, you can change these formats in **Hopex**.

💣 **This customization is lost at Hopex upgrade.**

💣 **This modification uncompile technical data.**

To change the date/time format for a language:

1. Connect to **Hopex** with the **Hopex Customizer** profile.

☛ *Check that you are allowed to modify Hopex data (**Options > Installation > Customization**), see* Managing Hopex Data Customization.

2. In the search by object type tool, in the first field, select **Languages**.

3. Click **Find** 🔍 .

4. Access the **Properties** of the language concerned.

5. Display the **Characteristics - Characteristics** page.

6. In the **_LanguageCharacteristics** pane, add the date format you want to be customized:

```
[DateFormat]
Date=<date format>
time=<time format>
```

For dates, you can use separating characters like for example:

```
"/", ",", "-", or " ".

Examples:

date=yyyy/MM/dd displays 2018/04/24

date=d-MM-yy displays 4-03-18

date=dd MMM yy displays 04 july 18
```

For times, you can use separating characters like for example:

```
"/", ".", or ":".

Examples:

time=HH:mm:ss displays 04:30:20

time=H:m displays 4:30
```
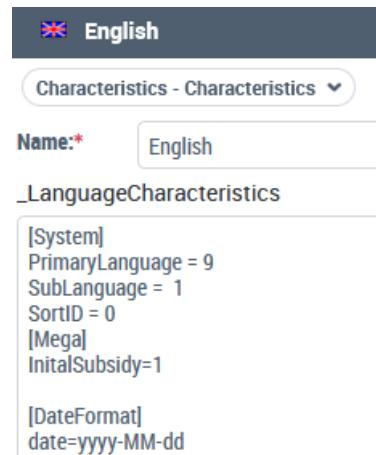

The modified formats (date and/or time) are automatically taken into account.

💣 **This modification uncompile technical data.**

7. Compile technical data.

☛ *See HOPEX Administration > Compiling an Environment documentation.*

Date Format	Description
d	The day of the month with one or two digits 1…9, 10, 11,..31
dd	The day of the month with two digits 01…09, 10, 11,..31.
M	The numeric format month with one or two digits 1…9, 10, 11, 12
MM	The numeric format month with two digits 01…09, 10, 11, 12
MMM	The abbreviated name of the month
Y	The year with one or two digits 9.18
yy	The year with two digits 09, 18
yyyy	The year with four digits 2018

Time Format	Description
HH	Time on two digits 00…23
H	Time on one or two digits 0…23
mm	Minutes on two digits 00…59
m	Minutes on one or two digits 0…59
ss	Seconds on two digits 00…59
s	Seconds on one or two digits 0…59

MANAGING HOPEX DATA CUSTOMIZATION

To ensure a correct use of **Hopex**, by default it is forbidden to modify **Hopex** data. Modifying a **Hopex** object can generate errors at **Hopex** upgrades, import of correctives, etc.

The **Authorizing Hopex Data Modification** option allows modifying the **Hopex** metamodel or any other **Hopex** technical object.

> 💣 **This option should only be selected in certain highly specific cases, at debugging operations or at Bizzdesign request, and for a temporary period.**

This option is:

- locked by default at environment level, with "Prohibit" value
  Only **Hopex Administrator** profile is allowed to modify this option.

    ☞ *See Controlling the modification of options.*

- accessible in the **Options > Installation > Customization** folder.

    💣 **Specify this access level only for a highly advanced profile.**

HIDING ERRORS TO USERS

For security reasons you can hide the error details to the users.

To hide the errors to users:

1. Access the environment options management window.

   ☛ See *Modifying options at environment level.*

2. In the Options tree, select **Installation > Web Application**.
3. In the right pane, use the drop-down menu to modify the value of the **Error display management in web Front-End** option to "Do not display message".
   You can also select "Display message, but not errors", or "Display only the application errors and messages".

   Default value: "Display message and errors".

CONFIGURING SMTP SETTINGS

SMTP settings are configured in the **Hopex Application Server** console

☛ *See Configuring the SMTP Server.*

☛ *SMTP settings can also be configures in Administration application (Windows Front-End) in the site level options (**Installation > Email)**.*

In the Administration desktop, you can view SMTP settings in the **Environment Options** (**Installation > Email**):

- **Default address of author via SMTP (FROM)**
  Default address, used when no email address is defined.

  ```
  For example at Web account initialization, if the
  administrator does not have an email address, this default
  address is used as the sender address of the email sent to
  the user to define his password.
  ```

- **Default address of sender via SMTP (SENDER)**
  Address used for security authentication purpose, in addition to the known address or to the default address (**Default address of author via SMTP (FROM)**) depending on the case.

  It enables to **Hopex** automatic emails to be validated by your company security checks.

  ```
  For example: at Web account initialization, this address is
  also used in the email sent to the user to define his
  password. If the administrator:

  - has an email address:

  SENDER@company.com on behalf of AdminName@company.com

  - does not have an email address:

  SENDER@company.com on behalf of FROM@company.com
  ```

- **SMTP Server**
  SMTP address of your server.

  ☛ *The domain used in the FROM and SENDER addresses must match the SMTP server domain.*

- **SPTP Port**
  By default: 25. You can add security (SSL or TLS).

To configure SMTP settings:

1. Access the **Hopex Application Server** console.
2. Select the **SMTP Configuration** navigation menu.
3. Define:
   - **Default address of author via SMTP (FROM)**

     ```
     Example: sender@company.com, AdminName@company.com
     ```

   - **Default address of sender via SMTP (SENDER)**

     ```
     Example: sender@company.com, AdminName@company.com
     ```

   - **SMTP Server**

     ```
     Example: exa.fr.company.com
     ```

4. Click Save .

GLOSSARY

access area member	Access area member groups all persons and person groups belonging to an access area. This area defines objects that can be accessed by the person or person group.
access path	An access path indicates which folder you can use when creating a reference for an environment database or a site environment. When all repositories are created in the same location as the environment, the path created at installation (the DB folder under the environment root) is sufficient and is given as the default. When you want to save a repository in a folder other than that of the environment, you must declare a new access path.
access rights	User access rights are the rules that manage access to software functions and databases. You can restrict the access rights of a user to the different repositories defined in his/her work environment. You can also restrict what software features a given user can run, such as the descriptor editor, modifying queries, designing report templates (MS Word), deleting objects, dispatching private workspaces, importing command files, managing environments, repositories, users, writing access, etc.
administration	Administration consists of managing the work environment of repository users. This function is usually the responsibility of the administrator. Administration tasks include backing up repositories, managing conflicts in data shared by several users and providing users with queries, descriptors, report templates (MS Word), etc. common to several projects.
Administration desktop	The **Hopex Administration** desktop (Web Front-End) is the Web version of the **Administration** (Windows Front-End) application accessible via an internet browser. It enables to manage Hopex users.

administrator   The administrator is a person who has administration rights to manage sites, environments, repositories and users. In addition to Administrator (who cannot be deleted) and MEGA users, both created at installation, you can grant administration rights to other users.

attribute   See *Characteristic*.

backup logfile   The backup logfile is an additional file stored outside the repository or private workspace. It ensures that the changes made to the repository or private workspace can be recovered even if the repository files become corrupted. Creation of this file is requested in the configuration of each repository (including the system repository). It is created when the first update is made in a private workspace or repository.

business role   A business role defines a function of a person in a business sense. A person can have several business roles. A business role is specific to a repository.

characteristic   A characteristic is an attribute that describes an object or a link. Example: the Flow-Type characteristic of a message allows you to specify if this message is information, or a material or financial flow. A characteristic can also be called an Attribute.

command file   A command file is a file containing repository update commands. It can be generated by backup or object export (.MGR extension) or by logfile export (.MGL extension).

description   Descriptors allow you to create reports (MS Word) containing part of the contents of the repository. Descriptor for an object includes the object characteristics, to which can be added the characteristics of objects directly or indirectly linked to it. The readable format for each of the objects encountered is entered as text in Word for Windows. You can insert descriptors into reports (MS Word) or report templates (MS Word) or use them to produce reports. Descriptors can be created or modified using the **Hopex Power Studio** technical module.

desktop   The desktop specific to each user contains projects, diagrams, reports (MS Word), etc. handled by this user. The user has a different workspace in each of the repositories he/she accesses.

discard	Discarding a private workspace cancels all modifications made since the last dispatch. All the work you have done since the beginning of the private workspace is lost. A warning message reminds the user of this. The user can request discard of his/her private workspace from the **Repository** (**Dispatch > Discard**) menu or at disconnection.
dispatch	Dispatching your work allows the other users to see the changes you have made to the repository. They will see these when they open a new workspace, either by dispatching, refreshing or discarding their work in progress
environment	An environment groups a set of *users*, the *repositories* on which they can work, and the *system repository*. It is where user private workspaces, users, system data, etc. are managed.
external reference	An external reference enables association of an object with a document from a source outside **Hopex**. This can relate to regulations concerning safety or the environment, legal text, etc. Location of this document can be indicated as a file path or Web page address via its URL (Universal Resource Locator).
functionality	A functionality is a means proposed by the software to execute certain actions (for example: the shapes editor and the descriptor editor are functionalities proposed as standard).
general UI permission	General UI permission defines if tools are available or not. By default, general UI accesses have *A value (A: Available, *: default value).
identifier	An absolute identifier is a string of characters associated with each object in the repository. This string is computed using the date and time the session was opened, the number of objects created since the session started, and the object creation date (in milliseconds). An absolute identifier provides a unique way to identify an object in the repository, so that even if the object is renamed, all the links to it are retained.
importing	Importing a command file, a backup file, or a logfile consists of applying the commands in the file to this new repository.
link	A link is an association between two types of object. There can be several possible links between two object types, for example: Source and Target between Org-Unit and Message.

lock	A lock is a logical tag assigned to an object to indicate that it is currently being modified by a user.
	Simultaneous access to an object by several users can also be checked. Locks apply to all types of object. When a user accesses an object to modify it, a lock is placed on the object. When a lock is placed on an object, another user is only able to view the object. This second user will not be able to modify the object until the first user dispatches his/her work, and the second user refreshes. This is done to avoid conflicts between the state of the object in the repository, and the obsolete view of the second user.
logfile	Logfiles contain all the actions performed by one or more users over a given period. The private workspace log contains all the changes made by a user in his/her private workspace. This logfile is used to update the repository when the user dispatches his work. For additional security, it is also possible to generate another log called the backup logfile.
logfile export	Export of a logfile creates a command file from the logfile of user actions in a repository. You can keep this file and import it later into a repository. You can selectively export modifications made in the work repository, or those made to technical data (descriptors, queries, etc.) in the system repository.
login	A Login uniquely defines a user or user group. It can be assigned to only one Person or Person Group.
MetaAssociation	see "link".
Metaclass	see object type
Metamodel	The metamodel defines the language used for describing a model. It defines the structure used to store the data managed in a repository The metamodel contains all the MetaClasses used to model a system, as well as their MetaAttributes and the MetaAssociations available between these MetaClasses. The metamodel is saved in the system repository of the environment. You can extend the metamodel to manage new MetaClasses. Repositories that exchange data (export, import, etc.) must have the same metamodel, otherwise certain data will be rejected or inaccessible.

object	An object is an entity with an identity and clearly defined boundaries, of which status and behavior are encapsulated. In a **Hopex** repository, an object is often examined along with the elements composing it. For example, a Diagram contains Org-Units or Messages. A Project contains Diagrams, themselves containing Org-Units, Messages etc. Database administration frequently requires consideration of consistent sets of objects. This is the case for object export, protection and object comparison.
object export	The export of one or several objects enables transfer of a consistent data set from a study to another repository. For example, export of objects from a project includes the project diagrams, together with the objects these diagrams contain, such as messages and org-units, as well as dependent objects. All the links between objects in this set are also exported.
Object type	An object type (or MetaClass) is that part of the database containing objects of a given type. The objects created are stored in the repository according to their type. Segments are used when searching for objects in the repository and when the metamodel is extended to include a new type of object. Example: message, org-unit, etc.
object UI permission	Object UI permission defines user rights on creation, reading, update, and deletion on these objects and their tools. By default, object UI permissions have *CRUD value (C: create, R: read, U: update, D: delete, *: default value).
person	A person is defined by his/her name and e-mail. A person can access **Hopex** once the administrator assigns him/her a login and a profile.
person group	A person group groups persons in a group. These persons share the same connection characteristics.
private workspace	A private workspace is a temporary view of the repository in which the user is working before dispatching his/her work. This view of the repository is only impacted by the changes of the user, and does not include concurrent modifications made by other users. This private workspace exists until it is refreshed, dispatched or discarded. Note that a private workspace is kept when the user disconnects from the repository, unless the user indicates otherwise. A user can see modifications dispatched by other users of this repository without dispatching his/her own modifications. To do this, the user refreshes his/her private workspace. The system then creates a new private workspace, and imports the logfile of his/her previous modifications into it.

private workspace log
The private workspace log contains all modifications made by a user in his/her private workspace. It is applied to the repository at dispatch, then automatically reinitialized. This log is stored in the EMB private workspace file.

profile
A profile defines what a person can see or not see and do or not do in the tools, and how the person sees the tools and can use them. The profile defines options, access rights to repositories and products, read/write and read-only rights on objects.

All users with the same profile share these same options and rights. A user can have several profiles. A profile is available for all repositories in a single environment.

protection
When several users work on the same project, it is important to provide them with the means to work on a new part of the project without inadvertently interfering with previous work. To do this, you can protect the objects concerned by assigning to them a writing access area (**Hopex Power Supervisor** technical module). It is then possible to connect these objects to others, if the link does not modify the nature of the object. The link orientation determines whether or not the nature of the object is affected.

query
A query allows you to select a set of objects of a given type using one or more query criteria. Most of the MEGA software functions can handle these sets. For example, you can use a query to find all enterprise org-units involved in a project.

reading access
see "reading access area".

reading access area
The user reading access area corresponds to the view the person or person group has of the repository: it defines objects that can be accessed by the person or person group.

reading access diagram
The reading access diagram enables definition of reading access areas and their hierarchical organization. This diagram also enables creation of users and their association with reading access areas.

refresh
Refreshing his/her private workspace allows the user to benefit from changes dispatched by other users since creation of his/her workspace. In this case, it keeps repository modifications carried out by the user without making these available to other users. The system creates a new private workspace and the logfile of previous changes is imported into it.

reject file	When updating a repository (importing, restoring, dispatching), a reject file is created in order to store rejected commands. Rejected commands are stored with the reason for which they were rejected. These are found in the "MegaCrd.txt" file located in the environment folder.
report (MS Word)	Reports (MS Word) managed by **Hopex** are objects allowing you to transfer written knowledge extracted from the data managed by the software.
report (MS Word) element	A report (MS Word) element is the instancing of a report template (MS Word) element. It is the result, formatted in the word processing software, of execution of the query defined in the report template (MS Word) element.
report file	The environment report file, MegaCrdYYYYmm.txt (where YYYY and mm represent year and month of creation) indicates all administration operations (backup, export, restore, controls, etc.) carried out in the environment. The report file is stored in the user work folder associated with the environment system repository: SYSDB\USER\XXX\XXX.WRI where XXX is the user code.
report template (MS Word)	A report template (MS Word) is a structure with characteristics that may be reproduced when producing reports (MS Word). A report (MS Word) can be created and modified as many times as necessary; however to produce several reports (MS Word) of the same type, use of a report template (MS Word) is recommended.
	A report template (MS Word) provides the framework for the report (MS Word), which is completed with data from the repository when the report (MS Word) is created. A template contains the formatting, footers, headers and text entered in MS Word. It also contains report template (MS Word) elements that allow you to format data from the repository. It allows you to produce reports (MS Word) associated with main objects of the repository.
report template (MS Word) element	A report template (MS Word) element is the basic element of a report template (MS Word). It comprises a query which enables specification of objects to be described and a descriptor for their formatting. When creating a report (MS Word) from a report template (MS Word), each report template (MS Word) element is instanced by a report (MS Word) element.

repository	A repository is a storage location where **Hopex** manages objects, links, and inter-repository links.
	The main part is managed by a database system (SQL Server). The remainder is in a directory tree (content of Business Document versions, backup logfiles, locks.
	The different users in the environment can access the repositories connected to it.
repository log	The repository log stores all the updates of users working in a repository. It is reinitialized during the repository reorganization procedure.
repository snapshot	A repository snapshot identifies an archived state of the repository.
	Creating a repository snapshot allows you to label important states in the repository life cycle.
	The repository archived states for which a snapshot exists are not deleted by repository cleanup mechanisms (Repository history data deletion).
restore	A physical restore consists of copying previously saved repository files.
saving	The work done in a private workspace is saved when you request it, or when you exit. By default, the software executes an automatic save (the time interval between two saves is specified in the options: **Options > Repository > Data Saving > Background automatic save**). Messages appear asking you to confirm saving the changes you made in each open report template (MS Word) or report (MS Word) (except during the automatic save). It is recommended that you regularly save your work to avoid losing your work if your computer locks up or loses power.
session	A session is the period during which a user is connected to a repository. A session begins when the user establishes connection and ends when he/she exits **Hopex**. Sessions and private workspaces can overlap. When you dispatch, refresh or discard a private workspace, a new private workspace is created in the same session. Conversely, a user can keep his/her private workspace when exiting a session.
set	A set is a collection of objects with common characteristics. For example, you can build a set of messages sent or received by a certain org-unit in the enterprise. These sets are usually built using queries, and can be handled by most functions of the software.
snapshot	See *repository snapshot*

style A style is a particular format applied to a paragraph of text in a word processor. Styles allow you to systematically apply formats such as fonts, margins, indents, etc. Several styles are available for report (MS Word) configuration. These styles have the M- prefix and are based on the M-Normal style that is similar to the Word Normal style. Note that the M-Normal style text is in blue. All these styles are contained in the Megastyl.dot style sheet.

Terminology A Terminology defines a set of terms used in a specific context instead of the standard term.

text You can associate text with each object found when browsing object descriptors (**Hopex Power Studio** technical module). This text is formatted for MS Word. It presents what will be displayed for each of the objects in the generated report (MS Word). In the text you can insert the object name, its characteristics, and its comment. You can also insert the characteristics of other objects linked to it.

user A user is a person with a login.

The code associated with the user is used to generate file names as well as a specific work folder for the user.

By default at installation, Administrator (Login: System) and Mega (Login: Mega) persons enable administration of repositories and creation of new users.

variable A setting is a parameter of which value is only determined when the function with which it is associated is executed. You can use variables to condition a query (**Hopex Power Studio** technical module). When you execute this query, a dialog box asks you to enter these settings, with a box for each setting defined in the query.

writing access   see "writing access area".

Writing access area   A writing access area is a tag attached to an object to protect it from unwanted modifications. Each user is assigned a writing access area. There is a hierarchical link between writing access areas. A user can therefore only modify objects with the same or lower authorization level. The structure of writing access areas is defined in the writing access diagram. By default there is only one writing access area, "Administrator", to which all objects and users are connected. Writing access management is available with the **Hopex Power Supervisor** technical module.

writing access diagram   The writing access diagram is available if you have the **Hopex Power Supervisor** technical module. With this diagram, you can create users and manage their writing access rights for repositories and product functions. By default only one writing access area is defined, named "Administrator". Attached to it are the "Administrator" and "Mega" persons. This is the highest writing access level and it should normally be reserved for repository management. You cannot delete this writing access area.