MEGA Administration-Supervisor

Web Administrator Guide

HOPEX Aquila 6.1

MEGA
a Bizzdesign company

CONTENTS

Contents

Contents

ABOUT HOPEX ADMINISTRATION

HOPEX administration management is performed via the **Administration** application (Windows Front-End) and via the **Administration** desktop (Web Front-End).

The **Administration** application (Windows Front-End) is the **HOPEX** administration application accessible from the Windows desktop. This application contains the tools required to manage an environment and its repositories (workspaces, locks, repository snapshots, Scheduler). It is also used to manage data accesses (writing access as well as confidentiality using reading access management).

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

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

The **Administration** desktop (Web Front-End) is the **HOPEX** administration application available via an internet browser. This application is used to manage users (persons, person groups, business roles, profiles), repositories (workspaces, locks, repository, repository snapshots) and UI accesses (permissions). This application also provides access to tools (Excel import/export, Import/Export of command files, Scheduler, Exchange Rate) and is used to manage person skills.

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

Most of the functions described here can be used by the User management administrator, whatever the products enabled through his/her security key. However, certain functionalities, like object management are only available with specific technical modules (**HOPEX Power Studio** or **HOPEX Power Supervisor**). These are indicated by a note.

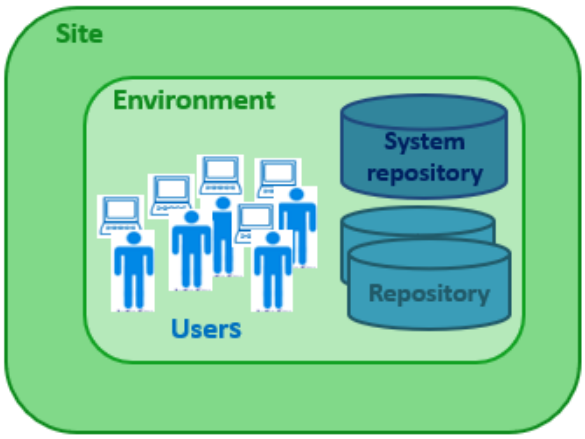
PRESENTATION OF THIS GUIDE

The following points are covered here:

- Web Administration Desktop: access to and description of the **HOPEX** Administration desktop.
- Users: creation of users, user groups and their profiles.
  - The **HOPEX Power Supervisor** technical module is necessary to manage profiles.
  - The **HOPEX Power Studio** technical module is necessary to create profiles.
- Workspaces: principle of private workspaces, dispatch and refresh private workspaces, and lock management.
- Objects: Advanced administration functions available with:
  - the **HOPEX Power Studio** technical module to extract objects
  - the **HOPEX Power Supervisor** technical module for access management to the UI.
- Command File Syntax: description of the syntax used in command files.
- Options: access to options, user level options and language management.
- Glossary: definition of the main terms used in this guide.

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, system data, etc. are managed.
- ***user***
  A user is a person (or person group) with a login and a profile. 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.

1

WEB ADMINISTRATION DESKTOP

The points covered here are:

- ✓ Introduction to Web Administration Desktop
- ✓ Administration Desktop Description

INTRODUCTION TO WEB ADMINISTRATION DESKTOP

The 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, person groups, business roles, profiles)
- repositories (workspaces, locks, repository, repository snapshots)
- permissions (UI accesses).

This application also provides:

- access to tools (Excel import/export, Import/Export of command files, Scheduler, Exchange Rate)
- management of person skills.

Connecting to the 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.*

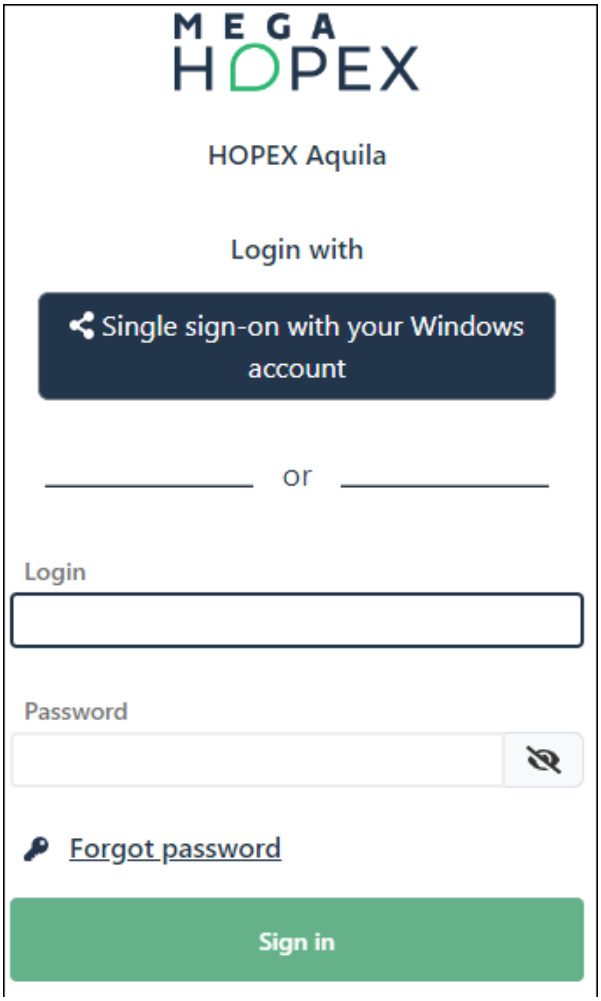
☛ *At installation, only the Mega user can connect to the Web Administration desktop.*

To connect to the **Administration** desktop:

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

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

   The connection page appears.



2. Click your own connection button, or
   use the connection managed by **HOPEX**:
   - In the **Login** field, enter your 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, a new dialog box appears.

4. 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.*

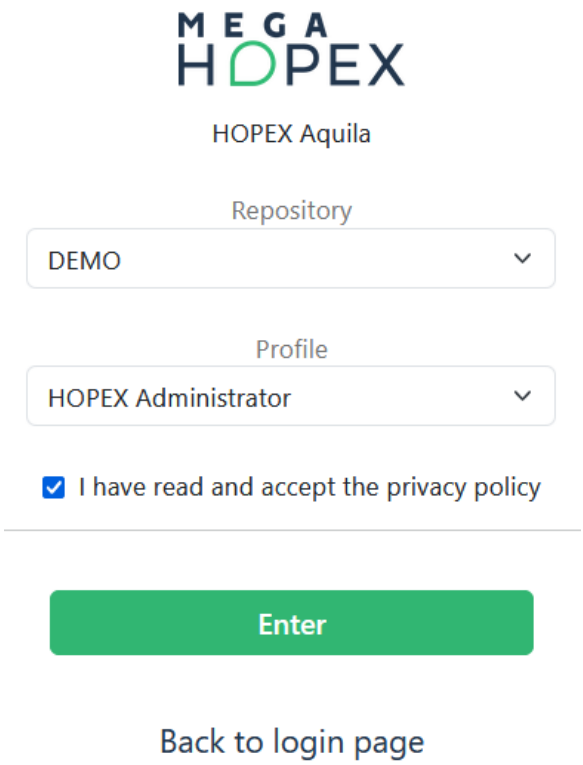
5. In the drop-down menu for profiles, select an administration profile:
   - **HOPEX Administrator**, for global management of users and repositories.
   - **MEGA Administrator - Production**, if you are in production mode
   - **Web user Administrator**, for management limited to users and locks.

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

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

6. (If you belong to a person group) In the group drop-down menu, select the group with which you want to connect or "My assignments" to connect with one of your own assignments.
7. Click the **Privacy and Cookie Policy** link bellow and read the confidentiality policy, then select **I have read and accept the privacy policy**.
   The **Enter** button is active.

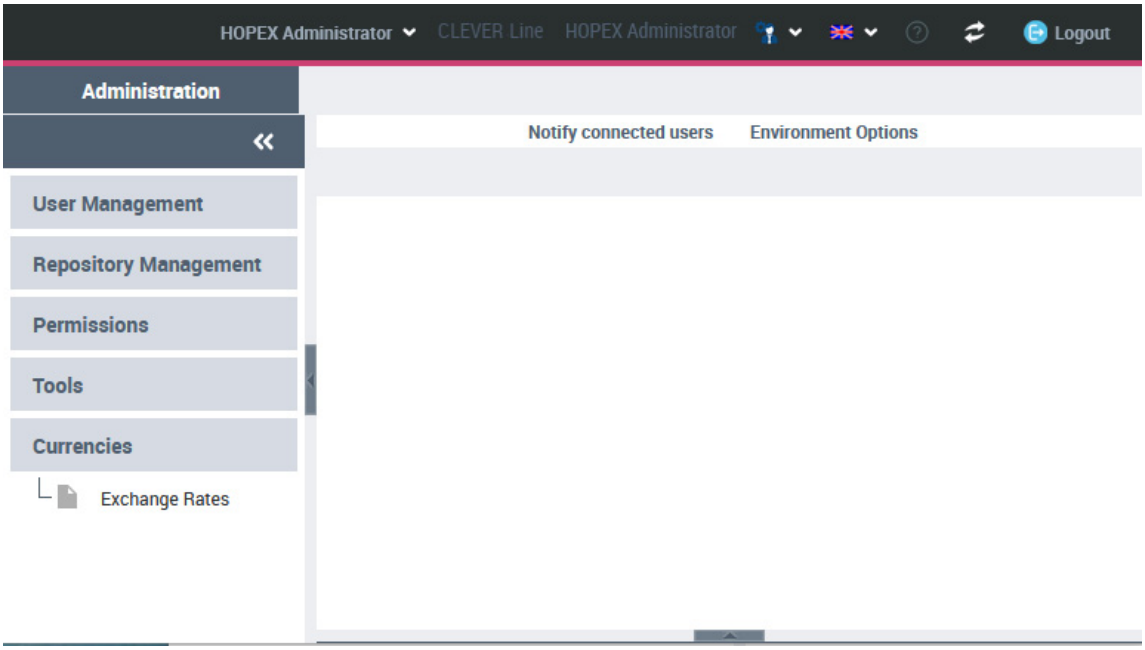
   ☛ *This step is requested only once, when you first log on to a **HOPEX** Web desktop. A certificate is automatically linked to your person.*



8. Click **Enter**.

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

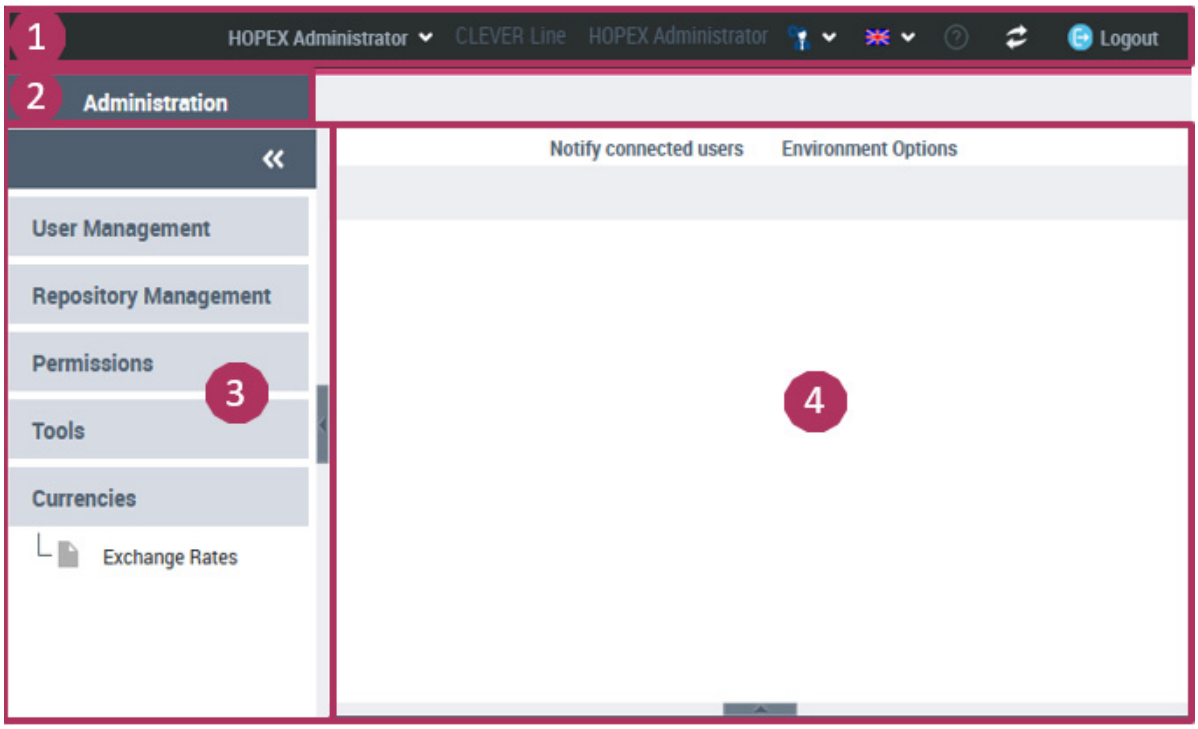
   The **Administration** desktop appears and the session is opened.



☛ *See Administration Desktop Description.*

ADMINISTRATION DESKTOP DESCRIPTION

To access the **Administration** desktop, see Connecting to the Administration Desktop.



1, Toolbar, 2: Administration tab, 3: Navigation panes, 4: Edit area

The **Administration** desktop includes:

- a toolbar.

  ☛ *See Toolbar.*

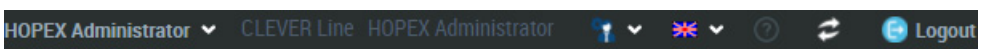
- an **Administration** tab that contains panes and trees to select the objects to manage.

  ☛ *See Navigation panes and trees.*

- an edit area to manage objects.

  ☛ *See Edit area.*

Toolbar



The toolbar displays the name of the user connected as well as the profile with which the user is connected.

From the **Administration** desktop toolbar, you can:

- switch to another profile
- access your account  (**My account**) to:
  - modify your password

    ☛ *See **HOPEX Common Features** - Modifying your Password section*
  - modify your options

    ☛ *For information on options available at user level, see Option Groups.*
  - manage your alerts

    ☛ *See the **HOPEX Common Features** guide - Communicating in **HOPEX** chapter.*
  - obtain information on your licenses
  - reinitialize your personal parameters

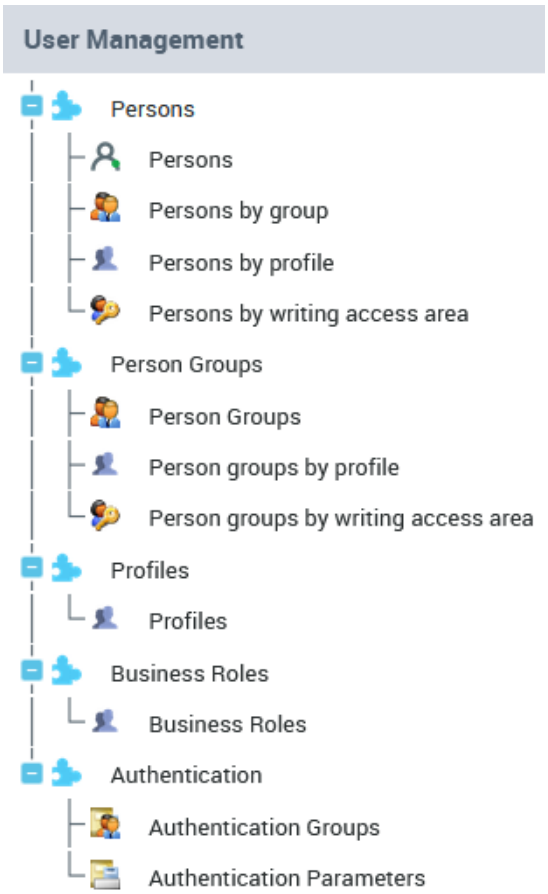
    ☛ *See the **HOPEX Common Features** guide - Resetting your Desktop Customizing section.*
  - access the documentation
- modify the interface data language 

  ☛ *To manage languages, see Managing Languages in Web Applications.*
- access online documentation 
- update your desktop 
- disconnect from the **Administration** desktop  .

Navigation panes and trees

In the **Administration** desktop, the **Administration** tab contains the following panes:

- the **User Management** pane to manage *users*:



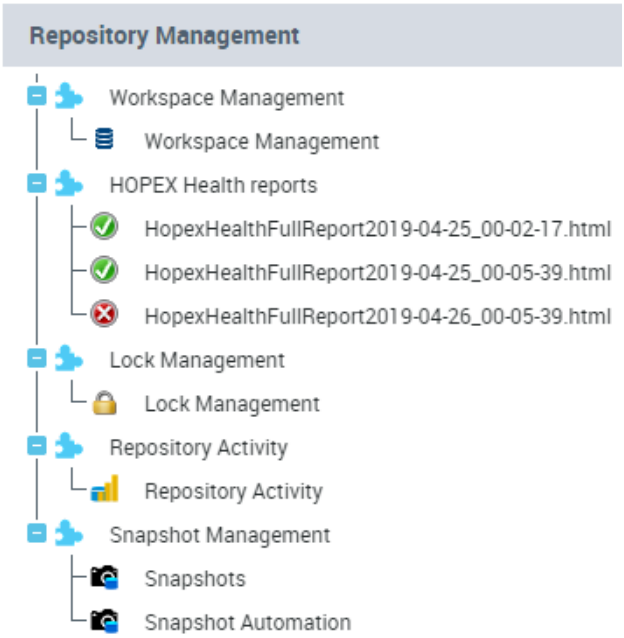
  - the *persons*

    ☛ *The **Persons by reading access area** sub-folder is available if reading access management is activated.*

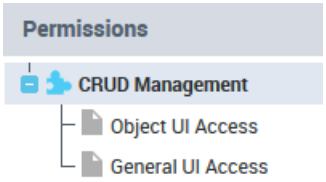
  - the *person groups*

    ☛ *The **Person groups by reading access area** sub-folder is available if management of reading access is activated.*

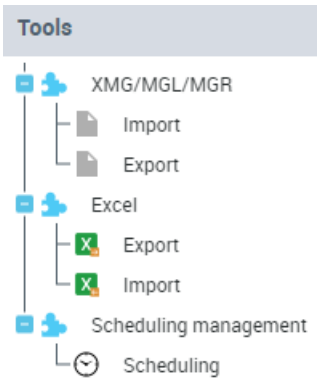
  - the *profiles*
  - the *business roles*
  - the authentication
- the **Repository Management** pane to
  - manage the *workspaces*, the *locks*, the *repository* and the *snapshots*
  - access the repository health reports



- the **Permissions** pane to manage *object UI access* and *general UI access*



- the **Tools** pane to:
  - import or export command files or data in XMG, MGL or MGR formats
  - import or export objects with the Excel import/export wizard
  - import Visio diagrams
  - view the scheduling (Triggers)



- **Currency** pane to manage exchange rates.

  ☛ *See the "Functional Administration" chapter for the **HOPEX** solutions concerned.*

Edit area

When you select an element in the left part (navigation panes and trees), the management page of this element appears in the edit area.

You can:

- notify connected users by e-mail (**Notify connected users**)
- manage the environment options (**Environment Options**)

USERS

This chapter explains 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:

Overview

- ✓ Big Picture: Actions to Define a User

Introduction

- ✓ Introduction to Profile Management
- ✓ Introduction to User Management
- ✓ Introduction to Person Group Management

Management

- ✓ Managing Profiles (Available with HOPEX Power Supervisor)
- ✓ Access to User Management
- ✓ Creating and Managing Users
- ✓ Creating and Managing a Person Group
- ✓ Managing User Options
- ✓ Authentication in HOPEX
- ✓ Mapping
- ✓ Managing the Password of a Web User
- ✓ Managing Languages
- ✓ Managing Business Roles

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.
- Ensure that the profile that you want to assign him/her is created. Then you can create the user in a predefined way with the profile criterion.

  ☛ *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 Login Characteristics), the products accessible to this user are at the intersection of 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 Connection Diagrams.*

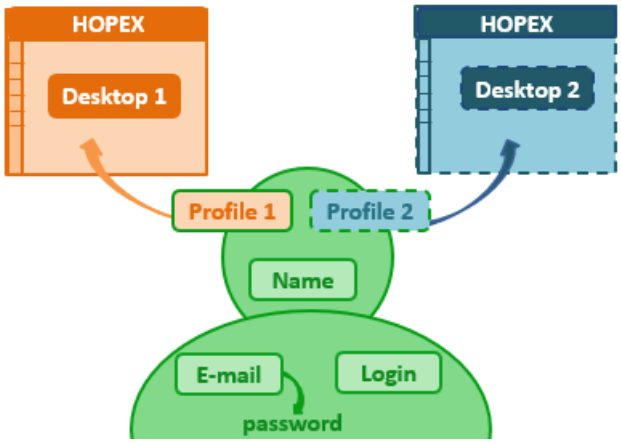
- the UI access rights (permissions) of the user

Assigning a profile to a person defines:

☛ *See Assigning a Profile to a Person.*

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

Compulsory Actions to Define a User



To create a user who can connect to **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 Specifying SMTP Configuration.*

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

  The user must have at least one profile assigned to be able to connect to HOPEX, or must belong to a person group.

  A person belonging to a person group can connect 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 for the connection.

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 Specifying SMTP Configuration.*

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

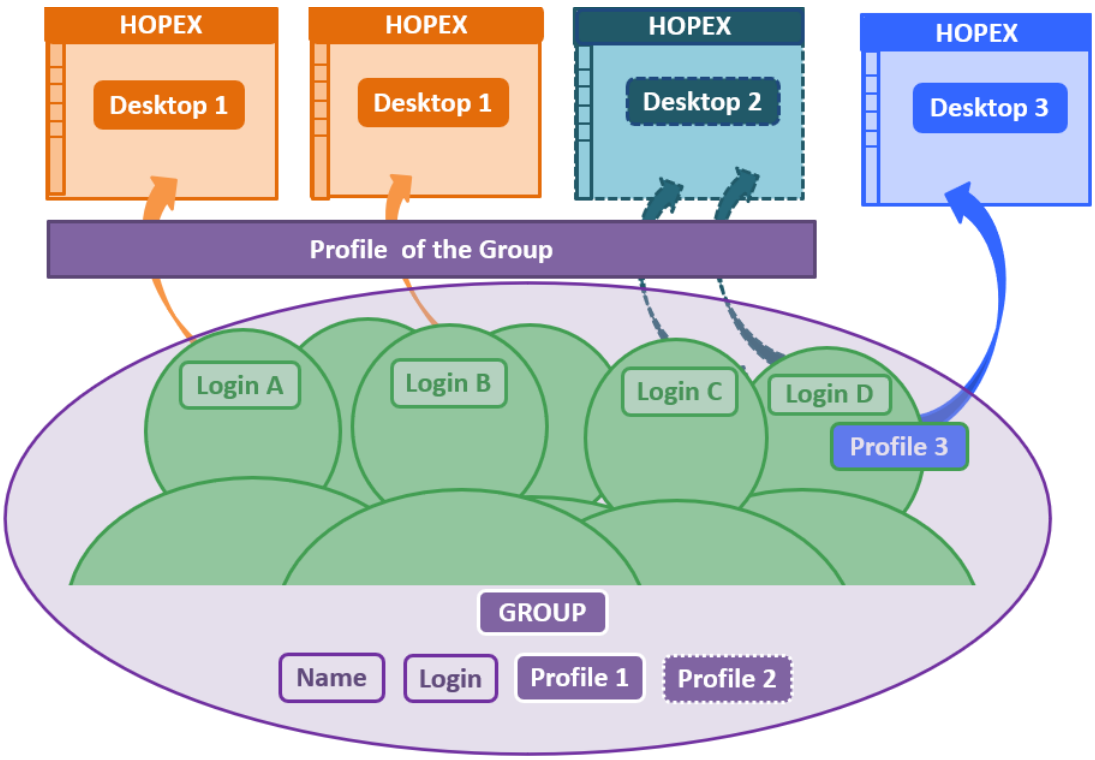
  ☛ *To send the account activation e-mail again, see Initializing a User Web Account.*

- 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.*

- define the ***login*** 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.

  ☛ *The login of the person group is automatically created at creation of the person group, see Creating a Person Group.*

  ☛ *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 a mass assignment of profiles 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 and questionnaires, or when a user loses his/her password.*

  ☛ *See Defining a Person.*

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

  ☛ *See Defining a Person.*

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

- (where reading access management is 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.*

Other Actions to Set or Manage a User

You can:

- define the telephone number and initials of the person
  - ☛ *See Defining a Person.*
- define the data language of the Web user
  - ☛ *See Defining a Person.*
- restrict 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 user authentication mode
  - ☛ *See Defining the Login of a Person.*
- make the user inactive.
  - ☛ *See Defining the Login of a Person.*
  - ☛ *See Preventing User Connection.*

Checking the Configuration of Users

From the **Administration** desktop, you can check the persons who do not comply with all the definition rules.

To check the configuration of users:

1. Access the **User Management** pages.
   - ☛ *See Accessing the User Management Pages.*
2. Select the **Persons** or **Person Group** sub-folder.
3. In the list of persons, select the persons whose configuration you want to check.
   - ☛ *If you do not select a person, the check takes place on all the persons listed in all the pages.*
4. In the edit area, click **Check**  .
   - ☛ *If the button is hidden, click*  *to access it.*

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

INTRODUCTION TO PROFILE MANAGEMENT

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:

- Description of a Profile
- Connection Diagrams
- Administration Profiles Provided
- Profile Properties

Description of a Profile

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.*

Definition of the profile

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

`E.g.: Administrateur Fonctionnel EA, 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 online documentation: Concepts > Profiles.*

If a user already has restricted access rights to products (see Viewing the Login Characteristics), the products accessible

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

- the desktops to which the user can access.

  ☛ *See Connection Diagrams.*

  ☛ *See Assigning a WET to a profile or Defining the applications accessible to the users of a profile (non WET-based configuration).*

- the user's access rights to UIs (permissions)

  ☛ *See Managing UI Access (Permissions).*

- the same options for all the users connected with this profile

  ☛ *See Options.*

Profile assignment

You must assign each person at least one profile so that this person can connect to **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 person's data access rights (reading, writing) 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.*

Connection Diagrams

The connection diagram relies on the desktop creation, that is whether the desktop is based on a Work Environment Template (WET) or not.

Connection diagram (with WET)

Using a Working Environment Template (WET) enables to homogenize the display of the desktops.

☛ *For detailed information regarding the WET creation, see HOPEX Power Studio - Versatile Desktop documentation.*

To connect to **HOPEX**, a person must have:

- a login

  ☛ *See Creating a User.*

  ☛ *The login status must be active so the person can connect, see Status (Login).*

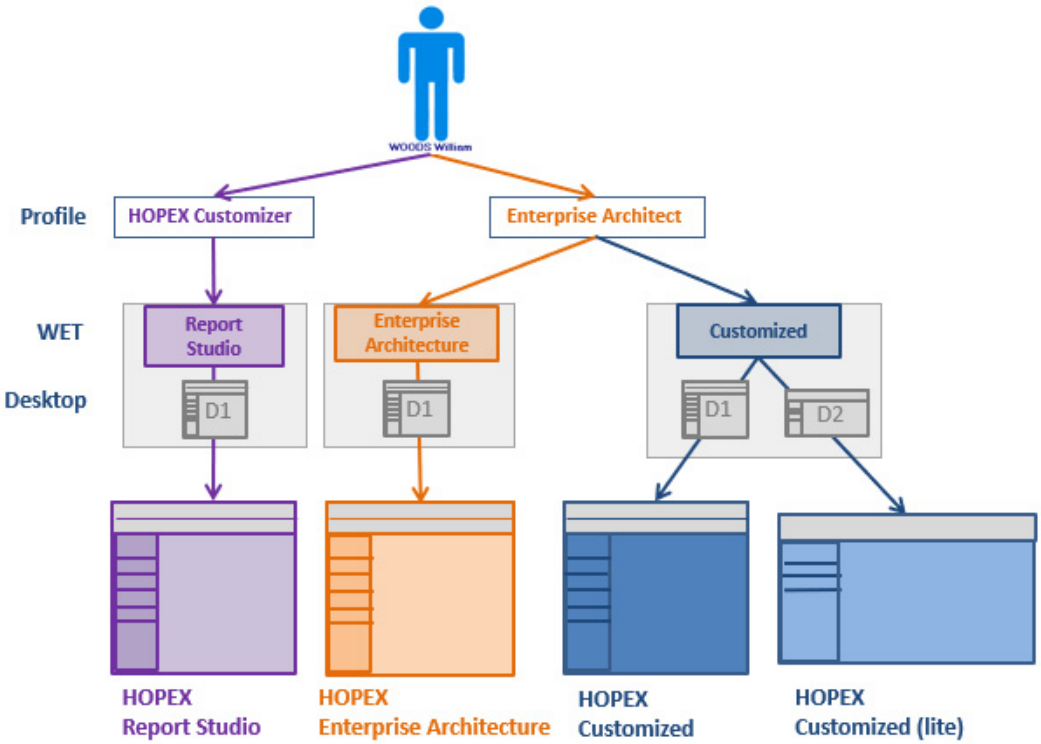
- at least one profile
  The profile gives access to one or several WET-based desktops.

  ☛ *See Assigning a Profile to a Person.*

  At least one WET (with one or several associated desktops) must be assigned to the profile. A desktop manager enables to define the desktops associated with this WET-profile assignment.

  ☛ *See Assigning a WET to a profile.*

  ☛ *In a non WET-based configuration, applications (and their associated desktops) are connected to the profile.*



In the above example, William WOODS has an active login. He can connect to:

- **HOPEX Report Studio** with the **HOPEX Customizer** profile.
- **HOPEX Enterprise Architecture** with the **Enterprise Architect** profile.
- **HOPEX Customized** with the **Enterprise Architect** profile and choose a device (computer or tablet) adapted display.

Connection diagram (without WET)

To connect to **HOPEX**, a person must have:

- a login

  ☛ *See Creating a User.*

  ☛ *The login status must be active so the person can connect, see Status (Login).*

- at least one profile.

  ☛ *See Assigning a Profile to a Person.*

  So that a user of a profile can connect to an application, you must connect this application to the profile concerned.

  All desktops connected to the application are then accessible.

  ☛ *To modify a profile provided by **MEGA**, see Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile.*

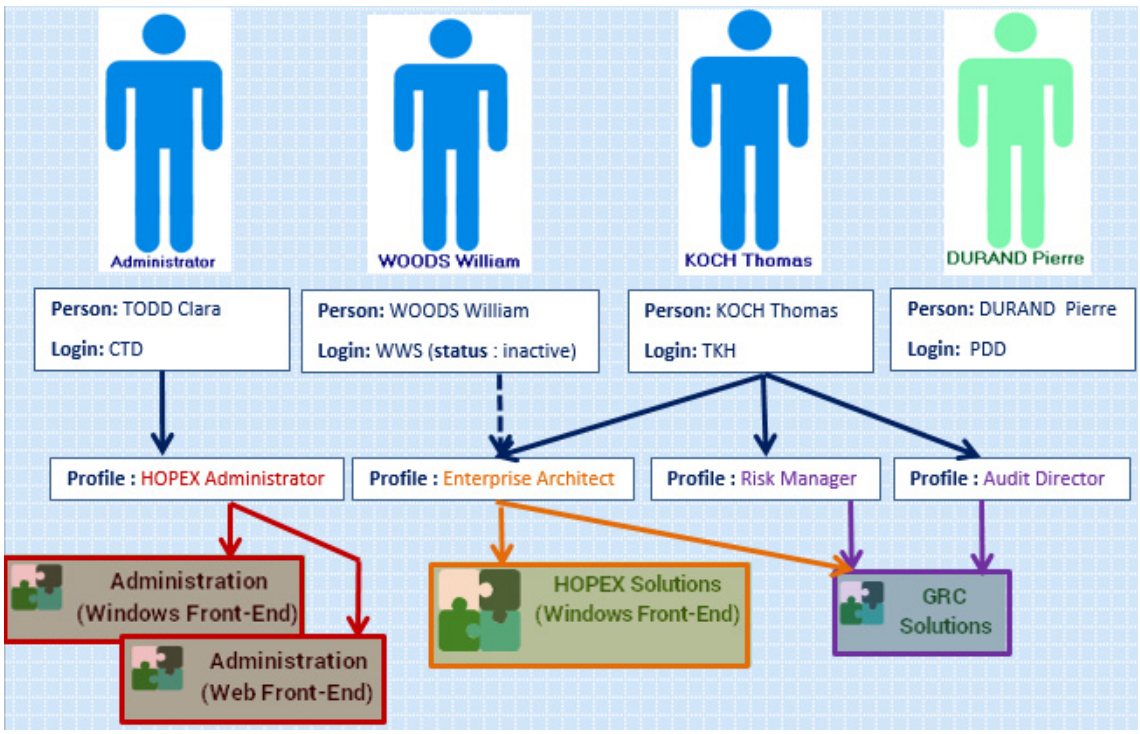
  ☛ *To enable access to only certain desktops of the application, see Restricting access to the desktops of an application.*

  Example:

  A1 application is connected to **P1** profile and **A2** application is connected to **P2** profile.

  None of the desktops of **A1** and **A2** applications are directly connected to **P1** and **P2** profiles.

  The user U1, who is assigned the **P1** and **P2** profiles, has access to all of the desktops of **A1** and **A2** applications.



In the previous example:

- Clara TODD has a login and the **HOPEX Administrator** profile assigned: she can connect to **Administration** applications (Windows Front-Endand Web Front-End).
- William WOODS has the **Enterprise Architect** profile assigned but the status of his login is inactive:
he cannot connect to **HOPEX**.
- Thomas KOCH has a login and the **Enterprise Architect**, **Risk Manager** and **Audit Director** profiles assigned:
he can connect to **HOPEX Solutions (Windows Front-End)** and **GRC Solutions** applications.
- Pierre DURAND has a login but does not have an assigned profile:
he cannot connect to **HOPEX**.

Restricting access to the desktops of an application

A user can connect to an application via customized desktops according to actions to be performed.

If an application contains several desktops, you can specifically define application desktops that are accessible to the concerned profile. To do this, you must connect to the profile:

> ☛ *To modify a profile provided by **MEGA**, see Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile.*

- the application containing the desktops.

> ☛ *See Defining the applications accessible to the users of a profile (non WET-based configuration).*

- the desktops you want the users of the profile can connect to.
The application desktops that are not connected to the profile are not accessible to users of the profile.

> ☛ *To enable access to only certain desktops of the application, see Defining the application desktops accessible to the users of a profile (non WET-based configuration).*

Example:

P1 profile is connected to:

- **A1** application, which particularly includes D1, D2, D3, D4, and D5 desktops.

- D2 and D5 desktops of the A1 application.

User U1 with the **P1** profile can connect only to the D2 and D5 desktops of the **A1** application. He is not allowed to access D1, D3, and D4 desktops.

Administration Profiles Provided

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

When several users with an Administration profile connect to **HOPEX Administration** at the same time, certain actions, such as user management, are exclusive.

These profiles are dedicated to:

- global Administration, with exclusive access to **Administration** applications (Windows Front-End and Web Front-End):
  HOPEX Administrator

  ☛ *See HOPEX Administrator profile.*
- Administration (Web Front-End), with exclusive access to the **Web Administration** desktop:
  - **HOPEX Administrator - Production**

    ☛ *See HOPEX Administrator - Production profile.*
  - **User Management Web Administrator**

    ☛ *See User Management Web Administrator profile.*

    ☛ *See Profile Properties.*

If needed you can modify the rights and access to applications defined on these profiles.

☛ *See Customizing the UI Access (Permissions) of an Existing Profile and Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile.*

HOPEX Administrator profile

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

In the **Web 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.*

- **Profiles**

  ☛ *See Managing Profiles.*
- *users* (**Persons** and **Logins**)

  ☛ *See Creating and Managing Users.*
- *User groups* (**Person groups** and **Logins**)

  🕮 *(Web Front-End specific) A person group groups persons in a group. These persons share the same connection characteristics.*

  ☛ *See Creating and Managing a Person Group.*
- **Business Roles**

  ☛ *See Managing Business Roles.*
- **Permissions**

  ☛ *See Managing UI Access (Permissions).*
- **Authentication**

  ☛ *See Authentication in HOPEX.*

It also allows to perform tasks linked to:

- **Repository management**:
  - workspace management
    - ☛ *See Workspaces.*
  - repository activity management
    - ☛ *See Managing Updates.*
  - lock management
    - ☛ *See Managing locks.*
  - snapshot management
    - ☛ *To create a repository snapshot, see the **HOPEX Common Features - Repository Snapshots** guide.*
- **Tools** such as:
  - XMG/MGL/MGR file import/export
    - ☛ *See Importing a command file in HOPEX.*
    - ☛ *See Exporting Objects.*
  - Excel file import/export
    - ☛ *See the **HOPEX Common Features** guide, "Exchanging Data With Excel" chapter.*
  - scheduler use
    - ☛ *See Scheduling (Scheduler).*

HOPEX Administrator - Production profile

The **HOPEX Administrator - Production** profile is the equivalent of the **HOPEX Administrator** profile in the **Web Administration** Desktop, without permission management rights.

User Management Web Administrator profile

The **User Management Web Administrator** profile allows, in particular, to manage:

- *users* (**Persons** and **Logins**)
  - ☛ *See Creating and Managing Users.*
- *User groups* (**Person groups** and **Logins**)
  - 🕮 *(Web Front-End specific) A person group groups persons in a group. These persons share the same connection characteristics.*
  - ☛ *See Creating and Managing a Person Group.*
- **Business Roles**
  - ☛ *See Managing Business Roles.*

It also gives access to management of:

- **Authentication**
  - ☛ *See Authentication in HOPEX.*
- **Locks**
  - ☛ *See Managing locks.*

Profile Properties

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

☛ *See Description of a Profile.*

☛ *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.*

☛ *To manage profiles, see Managing Profiles.*

Name

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

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 determine 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 Login Characteristics), 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**.*

Profile display

A profile is provided by default at connection when it is not included in another profile.

The **Profile Display** attribute defines when the profile is provided at connection:

- "always": the profile is provided at connection even if it is included in the definition of another profile,

  ☛ *See Customizing the UI Access (Permissions) of an Existing Profile.*

- "If not included in another profile" (default value): the profile is provided at connection only if it is not included in another profile.

Profile status

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

Administrator profile

Only the user whose current profile has the **Administrator Profile** attribute with value "Yes" can:

- assign an administrator profile (see Administration Profiles Provided) to another user.
- declare a profile as administrator.
  That is, specify value "Yes" for the **Administrator Profile** attribute of any profile.

The default value of **Administrator Profile** is "No".

Assignable

The **Assignable** attribute defines if the profile is assignable to a Login or not.

☺ *This attribute enables filtering of profiles and improves visibility of profiles to be assigned.*

☛ *The default value is "No".*

_GUIName

The **_GUIName** attribute enables definition of the profile name display in the interface.

Set of UI access rights

Set of UI Access Rights defines permissions associated with one or several profiles.

Covered domain

Covered Domain defines the domain covered by the profile. This domain defines in particular certain elements of the profile desktop homepage and diagram types proposed in the diagram creation wizard. The same **Covered Domain** can be used by several profiles.

Homepage report

Homepage Report enables to define a default report on the profile homepage for users connected with the current profile.

☛ *See Defining a default report on the homepage.*

Tiles Homepage (WET)

Tiles Homepage defines the profile homepage, that is:

- the tiles included in the homepage
- the color or image background
- the tile default color

This homepage must be one of the homepages defined for the WET assigned to the profile.

☛ *For more details on the homepage, see HOPEX Power Studio - Versatile Desktop - Using a Working Environment Template (WET) documentation.*

Homepage

Homepage defines the homepage of the current profile.

MetaPicture

MetaPicture enables customization of the icon representing the current profile.

Persons and Person Groups

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

Working Environment Template (WET)

The **Working Environment Template Assignments** page enables to assign a WET (Working Environment Template) to the profile. This WET defines the desktops to which the profile gives access and their display.

☛ *See Assigning a WET to a profile.*

☛ *For more details on the WET use and creation, see HOPEX Power Studio - Versatile Desktop - Using a Working Environment Template (WET).*

Available applications

In cases where a **Working Environment Template (WET)** is not defined, the **Available Applications** page is used to define the applications to which the current profile gives access.

☛ *See Defining the applications accessible to the users of a profile (non WET-based configuration).*

Available desktops

In cases where a **Working Environment Template (WET)** is not defined, the **Available Desktops** page is used to restrict the desktops to which the current profile gives access. By default all the desktops connected to the application are accessible.

☛ *To restrict the desktops accessible, see Defining the application desktops accessible to the users of a profile (non WET-based configuration).*

Reporting presentation

The **Reporting** property page of an object gives access to the available reports of the accessible products. Reports of the main product are displayed at the first level.

The **Reporting presentation** page enables to define this first level.

☛ *See Defining the report display level (property pages of an object).*

Assignable profiles

The **Assignable Profiles** page lists the profiles that the current profile allows to assign.

Profiles with **Administrator Profile** attribute to "Yes" can assign any profile.

☛ *To assign a profile, see Assigning a Profile to a Person.*

Terminology

The **Terminology** page is used to associate a terminology with the profile.

☛ *See Associating a terminology with a profile.*

Available types

The **Available Types** page enables definition of the specific objects available for the profile:

- Document category
- Business Document Pattern
- Report DataSet Definition
- Widget

☛ *See Defining the object types available for a profile.*

INTRODUCTION TO USER MANAGEMENT

☛ *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.*

- permissions:
  - *object UI access*

    📖 *Object UI access defines user rights on creation, reading, update, and deletion on these objects and their tools. By default, object UI accesses have value *CRUD (C: create, R: read, U: update, D: delete, *: default value).*

  - *general UI access*

    📖 *General UI access defines if tools are available or not. By default, general UI accesses have value *A (A: Available, *: default value)*

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 Person Characteristics
  - Viewing the Login Characteristics

Users Provided

By default, at installation the following are created in the environment:

- 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).*

    ☛ *The "Administrator" user can create a first user with the "HOPEX Administrator" profile to manage repositories and users.*
  - ***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 by way of 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 manage repositories and users.*

User: Definition

For each environment, a user has:

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

  ☛ *see Viewing the Person Characteristics.*
- a **login** which defines his/her connection identifier, his/her status and his/her 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 **profile** assigned that 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 Managing Profiles.*

  ☛ *see Assigning a Profile to a Person.*
- **options**

  ☛ *see Options.*
- (optional) one (or more) **business role(s)** is/are used to assign a task to a person (example: an audit mission or an action plan) and, where appropriate, for a specific location (example: Paris agency).

  ☛ *see Assigning a Business Role to a Person.*

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

☛ *see Administration Profiles Provided.*

Person Properties

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

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

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
```

Data language

The **Data language** attribute of the person is specific to Web applications. It enables definition of 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 in the environment options for all users at installation (**Options>Installation>Languages**) via 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 are only visible when the **Activate reading access diagram** option is selected in the **Options** of the **Repository** of 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 is a ***reading access areas***.

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.

Person 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.

Login

The login of a person is a unique character string uniquely identifying the person that can connect. The person without a login cannot connect to ***HOPEX***.

`Example: pdurand, pdd`

☛ *For more details, see Login Properties (Person).*

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 or group connected to a macro).

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

  ☛ *See Defining a dynamic person group with a Macro.*

  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 or group connected to a macro): 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.

Assignments - Profile Assignments

To connect to **HOPEX**, a person must have at least one profile assigned. The profiles assigned to the person are listed in the **Assignments > Profile Assignments** page.

The profile determines:

- the objects and tools to which the person has access

  ☛ *See Managing UI Access (Permissions).*
- the Web applications to which the person can connect.
- repository access
- access to products

  ☛ *See Description of a Profile.*

  ☛ *See Assigning a Profile to a Person.*

Object assignments

Object assignment enables to assign a task to a person (example: an audit mission or action plan) and where appropriate, for a specific location (example: Paris agency). The objects assigned to the person are listed in the **Assignments > Assignment of profiles** page.

☛ *See Managing Business Roles.*

☛ *See Assigning a Business Role to a Person.*

Login Properties (Person)

To:

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

User code

The **User Code** is the short identifier (upper case, maximum length 6 characters) of the user that serves as the basis for private workspace naming.

This code is defined automatically on user creation. To ensure data consistency, it should not be modified.

E.g.: PDD

Login Holder

The login holder is the person associated with the login.

E.g.: DURAND Pierre

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.

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).
- **Windows (deprecated)**
  Passwords are stored and managed by Windows. The user connected via Windows is automatically recognized in HOPEX (his/her password is not requested)

INTRODUCTION TO PERSON GROUP MANAGEMENT

☛ *Only a user with Administrator type profile has management 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*

    📖 *(Web Front-End specific) 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.*

- *object UI access*

  📖 *Object UI access defines user rights on creation, reading, update, and deletion on these objects and their tools. By default, object UI accesses have value *CRUD (C: create, R: read, U: update, D: delete, *: default value).*

- *general UI access*

  📖 *General UI access defines if tools are available or not. By default, general UI accesses have value *A (A: Available, *: default value)*

The following points are detailed here:

- introduction:
  - Managing Person Groups Rather than Persons
  - Belonging to a Person Group
- properties:
  - Person Group Properties
  - Login Properties (Person Group)
- access:
  - Accessing the User Management Pages
- characteristics:
  - Viewing the Person Group Characteristics
  - Viewing the Login Characteristics

Managing Person Groups Rather than Persons

To facilitate 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 Description of a Profile.*
- 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 through the group or via his/her 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 more than one person 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 or group connected to a macro).
  - ☛ *See Defining a dynamic person group (SSO).*
  - ☛ *See Defining a dynamic person group with a Macro.*

  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 or group connected to a macro): 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 Person Group Characteristics, and Modifying a Person Group Login.*

Name

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

```
E.g.: HR Department
```

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** is selected in the **Options** of the **Repository** of the environment.*

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 is a ***reading access areas***.

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.

Login

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

☛ *For more details, see Login Properties (Person Group).*

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

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.*

Person group types

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 group persons on the fly.
  ☛ *See Connection request and user created on the fly.*
  Examples of dynamic groups:
  - SSO type groups (SSO authentication case)
    ☛ *See Defining a dynamic person group (SSO).*
  - groups connected to a macro (the macro checks if the person belongs to the group or not)
    ☛ *See Defining a dynamic person group with a Macro.*

SSO type dynamic group

An SSO type group is characterized by claims.

Dynamic group connected to a macro

The implemented macro calculates a list of persons connected to the person group. Persons resulting from the macro use the configuration defined on the person group, notably access to roles.

The macro should implement the following function:

```
Function IsUserExists (oPersonGroup, sUserName as String)
as Boolean

sUserName: authentication login of the person.

oPersonGroup: person group object executing the query.
```

The function returns TRUE if the person belongs to the group, FALSE if not.

Persons

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

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 in the environment options for all users at installation (**Options>Installation>Languages**) via the **Data language** option.*

Assignments - Profile

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 profiles assigned to the person group are listed in the **Assignments > Profile Assignments** page.

The profile determines the following for the person group:

- the applications and desktops accessible
- access to repositories
- the products accessible

  ☛ *See Description of a Profile.*
- the objects and tools accessible

  ☛ *See Managing UI Access (Permissions).*

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 Login Characteristics.
- 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.

Authentication mode (case of authentication managed within HOPEX)

Default value of the **Authentication Mode** parameter on the user login is inherited at user creation from the **Authentication Mode** option defined in the options of the environment (**Options** > **Installation** > **User Management**).

☛ *See Modifying the HOPEX Authentication Mode.*

Authentication mode of a user is by checking the user password. Available authentication modes are:

- **MEGA**
  Passwords are managed and stored in the **HOPEX** repository.
  This is default authentication mode.

  ☛ *For more details, see Authentication in HOPEX.*

- **Windows**
  Passwords are managed and stored in Windows. This allows the user connected to Windows to be recognized automatically when he/she is connected to **HOPEX** (Windows Front-End), not requiring entry of his/her password.

  ☛ ***Attention**: to connect to a **HOPEX** (Web Front-End) application, the user must enter his/her password.*

  The list of users in your **HOPEX** environment is automatically synchronized with the list of users defined in your Windows network.

  ☛ *For more details, see Configuring SSO Authentication.*

MANAGING PROFILES

☛ *Profile management is only available with the **HOPEX Power Supervisor** technical module.*

☛ *Profile creation is only available with the **HOPEX Power Studio** technical module.*

The *profiles* are managed in the **HOPEX Administration** desktop.

☛ *See Introduction to Profile Management.*

🕮 *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
- Customizing the UI Access (Permissions) of an Existing Profile
- Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile
- Creating a Profile
- Configuring a Profile
- Checking Profile Compliance with Connection Regulation
- Assigning a Profile to a Person
- Assigning a Profile to a Person Group
- Deleting a Profile

To:

- modify profile options

  ☛ *See Options.*

- manage metamodel filters at profile level

  ☛ *See Managing UI Access.*

- implement data access rules for the profile

  ☛ *See Managing Data Access Dynamically (HOPEX Administration documentation).*

- compare profile permissions

  ☛ *See Generating a Report on Permissions by Profile.*

Viewing Profile Characteristics

To view profile characteristics:

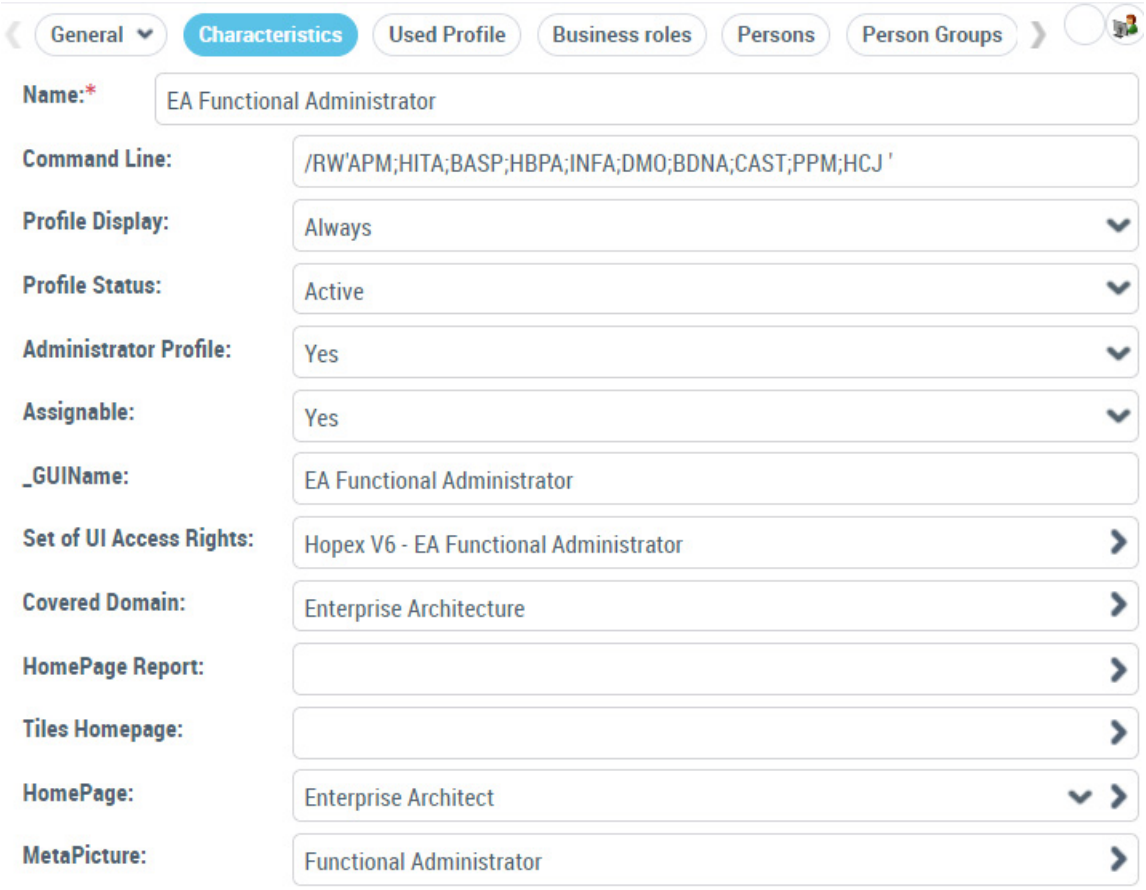
1. Access the user management pages.

   ☛ *See Accessing the User Management Pages.*

2. Select the **Profiles** sub-folder.
3. In the edit page, select the profile.

4. In the toolbar, click **Properties** .
   The profile **Properties** window are displayed.

   ☛ *For detailed information on characteristics of a profile, see Profile Properties.*



☛ *See Configuring a Profile.*

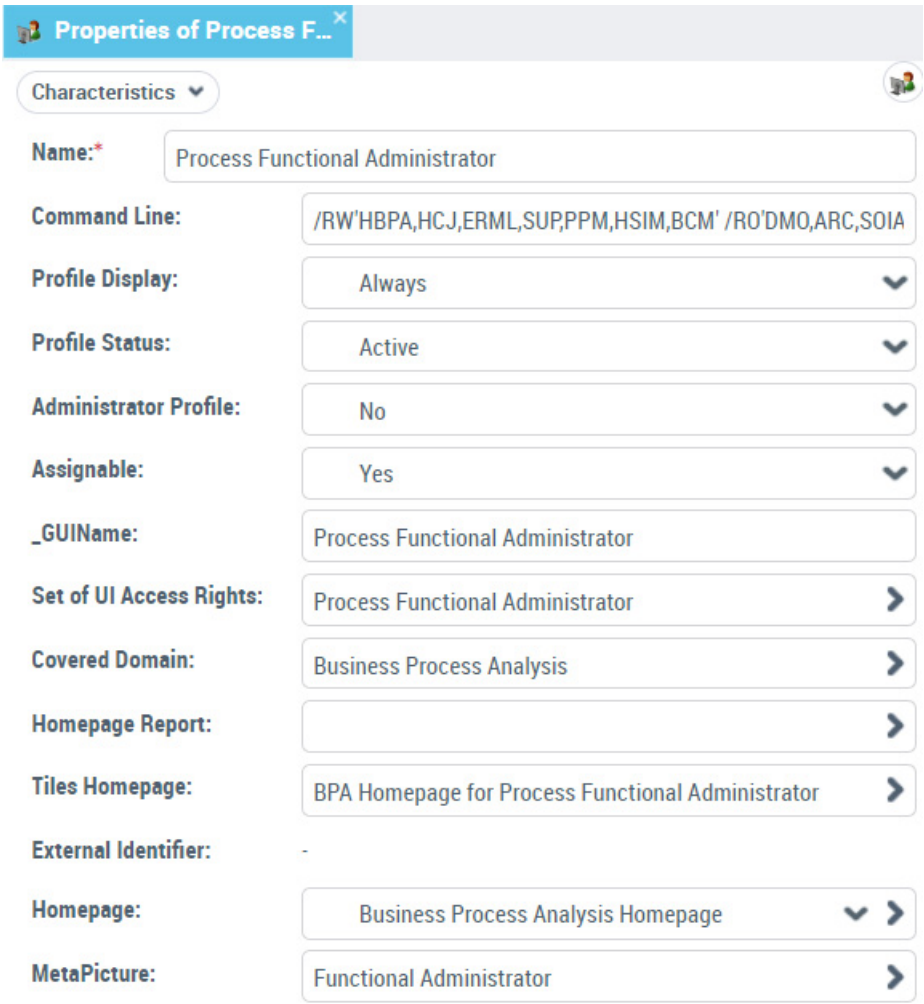
Customizing the UI Access (Permissions) of an Existing Profile

MEGA provides profiles adapted to each Solution or product. However, you might need to customize the UI access (permissions) of these profiles. For this purpose **MEGA** recommends you to create a **Set of UI Access Rights** from the **Set of UI Access Rights** of the profile concerned, then to customize it.

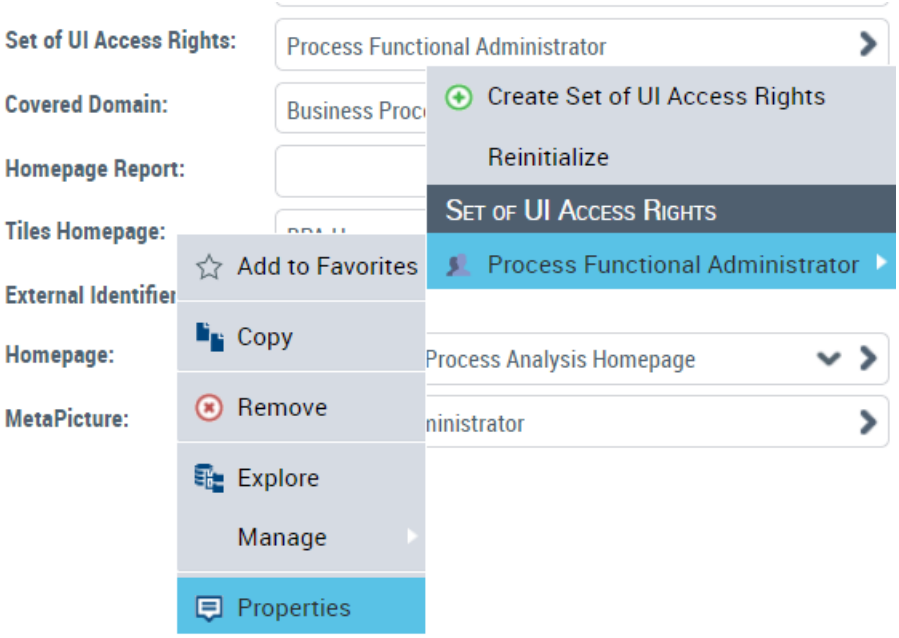
To customize the UI Access (Permissions) of a profile:

1. Access the properties of the profile.

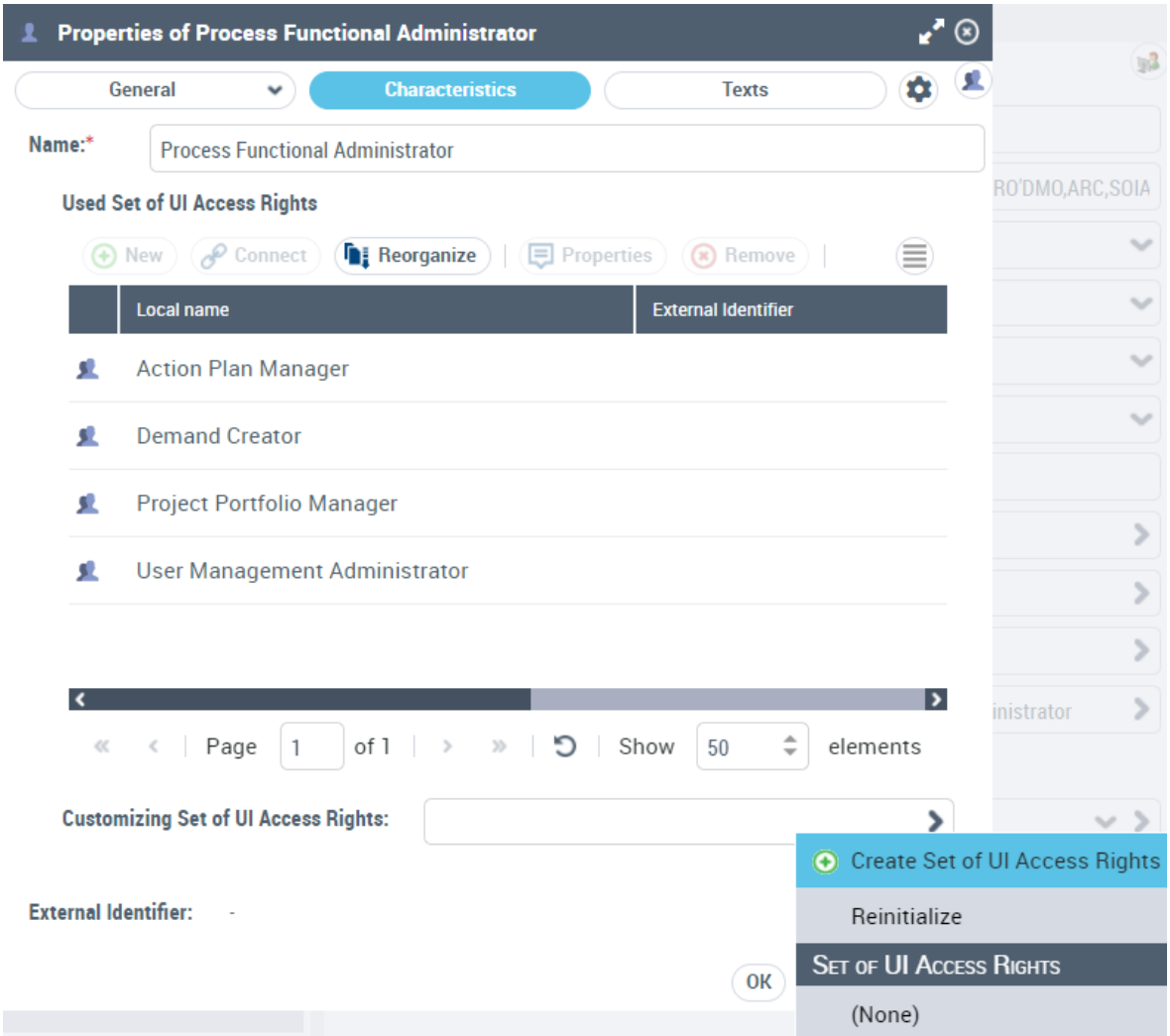
   ☛ *See Viewing Profile Characteristics.*



2. In the **Set of UI Access Rights** field, click the arrow and access its **Properties**.

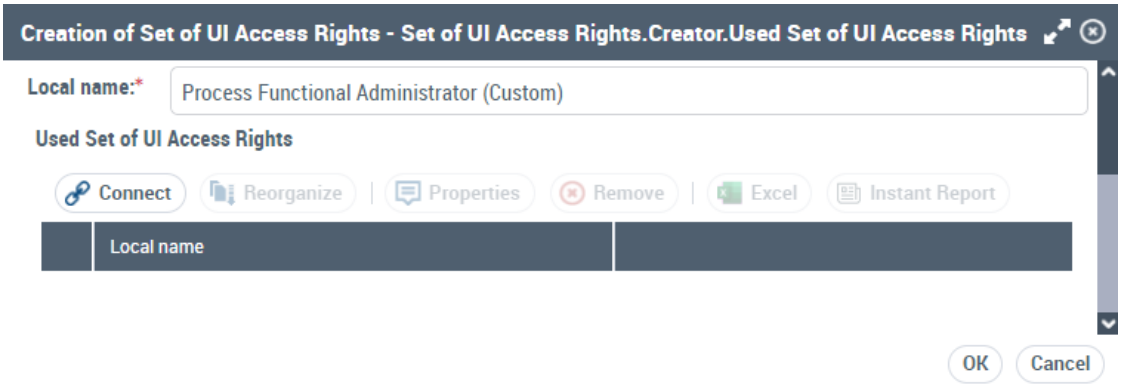


3. In the **Characteristics** page, click the arrow of the **Customizing Set of UI Access Rights** and select **Create Set of UI Access Rights**.

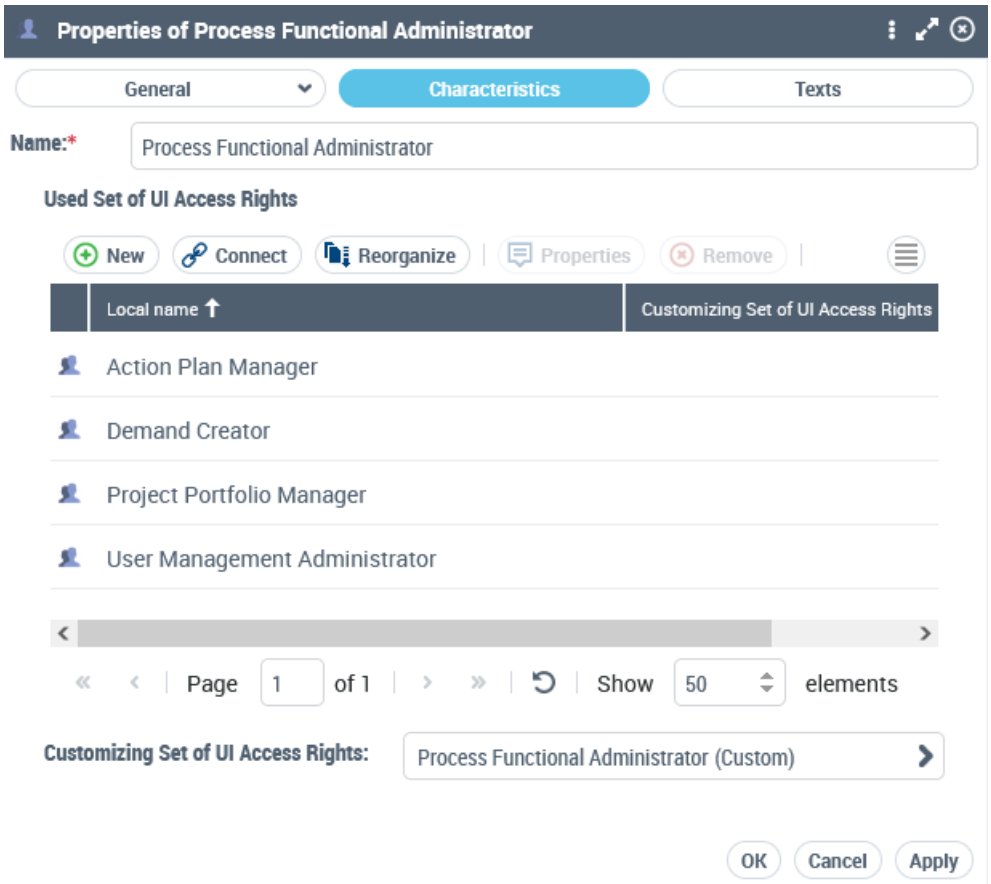


The name format of the Set of UI Access Rights is predefined as:

```
<Name of the Set of UI Access Rights of the profile
concerned> (Custom)
```



4. (If needed) Modify its **Name**.
5. Click **OK**.
   The set of UI access rights you created is predefined with the same UI access rights as those defined for the profile concerned.



6. Click **OK**.

7. Customize the UI Access of the set of UI Access rights you just created.

   ☛ *See Managing UI Access (Permissions) and in the **Access Rights** field select the Set of UI access rights you just created.*

Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile

MEGA provides profiles adapted to each Solution or product. However, you may need to customize the characteristics of a profile provided by **MEGA** (for example connect a terminology).

☺ ***To customize a profile provided by MEGA, MEGA recommends to create a profile and base its Set of UI access rights on those of the profile you want to customize.***

To customize the characteristics of a profile provided by **MEGA**:

1. Create a profile and configure its **Set of UI Access Rights** by aggregating the set of UI access rights of the profile on which is based your profile.

   ☛ *See Creating a Profile.*

2. Configure the profile.

   ☛ *See Configuring a Profile.*

Creating a Profile

☛ *Profile creation is only available with the **HOPEX Power Studio** technical module (MTS2).*

Users with the same profile share common characteristics (e.g.: options, authorized products, UI access rights).

To create a profile you must define:

- its name
- its set of UI access rights

  ☛ *Defining UI access rights might be tricky. To facilitate the definition, you can use one (or several) **Set of UI access rights** already defined.*

  The set of UI access rights created inherits from all of the permissions defined on the Sets of UI access rights you have connected to it.

- its characteristics
- (WET-based desktop) its assigned WET
- (Non WET-based desktop) its accessible desktops and applications

  ☛ *For detailed information on a WET, see **HOPEX Power Studio** - Using a Working Environment Template documentation.*

To create a profile:

1. Access the Profiles management pages.

   ☛ *See Accessing the User Management Pages.*

2. In the **Assignable Profiles** page, click **New**  .

3. In the profile creation window, enter the **Name** of the profile.

   ☛ *By default the **Name** of the profile is created in format "Profile-x" (x is a number that increases automatically).*

4. In the **Set of UI Access Rights** field, click the arrow and select **Create Set of UI Access Rights**.
5. In the **Name** field, enter a name for the Set of UI access rights of the profile.
6. (Optional, to use one or several Sets of UI access rights already defined)

   Click **Connect** :
   - (Optional) In the search field, enter the character string to be searched for.
   - Click **Find** .
   - In the list, select the Set of UI access rights on which you want to base the Set of UI access rights of your profile.

     ☛ *You can select several Sets of UI access rights.*

     The set of UI access rights you are creating inherits from the permissions defined on all the sets of UI access rights you connected to it.
   - Click **Connect**.
7. Click **OK**.
   The new profile is listed in the **All Profiles** page.
8. Configure the profile characteristics.

   ☛ *See Configuring profile characteristics.*

   `E.g.: in the Characteristics page, set the Assignable parameter to "Yes", connect a Tiles Homepage.`
9. (WET-based desktop) Assign a WET to the profile.

   ☛ *See Assigning a WET to a profile.*
10. (Non WET-based desktop) Define:
    - the accessible desktop(s)

      ☛ *See Defining the application desktops accessible to the users of a profile (non WET-based configuration).*
    - the available applications

      ☛ *See Defining the applications accessible to the users of a profile (non WET-based configuration).*

    `E.g.: "The Web Front-End for a Web application.`
11. (If needed) Define the Set of UI access rights of the profile.

    ☛ *See Managing UI Access (Permissions).*

Configuring a Profile

From the profile properties window you can define:

☛ *See Profile Properties.*

- products accessible to users with the current profile.

  ☛ *See step 2.*

- if the profile is assignable or not.

  ☛ *See step 3.*

- if the profile is an administrator profile or not.

  ☛ *See step 4.*

- if the profile is provided at connection.

  ☛ *See step 5.*

- if the profile is active or not.

  ☛ *See step 6.*

- a default report on the homepage associated with the profile.

  ☛ *See step 7.*

- the profile display name in the interface.

  ☛ *See step 8.*

- the profile icon in the interface.

  ☛ *See step 9.*

- the ***Working Environment template (WET)***, which defines the desktops to which the users of the profile have access.

  ☛ *See Assigning a WET to a profile.*

  Or in a non WET-based configuration:

  - applications accessible to the users of the profile.

    ☛ *See Defining the applications accessible to the users of a profile (non WET-based configuration).*

  - (If needed) desktops accessible to the users of the profile.

    ☛ *See Defining the application desktops accessible to the users of a profile (non WET-based configuration).*

- ***reports***:
  - the display level of reports displayed in an object property pages

    ☛ *See Defining the report display level (property pages of an object).*

  - the display order of the report folders displayed in an object property pages

    ☛ *See Modifying the report folder display order (property page of an object).*

  - the default report displayed on the homepage

    ☛ *See Defining a default report on the homepage.*

- the terminology associated with the profile.

  ☛ *See Associating a terminology with a profile.*

- object types available.

  ☛ *See Defining the object types available for a profile.*

You can also:

- customize profile UI access
  - ☛ *see Customizing the UI Access (Permissions) of an Existing Profile.*
- perform a mass profile assignment to persons
  - ☛ *See Performing a Mass Profile Assignment to Persons or Performing a mass assignment of profiles to person groups.*
- check that the profile complies with the connection regulation
  - ☛ *See Checking Profile Compliance with Connection Regulation.*

Configuring profile characteristics

To configure profile characteristics:

1. Access the properties of the profile.
   - ☛ *See Viewing Profile Characteristics.*
2. (Optional) In the **Command Line** field, enter the command defining products that can be accessed by users with the current profile.
   - ☛ *See Products accessible on the license (Command Line).*
3. (Optional) In the **Assignable** field, modify the attribute value via the drop-down menu.
   - ☛ *By default, the profile is not assignable.*
   - ☛ *See Assignable.*
4. (Optional) In the **Administrator Profile** field, modify the attribute value.
   - ☛ *By default, the profile is not an administrator profile.*
   - ☛ *See Set of UI access rights.*
5. (Optional) In the **Profile Display** field, modify the default behavior of the profile display at connection.
   - ☛ *A profile is provided by default at connection when it is not included in another profile.*
   - ☛ *See Profile display.*
6. (Optional) In the **Profile Status** field, modify the attribute value.
   - ☛ *By default, the profile is active.*
7. (Optional) In the **Homepage Report** field, connect a report to the profile homepage.
   - ☛ *See Defining a default report on the homepage.*
8. (Optional) In the **_GUIName** field, enter the profile name displayed in the interface.
9. (Optional) In the **MetaPicture** field, click the arrow and select **Connect MetaPicture**.
   - In the search field, enter the characters you want to find and click **Find**.
   - In the results list, select the icon and click **Connect**.

Assigning a WET to a profile

☛ *To see the connection diagram, see Connection diagram (with WET).*

☛ *For more details on the WET creation and its use with profiles, see **HOPEX Power Studio - Versatile Desktop - Using a Working Environment Template (WET)**.*

With a WET-based configuration, you must assign a WET to the profile. This WET assignment to the profile enables you to define:

- the (unique) desktop associated with the profile, or
- the desktops associated with the profile.
  The desktop definition is done through a Desktop Manager. Thanks to this Desktop Manager you can, for example, define a desktop display adapted to the device (tablet or computer) used by the user.

  E.g.: the user can connect to HOPEX Explorer application from a tablet or a computer with an adapted desktop display.

For specific purposes you may need to assign several WETs to the profile.

☛ *In a non WET-based desktop configuration, you must define the applications accessible to the profile, see Defining the applications accessible to the users of a profile (non WET-based configuration).*

Assigning a WET to a profile (standard version)

To assign a WET to a profile (standard version):

1. Access the properties of the profile.

   ☛ *See Viewing Profile Characteristics.*
2. Select the **WET Assignments** page.
3. Click **New**  .
4. In the **WET** field, select the Working Environment Template you want to assign to the profile.
5. In the **Assigned WET** field, select the WET you want to assign to the profile.
6. Select the desktop selection mode: **Direct selection**.
7. In the **Assigned Desktop** field, select the desktop you want to assign to the profile.
8. Click **OK**.
   The selected WET is assigned to the profile and its associated desktop is defined.

Assigning a WET to a profile (muti-device version)

To assign a WET to a profile (multi-device version):

1. Access the properties of the profile.

   ☛ *See Viewing Profile Characteristics.*
2. Select the **WET Assignments** page.
3. Click **New**  .
4. In the **Assigned WET** field, select the WET you want to assign to the profile.
5. Select the desktop selection mode: **Selection via Desktop Manager**.

6. Select **Create a Desktop Manager**.

   ☛ *To reuse a Desktop Manager, keep **Reuse existing Desktop Manager** and in the drop-down list select the Desktop Manager.*

7. Click **Next**.
8. (Optional) In the **Name** field, modify the default desktop manager name.

   ☛ *The default name is **<Profile name> / <Assigned WET name> / Desktop Manager**.*

   ☺ *This can be useful if you need to reuse this desktop manager for another WET assignment.*

9. Click **Connect** and connect the device matching the desktops you want to define for the profile.
10. Click **OK**.
    The desktops associated with the **Desktop Manager** are specified.
    You must define each desktop use context.
11. In the desktop list, for each desktop, in the **Device** column, select the device type adapted to the desktop.

    `E.g.: Tablet, Computer`

12. Click **OK**.
    The selected WET is assigned to the profile and its associated desktops are defined with their use context.

    `Example:`

    `When the user connects through a tablet, the tablet matching desktop is loaded.`

    `When the user connects through a computer, the computer matching desktop is loaded.`

Defining the applications accessible to the users of a profile (non WET-based configuration)

☛ *To modify a profile provided by **HOPEX**, you must create a new profile; see Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile.*

So that a user of a profile can connect to an application, you must connect this application to the profile concerned.

☛ *See Connection diagram (without WET).*

All desktops connected to the application are then accessible. To enable access to only certain desktops of the application, see Defining the application desktops accessible to the users of a profile (non WET-based configuration).

To define applications available for a profile:

1. Access the Properties pages of the profile.

   ☛ *See Viewing Profile Characteristics.*

2. Select **Available Applications**.
3. In the toolbar, click **Connect**.
   The application search tool appears.
4. (Optional) In the second field, enter the characters to search for.
5. Click **Find**.
6. In the search results, select the application you want to connect.

7. Click **Connect**.
   The applications are connected to the profile.

Defining the application desktops accessible to the users of a profile (non WET-based configuration)

A user can connect to an application via customized desktops according to actions to be performed.

If an application contains several desktops, you can specifically define application desktops that are accessible to the concerned profile.

☛ *See Restricting access to the desktops of an application.*

To do this, you must connect to the profile:

- the application containing the desktops.

  ☛ *See Defining the applications accessible to the users of a profile (non WET-based configuration).*

- the desktops you want the users of the profile can connect to.

  ☛ *The application desktops that are not connected to the profile are not accessible to users of the profile.*

  ☛ *To modify a profile supplied by **MEGA**, **MEGA** recommends you create a new profile, see Creating a Profile.*

To define application desktops available for a profile:

Prerequisite: The application accessible to users of the profile is defined.

☛ *See Defining the applications accessible to the users of a profile (non WET-based configuration).*

1. Access the Properties pages of the profile.

   ☛ *See Viewing Profile Characteristics.*

2. Select **Available Desktops**.
3. In the toolbar, click **Connect**  .
   The desktop search tool appears.
4. (Optional) In the second field, enter the characters to search for.
5. Click **Find**  .
6. In the search results, select the desktop you want to connect.
7. Click **Connect**.
   The desktops are connected to the profile.

Defining the report display level (property pages of an object)

In an object property pages, the **Reporting** page gives access to the reports of the products accessible by the profile. These reports are sorted by product and topics.

You can display the reports:

- directly at first level

  For example, the reports associated with the main product only.

- sorted in the topic folders
  The folders are displayed by alphabetical order, you can modify their order.

  ☛ *If the folder includes a single report, the latter is displayed at first level (its folder is hidden).*

To define the reports and their display level:

1. Access the Properties pages of the profile.

   ☛ *See Viewing Profile Characteristics.*

2. Select **Reporting Presentation**.
3. In the **Folders of Report Templates** list, click **Connect** .
   The folder of Report Templates search tool appears.
4. (Optional) In the second field, enter the characters to search for.
5. Click **Find** .
   In the search results, select the folder(s) of Report Templates concerned.
6. Click **Connect**.
   The folder(s) of Report Templates selected are listed. By default their **Menu level** value is set to: "Root level".
   In that case, the **Reporting** property page of an object displays the reports (belonging to the selected folders) at first level (sorting folders are hidden).
7. (If you want to display the sorting folders) Access the corresponding folder property pages, and in its **Characteristics** page, set the **Menu level** value to "Sub level".
   the **Reporting** property page of an object displays the sorting folder at first level, and then its reports.

Modifying the report folder display order (property page of an object)

In an object property pages, the **Reporting Presentation** page gives access to the reports of the products accessible by the profile. If these reports are sorted by topic folders, you can modify the folder display order.

To modify the folder display order:

1. Access the Properties pages of the profile.

   ☛ *See Viewing Profile Characteristics.*

2. Select **Reporting Presentation**.
3. In the **Folders of Report Templates** list, click **Reorganize** .
4. Drag and drop the folders to get the required display order.
5. Click **OK**.

Defining a default report on the homepage

You can define a default report on the homepage associated with the profile, for all the users connected with the current profile. Each user can change this report.

To define a default report for the profile:

1. Access the Properties pages of the profile.
   ☛ *See Viewing Profile Characteristics.*
2. In the **Characteristics** page, click the **Homepage report** arrow and select **Connect**.
3. Select the report and click **Connect**.
   The report is linked to the profile desktop homepage.

Associating a terminology with a profile

📖 *A Terminology defines a set of terms used in a specific context instead of the standard term.*

☛ *For information on creating and managing a Terminology, see **HOPEX Power Studio - Renaming HOPEX Concepts**.*

To associate a terminology with a profile:

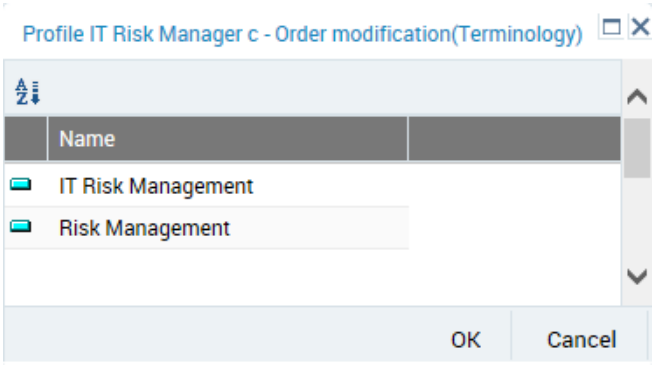
1. Access the Properties pages of the profile.
   ☛ *See Viewing Profile Characteristics.*
2. Select **Terminology**.
3. In the toolbar, click **Connect** 🔗.
   The terminology search tool appears.
4. (Optional) In the second field, enter the characters to search for.
5. Click **Find** 🔍.
6. In the search results, select the terminology you want to connect.
   ☛ *You can select several terminologies.*
7. Click **Connect**.
   The terminology is connected to the profile.

If you associate more than one terminology with the profile, you must define an order of priority for them.

To define the priority of the terminologies of a profile:

1. Access the Properties pages of the profile.
   ☛ *See Viewing Profile Characteristics.*
2. Select **Terminology**.
3. In the toolbar, click **Reorganize**  .

4. Drag and drop to place the priority terminology at the top.



In the example above, the terms of the Risk Management terminology are used when they are not defined in the IT Risk management terminology.

Defining the object types available for a profile

You can define which specific object types are available for a profile:

- document categories
- document models
- Report DataSet Definitions
- widgets

To define the object types available for a profile:

1. Access the properties of the profile.
   ☛ *See Viewing Profile Characteristics.*
2. In the **Available Types** page, select **Available Objects**.
3. In the toolbar, click **Connect** 🔗.
   The object type search tool appears.
4. (Optional) In the search tool, in the first field, select the object type category.
5. (Optional) In the second field, enter the characters to search for.
6. Click **Find** 🔍.
7. In the search result, select the object types to make available for the profile.
8. Click **Connect**.
   The object types selected are made available for the profile.

Checking Profile Compliance with Connection Regulation

A profile must comply with modeling regulation.

To check that the profile complies with the connection regulation:

1. Access the **Profiles** management pages.

   ☛ *See Accessing the User Management Pages.*

2. In the **Profiles** page, right-click the profile concerned and 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) a 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.

  ☛ *To create a repository snapshot, see **HOPEX Common Features - Managing Repository Snapshots** documentation.*

See:

- Assigning a profile to a person
- Performing a Mass Profile Assignment to Persons
- Mass assignment of profiles to persons

Assigning a profile to a person

☛ *To assign one or more profiles to one or more persons at a time, see Mass assignment of profiles to persons*

☛ *To assign a profile to a person from the user management page, see Mass assignment of profiles to persons).*

To assign a profile to a person:

1. Access the properties of the person.

   ☛ *See Viewing the Person Characteristics.*

2. In **Assignments**, click **Profile Assignments**.
3. Click **New** .

4. In the **Profile assigned** field, click the drop-down menu and select the profile you want to assign to the person.

   ☛ *To execute a filtered query on a profile, click the arrow and select **Query**.*
5. (If needed) In the **Repository** field, click the drop-down menu and change the repository to which you want to assign the profile.

   ☛ *By default, the current repository is selected. You can select another repository or all the repositories.*
6. (Optional, with read-only data access) In the **Connection Snapshot** field, select a connection repository snapshot.
7. (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.
8. Click **OK**.
   The profile is assigned to the person on the selected repository for the specified duration.

Performing a Mass Profile Assignment to Persons

☛ *To perform a mass profile assignment with a validity date to persons, see Mass assignment of profiles to persons.*

To perform a mass profile assignment to persons:

1. Access the user management pages and select the **Persons by Profile** sub-folder.

   ☛ *See Accessing the User Management Pages.*
2. In the edit area, select the profile you want to connect to persons.
3. In the edit area, click **Connect** 🔗.
4. In the **Repository** field, select the repository concerned by the assignment.
5. (optional, to define a validity date) Click **Define validity dates**.
   - (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.
6. Select the persons to whom you want to assign the profile.
7. Click **OK**.
   The selected profile is assigned to the selected persons, on the selected repository, for the defined period.

Mass assignment of profiles to persons

To perform a mass assignment of profiles to persons:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*
2. Select the **Persons** sub-folder.
   The list of persons appears.
3. Select the persons to whom you want to assign one or more profiles.

4. Click **Assign Profiles**.
   The list of profiles appears.
5. In the **Repository** field, select the repository concerned by the assignment.
6. 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 and select a validity start date.
   - In the **Validity end date** field, click the calendar and select a validity end date.
7. Select the profiles that you want to assign to the selected persons.
8. 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 who belongs 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 a mass profile assignment to person groups
- Performing a mass assignment of profiles 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 Person Group Characteristics.*

2. In **Assignments**, click **New**  .
3. In the **Assigned profile** field, click the drop-down menu and select the profile you want to assign to the person group.
4. (If needed) In the **Repository** field, click the drop-down menu and change the repository to which you want to assign the profile.

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

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 **Valid start date** field, click the calendar and select a validity start date.
   - In the **Valid end date** field, click the calendar and select a validity end date.
7. Click **OK**.
   The profile is assigned to the person group on the selected repository for the specified duration.

Performing a mass profile assignment to person groups

To perform a mass profile assignment to person groups:

1. Access the **User Management** pages.
   ☛ *See Accessing the User Management Pages.*
2. Click the **Person groups by profile** sub-folder.
   The list of profiles appears.
3. In the edit area, select the profile you want to assign to several person groups.
4. In the edit area, click **Connect** 🔗.
5. In the **Repository** field, select the repository to which the profile is assigned.
   ☛ *You can select one repository or all of them.*
6. (Optional) By default, assignments do not have a validity limit. If you must define a validity period for assignments, select **Define validity dates**.
   - In the **Valid start date** field, click the calendar and select a validity start date.
   - In the **Valid end date** field, click the calendar and select a validity end date.
7. In the person group list, select the person groups to whom you want to assign the profile.
8. Click **OK**.
   The selected profile is assigned to the selected person groups, on the selected repository, for the defined period.

Performing a mass assignment of profiles to person groups

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

1. Access the **User Management** pages.
   ☛ *See Accessing the User Management Pages.*
2. Click the **Person Groups** sub-folder.
   The list of person groups appears.
3. Select the person groups to which you want to assign one or more profiles.
4. Click **Assign Profiles**.
   The list of profiles appears.

5. (If needed) In the **Repository** field, click the drop-down menu and change the repository to which you want to assign the profile.

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

6. By default, assignments do not have a validity limit. If you must define a validity period for assignments, select **Define validity dates**.
   - In the **Valid start date** field, click the calendar and select a validity start date.
   - In the **Valid end date** field, click the calendar and select a validity end date.
7. Select the profiles that you want to assign to the selected person groups.
8. Click **OK**.
   The selected profiles are assigned to the person groups selected for the defined period.

Deleting a Profile

If you delete a profile that is the only profile assigned to a person, this person can no longer connect to HOPEX.

To delete a **Profile**:

1. Access the **Profiles** management pages.

   ☛ *See Accessing the User Management Pages.*

2. In the **Profiles** tab, select the profile you want to delete.

   ☛ *You can select more than one.*

3. Click **Remove** .
   The **Deleting objects** window opens.
4. Click **Delete**.
   The profile is deleted from the environment

ACCESS TO USER MANAGEMENT

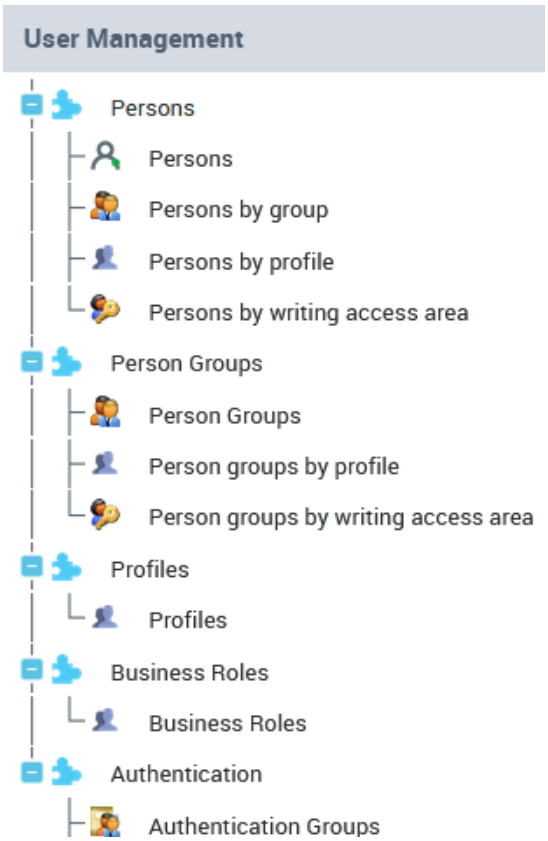
See:

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

Accessing the User Management Pages

To manage users from the **Web Administration** desktop:

1. Connect to the **HOPEX Administration** desktop.
   ☛ *See Connecting to the Administration Desktop.*
2. In the **Administration** tab, click the **User Management** pane.
   The user management tree appears.



3. In the user management tree, click a sub-folder of:
   - **Persons** to manage persons and logins
     ☛ *See Actions performed from the Persons management page.*
   - **Person Groups** to manage the persons who belong to the same person group
     ☛ *See Actions performed from the Person Group page.*
   - **Profiles** to manage profiles
     ☛ *See Managing Profiles.*
     ☛ *See Profile Properties.*
   - **Business Roles** to manage the business roles
     ☛ *See Managing Business Roles.*
   - **Authentication** to manage authentication (e.g.: authentication groups and parameters).
     ☛ *See Configuring SSO Authentication.*

   The management page selected appears.

See:

- Managing persons who have an identical characteristic
- Managing a group of persons who have a specific characteristic
- Actions performed from the Persons management page
- Actions performed from the Person Group page

Managing persons who have an identical characteristic

To manage persons who have an identical characteristic, see:

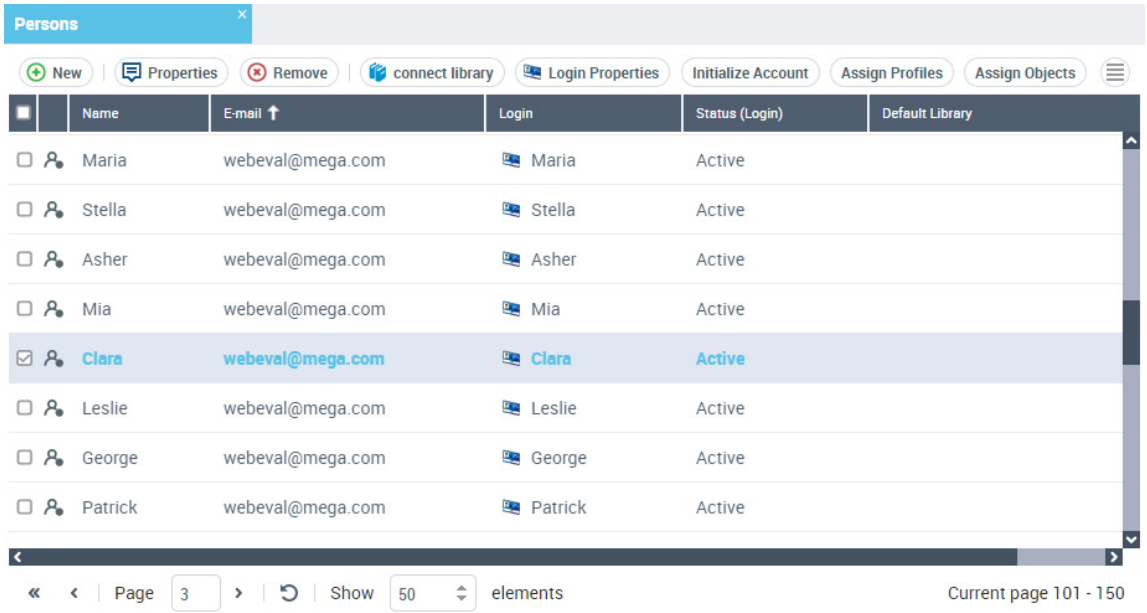
- Accessing the list of persons who have the same profile assigned
- Accessing the list of person who belong to the same group
- Accessing the list of persons connected to a specific writing access area
- Accessing the list of persons connected to a specific reading access area
- Accessing the list of persons who have or do not have a login

Managing a group of persons who have a specific characteristic

To manage persons who have a specific characteristic, see:

- Accessing a group of persons connected to a specific profile
- 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 from the Persons management page



From the **Persons** management page you can:

- create users
  - ☛ *See Creating a User.*
- create logins
  - ☛ *See Creating the Login of a Person.*
- access a person using his/her name
  - ☛ *Accessing a person using his/her name*
- configure the characteristics of a person
  - ☛ *See Defining a Person.*
- check the configuration of a person
  - ☛ *See Checking the Configuration of Users.*
- configure the characteristics of a login
  - ☛ *See Defining the Login of a Person.*
- delete users
  - ☛ *See Deleting a User.*
- modify the properties of users
  - ☛ *See Modifying User Properties.*
- assign a profile to a person
  - ☛ *See Assigning a profile to a person and Mass assignment of profiles to persons.*
- assign an object to a person
  - ☛ *See Assigning an object to a person and Mass assignment of objects to persons.*
- transfer the responsibilities of a person
  - ☛ *See Transferring Responsibilities to a Person.*
- duplicate the responsibilities of a person
  - ☛ *See Duplicate the Responsibilities of a Person.*
- initialize and manage the password of a Web user
  - ☛ *See Managing the Password of a Web User.*
- connect a person to a writing access area
  - ☛ *See Connecting a Person to a Writing Access Area.*
- connect a person to a reading access area
  - ☛ *See Connecting a Person to a Reading Access Area.*
- access user options
  - ☛ *See Modifying options at user level.*
- filter persons
  - ☛ *See Accessing the list of persons who have or do not have a login or Accessing a person using his/her name.*

Actions performed from the Person Group page

From the **Person Group** management page you can:

- create user groups
  - ☛ *See Creating a Person Group.*
- define the properties 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 with a writing access area
  - ☛ *See Connecting a Person Group to a Writing Access Area.*
- connect a person group with a reading area access
  - ☛ *See Connecting a Person Group to a Reading Access Area.*
- define a person group
  - ☛ *See Deleting a Person Group.*
- modify user group properties
  - ☛ *See Modifying a User Group Properties.*

Accessing the list of persons who have the same profile assigned

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

To access the list of persons who have the same profile assigned:

1. Access the user management page.
   - ☛ *See Accessing the User Management Pages.*
2. Select the **Persons by profile** sub-folder.
3. In the edit area, in the **Persons by profile** tab, select a profile.
   The **Persons** tab lists all the persons who have the selected profile assigned.
   - ☛ *See Actions performed from the Persons management page.*

Accessing the list of person who belong to the same group

You can list and manage all persons who belong to a specific group.

To access the list of person who belong to the same group:

1. Access the user management page.
   - ☛ *See Accessing the User Management Pages.*
2. Select the **Persons by group** sub-folder.
3. In the edit area, in the **Persons by group** tab, select a person group.
   The **Persons** tab lists all the persons who belong to the selected group.
   In the case of SSO groups or groups calculated by macros, the list of persons can be long. Click **Calculated** to display, in the **Persons** tab, the list of person who are part of the group selected.
   - ☛ *See Actions performed from the Person Group page.*

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

When several writing access areas are defined, you can list and manage all the persons and all the objects connected to a specific writing access area.

To access the list of persons and objects connected to a specific writing access area:

1. Access the user management page.
   ☛ *See Accessing the User Management Pages.*
2. Select the **Persons by writing access area** sub-folder.
3. In the edit area, in the **Persons by writing access area** tab, select a writing access area.
4. In the edit area, in the **Persons and objects** tab, click:
   - **Persons** to list all the persons who are connected to the selected writing access area.
   - **Objects** to list all the objects that are connected to the selected writing access area.

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

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

When management of reading access areas is activated, you can list and manage all the persons and all the objects connected to a specific reading access area.

To access the list of persons and objects connected to a specific reading access area:

1. Access the user management page.
   ☛ *See Accessing the User Management Pages.*
2. Select the **Persons by reading access area** sub-folder.
3. In the edit area, in the **Persons by reading access area** tab, select a writing access area.
4. In the edit area, in the **Persons and objects** tab, click:
   - **Persons** to list all the persons who are associated with the selected reading access area.
   - **Objects** to list all the objects connected to the selected reading access area.

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

Accessing the list of persons who have or do not have a login

You can filter persons according to their login.

To display the persons who have or do not have a login:

1. Access the user management page.
   ☛ *See Accessing the User Management Pages.*
2. Select a **Persons** sub-folder.
3. In the edit area, click **Display filters** .
   Fields appear under the header of each column.

4. In the **Login** column field, click the filtering operator and select:
   - **Shows non empty values only**
   The persons who have a login are listed.
   - **Shows empty values only**
   The persons who do not have a login are listed.

Accessing a person using his/her name

You can filter persons according to their name.

To find a person using his/her name:

1. Access the user management page.
   ☛ *See Accessing the User Management Pages.*
2. Select a **Persons** sub-folder.
3. In the edit area, click **Display filters**.
   Fields appear under the header of each column.
4. In the **Name** column field, enter the name (or a part of the name) of the person queried.
   The persons with the queried name (the string) appear.

Accessing a group of persons connected to a specific profile

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

1. Access the user management page.
   ☛ *See Accessing the User Management Pages.*
2. Select the **Person groups by profile** sub-folder.
3. In the edit area, in the **Person groups by profile** tab, select a profile.
   The **Person Groups** tab lists the person groups to which the selected profile is assigned.
   ☛ *See Actions performed from the Person Group page.*

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

When several writing access areas are defined, you can list and manage all the person groups and all the objects connected to a specific writing access area.

To access the list of person groups and objects connected to a specific writing access area:

1. Access the user management page.
   ☛ *See Accessing the User Management Pages.*
2. Select the **Person groups by writing access area** sub-folder.
3. In the edit area, in the **Person groups by writing access area** tab, select a writing access area.

4. In the edit area, in the **Person groups and objects** tab, click:
   - **Person Groups** to list all the person groups connected to the selected writing access area.
   - **Objects** to list all the objects that are connected to the selected writing access area.

☛ *See Actions performed from the Person Group page.*

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

When management of reading access areas is activated, you can list and manage the person groups and the objects connected to a specific reading access area.

To access the list of person groups and objects connected to a specific reading access area:

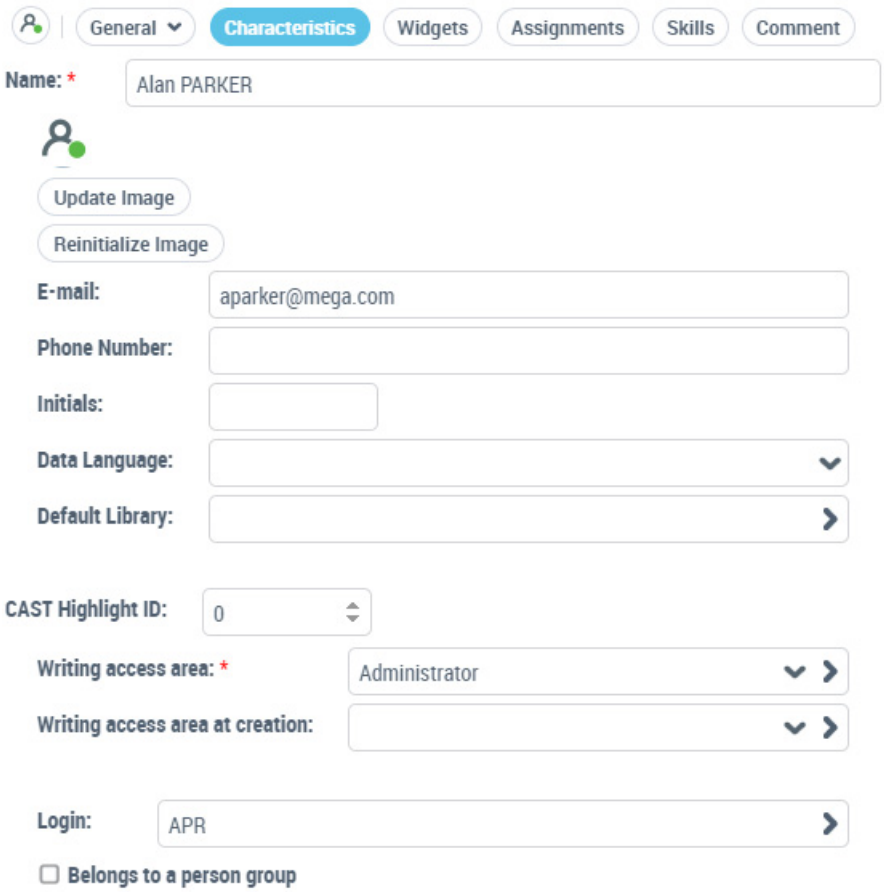
1. Access the user management page.

☛ *See Accessing the User Management Pages.*

2. Select the **Person groups by reading access area** sub-folder.
3. In the edit area, in the **Person groups by reading access area** tab, select a reading access area.
4. In the edit area, in the **Person groups and objects** tab, click:
   - **Person Groups** to list all the person groups connected to the selected reading access area.
   - **Objects** to list all the objects connected to the selected reading access area.

☛ *See Actions performed from the Person Group page.*

Viewing the Person Characteristics



The icon for a person is represented by:

- 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 configured 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 (or Performing a Mass Profile Assignment to Persons).*

To view the person characteristics:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Select:
   - the **Persons** sub-folder for a direct access, or
   - a classification sub-folder (**Persons by group**, **Persons by profile**, **Persons by writing access area**, or **Persons by reading access area**), then in the edit area select the **Group**, the **Profile**, the **Writing access area** or the **Reading access area** concerned.

   The list of persons appears, with for each person, the corresponding login and e-mail (if specified).

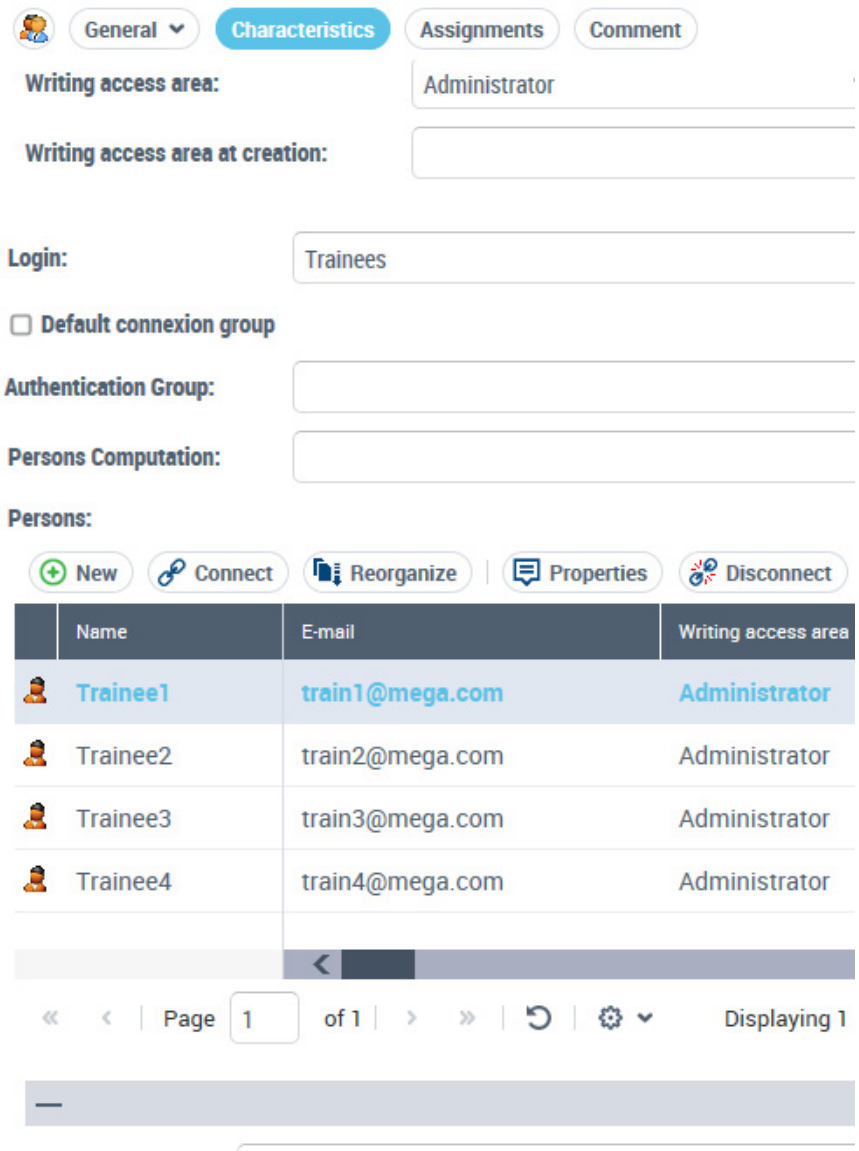
   ☛ *You can sort or filter the display according to columns. See Accessing the list of persons who have or do not have a login and Accessing a person using his/her name.*

   ☛ *You can modify the e-mail and the login of a person directly in this page (with a click in the corresponding field).*
3. In the Persons list, select the person.
4. In the toolbar, click **Properties**  .
   The **Properties** pages of the person are displayed.
5. Click:
   - **Characteristics** to display the person properties.

     ☛ *See Person Properties.*

     ☛ *See Defining a Person.*
   - **Assignments** to display the profiles and object responsibilities (via business roles) of the person.
6. To display the history of actions performed on the person: in the Persons list, right-click the person and select **History**.

Viewing the Person Group Characteristics



To view the person group characteristics:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Select:
   - the **Person Groups** sub-folder for direct access, or
   - a classification sub-folder (**Person groups by profile**, **Person groups by writing access area**, or **Person groups by reading**

access area), then in the edit area select the **Profile**, the **Writing access area** or the **Reading access area** concerned.

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

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

☛ *You can connect an SSO group or a macro to the group in this page (with a click in the corresponding field).*

3. In the person group list, select a person group.
4. In the toolbar, click **Properties** .
   The **Properties** pages of the person group are displayed.
5. Click:
   - **Characteristics** to display the person group properties.

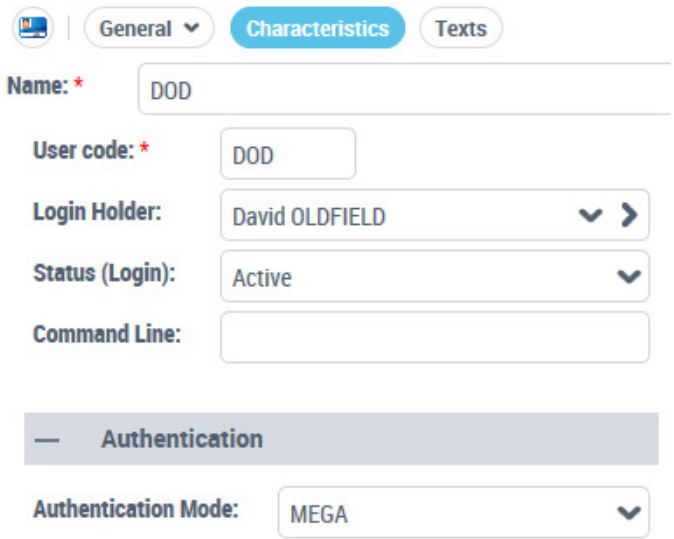
     ☛ *See Person Group Properties.*

     ☛ *See Defining a Person Group, Defining a dynamic person group (SSO), Defining a dynamic person group with a Macro.*
   - **Assignments** to display the profiles assigned to the person group.
6. To display the history of actions performed on the person group: in the Person Groups list, right-click the person group and select **History**.

Viewing the Login Characteristics

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

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



To view the login characteristics:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Select the **Persons** or **Person Groups** sub-folder.
3. In the Persons list, select the person concerned and 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 User Properties
  - 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 User Connection
  - Deleting a User
  - Creating and Managing a Person Group
  - Managing User Options

For information on managing business roles for persons, see:

- Assigning a Business Role to a Person
- Transferring Responsibilities to a Person
- Duplicate the 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 Specifying SMTP Configuration). 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 following 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.*

You can create the person as follows:

- not predefined
  > ☛ *See Creating a User.*
- predefined with one of the following criteria:
  - a person group
  - a profile
  - a writing access area
  - a reading access area (if reading access management is activated)

  > ☛ *See Creating predefined users.*

To complete the configuration of the person, see Defining a Person.

Creating a User

To create a user:

1. Access the **User Management** pages.
   > ☛ *See Accessing the User Management Pages.*
2. Select the **Persons** sub-folder.
3. In the edit area, click **New** ✚.
   The **Creation of Person - Characteristics** window opens.
4. In the **Name** field, enter the name of the person.

   `E.g.: WOODS William`
   > ☛ *Remember to use the same format for all persons.*
5. In the **E-mail** field, enter the e-mail address of the person.

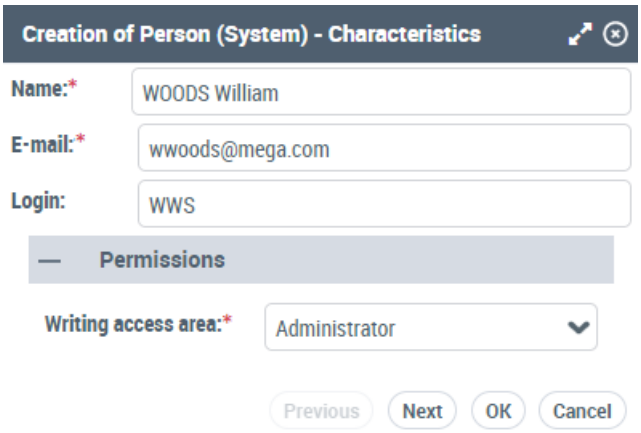
6. In the **Login** field, enter a login.

   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**.*



   ☛ *If **HOPEX** SMTP settings are not configured (See Specifying SMTP Configuration) in the **Password** field, enter a temporary password.*

7. (With the **HOPEX Power Supervisor** technical module) In the **Writing Access Area** field, use the drop-down menu to select the value of the writing access area 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".*

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

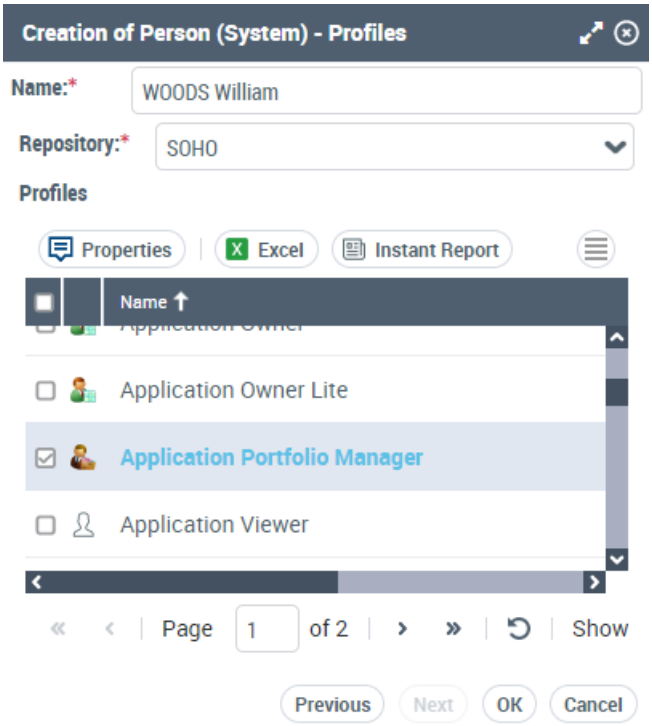
9. Click **Next**.
   The **Creation of Person - profiles** window opens.

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

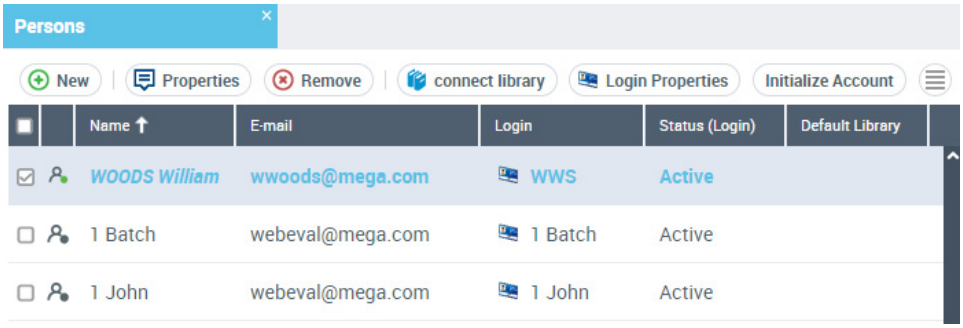
11. Select the profile you want to assign to the person.

    ☛ *You can assign several profiles to the person.*

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



12. 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 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.*

Creating predefined users

To facilitate creation of users with a similar characteristic you can predefine their creation with:

- **group** to create a person automatically connected to the group selected.
- **profile** to create a person and automatically assign this person the profile selected.
- **writing access area** (if several writing access areas are available) to create a person automatically connected to the writing access area selected.
- **reading access area** (if reading access management is activated) to create a person automatically connected to the reading access area selected.

To create a user with a predefined characteristic:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Click the sub-folder corresponding to the characteristic (**Persons by group**, **Persons by profile**, **Persons by writing access area**, or **Persons by reading access area**).

   E.g.: **Persons by profile**.

3. In the edit area, select the characteristic (the group, the profile, the writing access area, or the reading access area) that you want to connect to the person.

   E.g.: **Financial Controller** profile.

4. Click **New** ✚.
   The **Creation of Person - Characteristics** window opens.
5. In the **Name** field, enter the name of the person.

   E.g.: CHANOUX Lou

   ☛ *Remember to use the same format for all persons.*

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

   E.g.: LCX

   ☛ *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.*

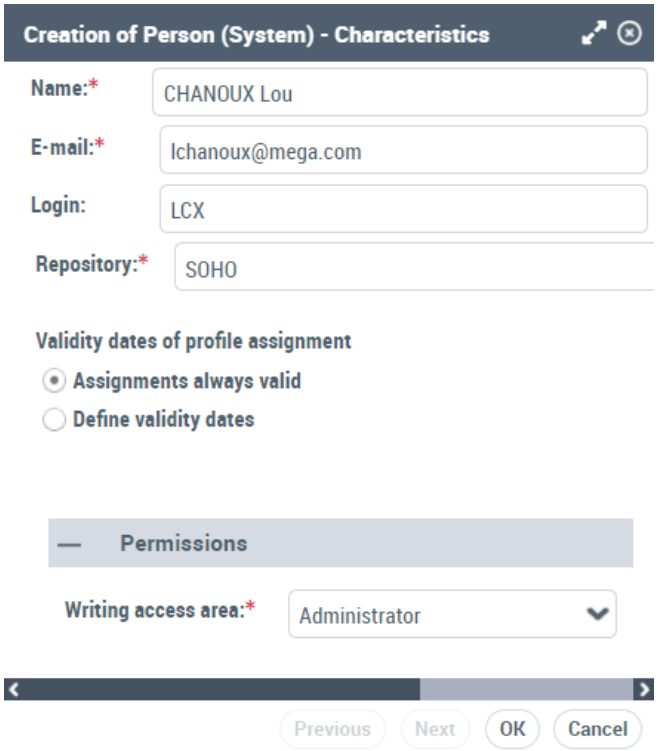
   ☛ *A **Person** can have only one **Login**.*

8. In the **Repository** field, select the repository in which you want to assign the profile to the person.
9. (If needed) Define validity dates for the profile assignment.
10. (With the **HOPEX Power Supervisor** technical module) Using the drop-down menu in the **Writing Access Area** field, select the value of the writing access area 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".*

11. (If required, with the **HOPEX Power Supervisor** technical module) Using the drop-down menu in the **Reading Access Area** field, select the value of the reading access area 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.*



12. 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 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.*

Defining a Person

> 🕮 ***Person*** *represents a physical person or a system.*
>
> ☛ *For more information on properties of a person, see Person Properties.*
>
> ☛ *To check the configuration of a person, see Checking the Configuration of Users.*
>
> ☛ *To assign:*
>
> *a profile to a person (mandatory), see Assigning a Profile to a Person.*
>
> *an object to a person (if needed), see Assigning a Business Role to a Person.*

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

- name of the person
- image of the person
- e-mail address of the person
- phone number and initials of the person
- data language of the Web user
- default library to store objects created by the person
- 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

  For information regarding reading access management, see HOPEX Administration > Managing data reading access documentation
- the login of the person
- if the person belongs to a person group.

To define a **Person**:

1. Access the properties of the person.

   ☛ *See Viewing the Person Characteristics.*
2. (Optional) To add or update the image of the person, click **Update Image**, select the image and click **OK**.

   ☛ *The image is stored in binary on an attribute of the person. To delete the image, click **Reinitialize Image**.*
3. (Recommended) In the **E-mail** field, enter 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 Web password.*
4. (Optional) Enter the **Phone Number** and the **Initials** of the person.
5. (Optional) In the **Data Language** field, using the drop-down menu, you can define a specific data language for this user.

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

   ☛ *See Managing Languages in Web Applications.*

6. (Optional) In the **Default Library** field, click the arrow and select the default library in which objects created by the user are stored if the creation context does not define one.
7. (Optional, with the **HOPEX Power Supervisor** technical module) You can modify the values at the following levels:
   - user writing access via the drop-down menu in the **Writing Access Area** field.

     ☛ *By default, all users are connected to the only writing access area that exists: "Administrator".*

     ☛ *See also Connecting a Person to a Writing Access Area.*
   - user writing access at creation via the drop-down menu in the **Writing Access Area** field.
   - reading access via the drop-down menu in the **Reading Access Area** field.

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

     ☛ *See also Connecting a Person to a Reading Access Area.*
   - reading access at creation via the drop-down menu in the **Writing Access Area** field.

     ☛ *This field only appears if reading access management has been activated.*
8. So that the person can connect to **HOPEX**, the person must have a **Login**.

   ☛ *See Creating the Login of a Person.*
9. (optional) If necessary select **Belongs to a Person Group**
   The person is configured.

   ☛ *To notify the users connected of your changes, click **Notify Connected Users**.*

Creating the Login of a Person

To connect to **HOPEX**, a person must have a Login.

When you create a person from:

- the Web administration desktop, the login of the person is automatically created.
  This person can connect to **HOPEX**.
- other desktops, for example to add the person to an organization chart, this person's login is not created automatically.
  So that the person can connect to **HOPEX**, you must create a login for the person.

To create the login of a person:

1. Access the properties of the person.

   ☛ *See Viewing the Person Characteristics.*
2. In the **Login** field, click the arrow and select **Create Login**.
   The **Creation of Login** window opens. The name of the login is already entered with the name of the login holder.

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

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

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

   E.g.: GDS

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

   E.g.: GDS.

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

   ☛ *If **HOPEX** SMTP settings are not configured (See Specifying SMTP Configuration), the **E-mail** field is changed for **Password**, enter a temporary password.*

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

Defining the Login of a Person

From the login Property pages, 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 the short identifier (upper case) of the user. It serves as a basis for naming user private workspaces.*
- 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. In the login Properties pages, display **Characteristics**.

   ☛ *See Viewing the Login Characteristics.*

   - 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. (Optional) Modify the **Status (Login)** field value, which defines if the user is active or not.

   ☛ *See Status (Login).*

3. (Optional) 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 determine 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 User Properties

You can modify user properties. For each user you can modify properties of:

- person:
  - its name
  - image
  - e-mail address
  - telephone number
  - initials
  - data language
  - default library
  - writing access area
  - reading access area
  - group
  - profile assignments (connection)
  - object assignments (business roles)
  - skills

    ☛ *See Person Properties.*

    ☛ *See Viewing the Person Characteristics.*

    ☛ *See Defining a Person.*
- login:
  - its name
  - user code

    To assure consistent actions history, the user code should not be modified.
  - its status
  - accessible products (Command Line)
  - authentication mode

    ☛ *See Login Properties (Person).*

    ☛ *See Viewing the Login Characteristics.*

    ☛ *See Defining the Login of a Person.*

Connecting a Person to a Writing Access Area

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

☛ *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 **User Management** pages.

   ☛ *See Accessing the User Management Pages.*
2. Select the **Persons by reading access area** sub-folder.
3. In the edit area, select a writing access area.

4. Click **Connect** .

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

5. (Optional) In the query field, enter the characters to search for.
6. Click **Find** .
7. In the result list, select the person you want to connect.
8. Click **Connect**.
   The selected person is connected to the selected 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 **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Select the **Persons by reading access area** sub-folder.
3. In the edit area, select a reading access area.
4. Click **Connect** .

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

5. (Optional) In the query field, enter the characters to search for.
6. Click **Find** .
7. In the result list, select the person you want to connect.
8. Click **Connect**.
   The selected person is connected to the selected reading access area.

Preventing User Connection

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

To make a user inactive:

1. In the login property pages of the user concerned, display **Characteristics**.

   ☛ *See Viewing the Login Characteristics.*

2. In the **Status (Login)** field, select "Inactive".
   The user can no longer connect to **HOPEX**.

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 User Connection.

To delete a user:

1. Access the user management page.

   See Accessing the User Management Pages.

2. In **Persons**, select the person to be deleted and click **Delete** .

   You can select more than one.

   The **Deleting objects** window opens: the person and corresponding login and assignments are selected.

3. Click **Delete** to confirm 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
- management:
  - Preventing 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 Person group types.
- 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 **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. You can create:
   - either a non-predefined person group:

   Select the **Person Groups** sub-folder and go to step 4.
   - or a predefined person group:

   Select the sub-folder:

   Person groups by profile *to create a person group automatically connected to the profile that you are going to select.*

   Person groups by writing access area *(available if several writing access areas are available) to create a person group automatically connected to the writing access area that you are going to select.*

   Person groups by reading access area *(available if reading access management is activated) to create a person group automatically connected to the reading access area that you are going to select.*
3. In the edit area, select the profile, the writing access area or the reading access area that you want to connect to the group.
4. Click **New** .

   The **Creation of Person Group - Characteristics** window opens.
5. In the **Name** field, enter the name of the person group.

   `Example: Marketing.`
6. (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.*
7. (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.*
8. Click **OK**.

   The person group is created and listed in the **Person Group** tab.

   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 types of person groups, see Person group types.

A person group can be created:

- statically
  - ☛ *See Adding persons to a static person group.*
- dynamically
  - ☛ *See Defining a dynamic person group (SSO).*
  - ☛ *see Defining a dynamic person group with a Macro.*

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 with access to a reading area
  - ☛ *See Connecting a Person Group to a Reading Access Area.*
- connect the person group with access 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 person group
  - ☛ *See Modifying a User Group Properties.*

Adding persons to a static person group

Case of a person group created statically.

To connect one or more persons to a **Person Group**:

1. Access the property pages of the person group you want to configure.
   - ☛ *See Viewing the Person Group Characteristics.*
2. Select **Characteristics**.
3. In the **Persons** pane, click **Connect** 🔗.
   - ☛ *To add a person not yet created, click **New** ➕, see Creating a User.*
4. (Optional) In the query field, enter the characters to search for.
5. Click **Find** 🔍.
6. In the result list, select the persons you want to connect.
   These persons must have a login.
   - 💣 **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.*

7. Click **Connect**.
   The person(s) are connected 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 group users on the fly (see Connection request and user created on the fly).*
>
> ☛ *For information on person group types, see Person group types.*

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 Properties pages of the person group.
   > ☛ *See Viewing the Person Group Characteristics.*
2. Select **Characteristics**.
3. In the **Authentication Group** field, click the arrow and connect the required authentication group.
4. Click **OK**.
   The dynamic person group is configured with SSO.

Defining a dynamic person group with a Macro

> 🕮 *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 group users on the fly (see Connection request and user created on the fly).*
>
> ☛ *For information on person group types, see Person group types.*

The **Computed Persons** attribute enables definition of a macro defining a list of persons connected to this person group. Persons defined by the macro use the configuration defined on the person group.

To define a dynamic **Person Group** with a macro:

1. Access the properties pages of the person group.
   > ☛ *See Viewing the Person Group Characteristics.*
2. Select **Characteristics**.

3. In the **Computed Persons** field, click the arrow and connect the required macro.

   Example of macro with login "sec" belonging to group "dev":

   ```
   Function IsUserExists (omPersonGroup, sLogin)
   IsUserExists = False
   if sLogin = "sec" then
                  IsUserExists = True
   end if
   End Function
   ```

   omPersonGroup represents the person group object executing the query.

   sLogin represents the authentication login of the person.

4. Click **OK**.
   The dynamic person group is configured with a macro.

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 Person group types.*

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 Properties pages of the person group.

   ☛ *See Viewing the Person Group Characteristics.*

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

Connecting a Person Group to a Writing Access Area

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

To connect a person group to a writing access area:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Select the **Person groups by writing access area** sub-folder.
3. In the edit area, select a writing access area.
4. Click **Connect**.

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

5. (Optional) In the query field, enter the characters to search for.
6. Click **Find**.

7. In the result list, select the person group you want to connect.
   ☛ *You can connect several person groups.*
8. Click **OK**.
   The person groups selected are connected to the writing access area selected.

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. Access the **User Management** pages.
   ☛ *See Accessing the User Management Pages.*
2. Select the **Person groups by reading access area** sub-folder.
3. In the edit area, select a reading access area.
4. Click **Connect** .
   ☛ *To add a person group not yet created, click **New** , see Creating a Person Group.*
5. (Optional) In the query field, enter the characters to search for.
6. Click **Find** .
7. In the result list, select the person group you want to connect.
   ☛ *You can connect several person groups.*
8. Click **OK**.
   The person groups selected 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 properties window, 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 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 type group, person group computed by macro, or persons directly connected to the group)
  - persons owned in the group

    See Person Group Properties.

    See Viewing the Person Group Characteristics.

    See Defining a Person Group.

    See Defining a dynamic person group (SSO).

    See Defining a dynamic person group with a Macro.
- login:
  - name and user code
  - status
  - authentication mode

    See Login Properties (Person Group).

    See Viewing the Login Characteristics.

    See Modifying a Person Group Login.

Preventing User Group Connection

When you want to temporarily prevent the persons in a group from connecting in the name of the group, you can disable this person group without deleting it from your repository.

To deactivate a person group:

1. Access the Properties pages of the login in question.
   ☛ *See Viewing the Login Characteristics.*
2. Select **Characteristics**.
3. In the **Status (Login)** field, select "Inactive".
4. Click **Apply**.

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 user management page.
   ☛ *See Accessing the User Management Pages.*
2. In **Person Groups**, select the person group to be deleted and click **Delete** .
   ☛ *You can select more than one.*
   The **Deleting objects** window opens.
3. Click **Delete** to confirm deletion.
   The person group and its login are deleted from the repository.

MANAGING USER OPTIONS

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

See:

- Authorizing Deletion of a Dispatched Object
- Making a Comment Mandatory on Dispatch
- Managing User Inactivity

See also:

- Modifying Password Security Settings

Private Workspace Specific

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 a Comment Mandatory on Dispatch

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 for how long user session time can remain inactive before closing.

☺ *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 the 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 **Options** at the environment level.

   ☛ *See Managing Options.*

2. In the **Options** tree, select **Workspace > Desktop**.
3. In the right pane, enter a value 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.

   When this duration has been reached, the user is disconnected and **HOPEX** closes without warning.

AUTHENTICATION IN HOPEX

Authentication is a process consisting of 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*

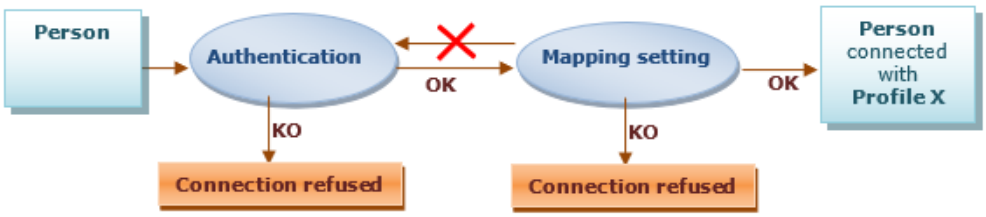
See:

- Authentication and Mapping Principle
- Choosing an authentication mode
- Modifying the HOPEX Authentication Mode
- 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, **MEGA** 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

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, right-click **Authentication groups** folder and select **New > Authentication group**.
   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. Associate an HOPEX person group with the authentication group.

   ☛ *See 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.

The 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.

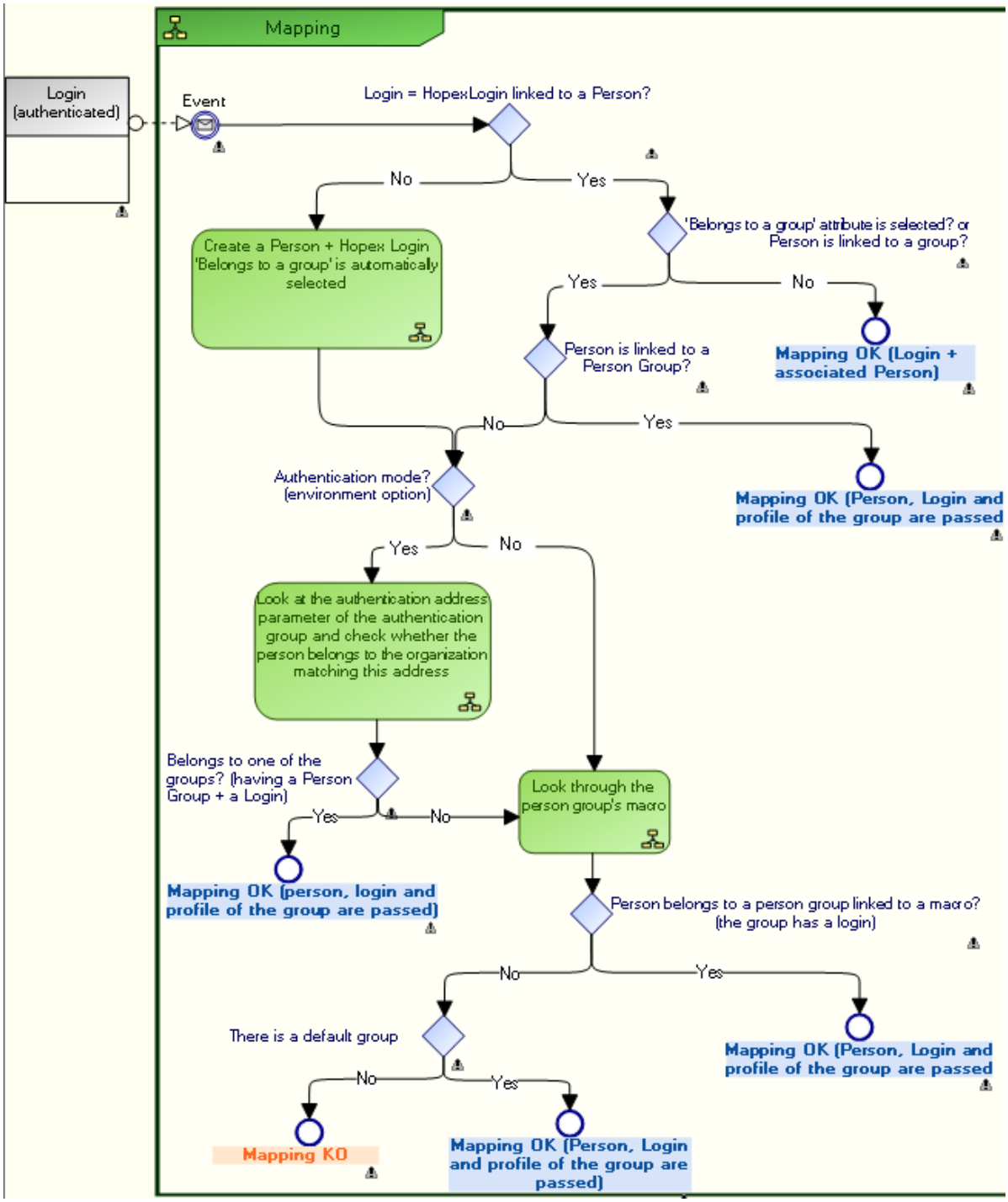
     ☛ *See Defining an SSO Authentication Group.*
   - Map the authentication groups with the person groups defined in HOPEX.

     ☛ *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**.


Mapping
Login (authenticated)
Event
Login = HopexLogin linked to a Person?
No
Yes
'Belongs to a group' attribute is selected? or Person is linked to a group?
Create a Person + Hopex Login 'Belongs to a group' is automatically selected
Yes
No
Person is linked to a Person Group?
Mapping OK (Login + associated Person)
No
Yes
Authentication mode? (environment option)
Mapping OK (Person, Login and profile of the group are passed
Yes
No
Look at the authentication address parameter of the authentication group and check whether the person belongs to the organization matching this address
Belongs to one of the groups? (having a Person Group + a Login)
Yes
No
Look through the person group's macro
Mapping OK (person, login and profile of the group are passed)
Person belongs to a person group linked to a macro? (the group has a login)
No
Yes
There is a default group
Mapping OK (Person, Login and profile of the group are passed
No
Yes
Mapping KO
Mapping OK (Person, Login and profile of the group are passed)

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 the case of SSO authentication, 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 in the name of 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 in the name of 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 in the name of 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 in the name of 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.
- Th 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 in 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 person 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 and select **Connect MetaAttribute**.
9. Perform the search and select the HOPEX MetaAttribute you want to associate with the SSO authentication identifier defined step 7.

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

MANAGING THE PASSWORD OF A WEB USER

When in 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.

Prerequisite:

Before initializing the Web account of a user:

- ensure the e-mail of the person is specified and correct.

  ☛ *See Viewing the Person Characteristics.*

- check that the following options relating to Web applications are specified:
  - Specifying the Web Applications Access Path
  - Specifying SMTP Configuration

  ☛ *These options can be specified at installation, see the **HOPEX Web Front-End Installation Guide** installation document.*

To initialize the Web account of a user:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Select the **Persons** sub-folder.
3. In the Persons list, select the person concerned.
4. Click **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 environment options.

   ☛ *See Modifying options at environment level.*

2. In the options tree, expand the **Installation** folder and 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 an uppercase
  - at least a lowercase
  - at least a special character
  - at least a 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 production 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 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 user management page.
   ☛ *See Accessing the User Management Pages.*
2. Select a **Persons** sub-folder.
3. In the edit area, select the person for whom you want to set a temporary password.
   ☛ *You can select several users. They will all have the same temporary password.*
4. Click **Set Password** 🔑.

5. In the **Password** field, enter the temporary password you want to set for the user.
6. 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 LANGUAGES

Managing the Data Language

The data language is the language with which the user connects by default the first time. If the user changes his/her data language (see Modifying the 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.
  - *See Defining a Person.*
  - *See Viewing the Person Group Characteristics.*

Managing the Interface Language

HOPEX interface is available in six languages: German, English, Spanish, French, Italian, and Portuguese.

The interface language is defined at environment level for all the users.

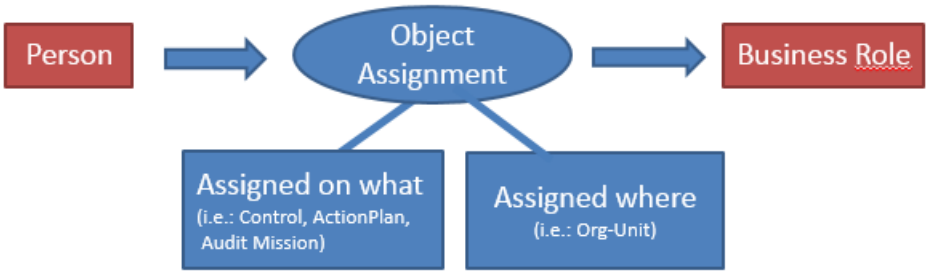
To modify the interface language for all the users:

- See Modifying the Interface Language at Environment Level.

MANAGING BUSINESS ROLES

A business role is used to assign a task to a person (example: a control, an audit mission or an action plan) and where appropriate, for a specific location (example: Paris agency).

Business roles are assigned to persons or person groups. The assignment manages the link between person or person group and business role.



See:

- Business Role Properties
- Creating Business Roles
- Defining a Business Role
- Assigning a Business Role to a Person
- Transferring Responsibilities to a Person
- Duplicate the Responsibilities of a Person
- Deleting a Business Role

Business Role Properties

Name

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

MetaPicture

The **MetaPicture** attribute enables customization of the icon representing the current business role.

_GUIName

The **_GUIName** attribute enables definition of the business role name display in the interface.

Multiplicity

In the **Business Role Definition** page, the **Business Role Multiplicity** defines the number of business role assignments possible for a person.

☛ *A multiplicity business role 1 or 0..1 cannot be assigned to more than one person at the same time.*

Creating Business Roles

Specific business roles are supplied with each Solution.

☛ *See the guides specific to the Solutions.*

To create a business role:

1. Access the user management pages and select the **Business Roles** sub-folder.

   ☛ *See Accessing the User Management Pages.*

2. Click **New** .
   The business role creation window appears.
3. (Optional) In the **Name** field, modify the business role name.

   ☛ *By default the **Name** of the business role is created in format "Business Role-x" (x is a number that increases automatically).*

4. Click **OK**.
   The new business role appears in the list of business roles.

   ☛ *To configure the business role, see Configuring a Business Role.*

   ☛ *To define the business role, see Defining a Business Role.*

Configuring a Business Role

Specific business roles are supplied with each Solution.

To configure a business role:

1. Access the user management pages and select the **Business Roles** sub-folder.

   ☛ *See Accessing the User Management Pages.*

2. Select the business role concerned and click **Properties** .
3. Click **Characteristics**.
4. (Optional) In the **Business Role Status** field, modify the attribute value.

   ☛ *By default, the business role is active.*

5. (Optional) In the **MetaPicture** field, click the arrow and select **Connect MetaPicture**.
   - In the query field, enter the characters you want to find and click **Find**.
   - In the results list, select the icon and click **OK**.
6. (Optional) In the **_GUIName** field, enter the business role name you want to be displayed in the interface.

Defining a Business Role

Defining a business role consists of defining:

- objects assigned to define a task to a person

  E.g.: control, audit mission, action plan.

- localizing objects to define a specific location (in the organization of the company)

  E.g.: USA agency.

  For example, for risk management specific to the country where it is applied.

- optional parameters:
  - multiplicity to define the number of assignments of business roles possible for a person.

    ☛ *A multiplicity business role 1 or 0..1 cannot be assigned to more than one person at the same time.*

  - candidate queries, to filter persons to whom the business role can be assigned.

    ☛ *See Assigning a Business Role to a Person.*

To define a business role:

1. Access the user management pages and select the **Business Roles** sub-folder.

   ☛ *See Accessing the User Management Pages.*

2. Select the business role concerned and click **Properties**.
3. Click **Business Role Definition**.
4. In the **Business Role Multiplicity** field, select the multiplicity for the business role.
5. (optional) In the **Assigned MetaClass** section, click **Connect**.

   You must specify at least one of the two sections, see step 6.

   The MetaClass search tool appears.
   - (Optional) In the second field, enter the characters to search for.
   - Click **Find**.
   - In the search results, select the MetaClass you want to connect.

     ☛ *Use the [Ctrl] key to select several MetaClasses at the same time.*

   - Click **Connect**.

   The MetaClasses are connected to the profile.

6. (optional) In the **Localizing MetaClass** section, click **Connect** .

   You must specify at least one of the two sections, see step 5.

   The MetaClass search tool appears.
   - (Optional) In the second field, enter the characters to search for.
   - Click **Find** .
   - In the search results, select the Localizing MetaClass you want to connect.

     Use the [Ctrl] key to select several Localizing MetaClasses at the same time.
   - Click **Connect**.

   The Localizing MetaClasses are connected to the profile.
7. (optional) In the **Candidates Queries** section, you can filter the persons to whom the business role can be assigned.

   Click **Connect** .

   The query search tool appears.
   - In the second field, enter the characters to search for.
   - Click **Find** .
   - In the query results, select the query you want to connect.
   - Click **Connect**.

   The filtering query is connected to the business role.

   ```
   E.g.: for the "Auditor of an audit mission" business role,
   the "Auditors and lead auditors (profile)" query is used to
   filter the persons who have the "Auditor" or "Lead Auditor"
   profile assigned.
   ```
   - By default, filtering is not offered when assigning the business role to a person; in the **_FavoriteRequest** field of the query, select "Yes" to offer the filtering.
   - Select **Propose all users** to, in addition to the query filtering, assign other persons who are not part of the filtering.

   The business role is defined and can be assigned to persons.

   See Assigning a Business Role to a Person.

Assigning a Business Role to a Person

A business role can be assigned to a person:

- for a specific object

  E.g.: Anne Martin is Process Manager for the Purchasing business process.

  ☛ *See Assigning an object to a person step 5.*

- to a given geographical location

  E.g.: David Oldfield is Risk Manager at London Branch.

  ☛ *See Assigning an object to a person step 6.*

- to a given geographical location for a specific object

  E.g.: Tom Woods is Process Manager for the Purchasing business process at Boston branch.

  ☛ *See Assigning an object to a person steps 5 and 6.*

See:

- Assigning an object to a person
- Mass assignment of objects to persons

Assigning an object to a person

☛ *To assign one or more objects to one or more persons at a time, see Mass assignment of objects to persons*

☛ *To assign an object to a person from the user management page, see Mass assignment of objects to persons.*

To assign an object to a person:

1. Access the properties of the person.

   ☛ *See Viewing the Person Characteristics.*

2. In **Assignments,** click **Object Assignments**.
3. Click **New** .
4. In the **Select a Business Role** field, click the drop-down menu and select the business role concerned.
5. (If necessary) In the **Assigned Object** field, click the arrow and select **Search**.

   ☛ *This field appears only if the selected business role has at least one assigned object, see Defining a Business Role.*

   In the search tool:

   - (if necessary) in the first field, select the object type to find.
   - (optional) in the **Find object** field, enter the characters to search for.
   - Click **Find** .
   - Select the object and click **OK**.

6. (if necessary) In the **Assignment Location** field, click the arrow and select **Connect**.

   ☛ *This field appears only if the selected business role has at least one Localizing MetaClass, see Defining a Business Role.*

   In the search tool,

   - (if necessary) in the first field, select the object type to find.
   - (Optional) in the second field, enter the characters to search for.
   - Click **Find** .
   - Select the object and click **Connect**.

7. Click **OK**.

Mass assignment of objects to persons

To perform a mass assignment of objects to persons:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Select a **Persons** sub-folder.
   The list of persons appears.
3. Select the persons concerned.
4. Click **Assign Objects**.
5. In the list of business roles, select the business role in question.

   ☛ *Only the business roles that can be assigned to more than one person at the same time (cardinality >1) are displayed.*

6. In the **Assigned Object** frame, click **Link** .
7. (Optional) Using the search tool:
   - (If necessary) in the first field, select the object type to find.
   - (Optional) in the second field, enter the characters to search for.
   - Click **Find** .
8. Select the object and click **Connect**.

   ☛ *You can select more than one.*

9. Click **Connect**.

Transferring Responsibilities to a Person

From the **Administration** desktop, you can transfer all or part of user responsibilities 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 Duplicate the Responsibilities of a Person.*

To transfer the responsibilities from one person to another:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Select a **Persons** sub-folder.

3. In the list of persons, select the person for whom you want to transfer the responsibilities and click **Transfer responsibilities**.

   ☛ *You can select more than one person.*

   The responsibilities transfer wizard opens.

4. (If required) Select the person then click **Properties** to view or modify the assignments of the source person.
5. Click **Next**.
6. Click **Connect**.
7. (Optional) In the query wizard, in the second field, enter the character string you want to search for.
8. Click **Find**.
9. Select the person to whom you want to transfer the responsibilities.

   ☛ *You can select more than one person.*

   If you select more than one target user, only the object assignments that can be assigned to more than one person are available.

10. Click **Connect**.
11. Click **Next**.
12. Select the responsibilities you want to transfer.
    - In the **Profile Assignment** frame, select the profiles that you want to transfer to the target user (or to the selected persons).
    - In the **Object Assignments** frame, select the object assignments that you want to transfer.
13. (optional) In the **Validity date of profile assignments** part, you can modify the validity dates defined for the source person. Select:
    - **Assignments always valid** to avoid restricting the validity of assignments.
    - **Define validity dates** (and select the validity start and end dates).
14. Click **OK**.
    The assignments selected are deleted from the source user (or source users) and transferred to the target user (or target users).

Duplicate the Responsibilities of a Person

From the **Administration** desktop, you can duplicate the responsibilities from one user to one or more users.

To duplicate the responsibilities from one person to another:

1. Access the **User Management** pages.

   ☛ *See Accessing the User Management Pages.*

2. Select a **Persons** sub-folder.

3. In the list of persons, select the person for whom you want to duplicate the responsibilities and click **Duplicate responsibilities**.
   - ☛ *You can select more than one person.*
   - ☛ *If the button is hidden, click*  *to access it.*

   The responsibilities duplication wizard opens.
4. (If required) Select the person then click **Properties**  to view or modify the assignments of the source person.
5. Click **Next**.
6. Click **Connect**.
7. (Optional) In the query wizard, in the second field, enter the character string you want to search for.
8. Click **Find**  .
9. Select the person to whom you want to duplicate the responsibilities.
   - ☛ *You can select more than one person.*
   - **Only object assignments that can be assigned to more than one person are available (see the definition of the multiplicity of a business role: Defining a Business Role).**
10. Click **Connect**.
11. Click **Next**.
12. In the **Profile Assignments** frame, select the profiles that you want to assign (duplicate) to the target user (or to the selected persons).
13. In the **Object Assignments** frame, select the assignments that you want to assign (duplicate) to the target user (or to the selected persons).
14. Click **OK**.
    The selected assignments are assigned (duplicated) to the target user (or target users).

Deleting a Business Role

To delete a business role:

1. Access the user management pages and select the **Business Roles** sub-folder.
   - ☛ *See Accessing the User Management Pages.*
2. Select the business role you want to delete.
   - ☛ *You want to select one or more business roles.*
3. Click **Remove**  .
   The business role deletion window appears.
4. Click **Delete**.
   The business role is deleted from the environment.

3

ACCESSES

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

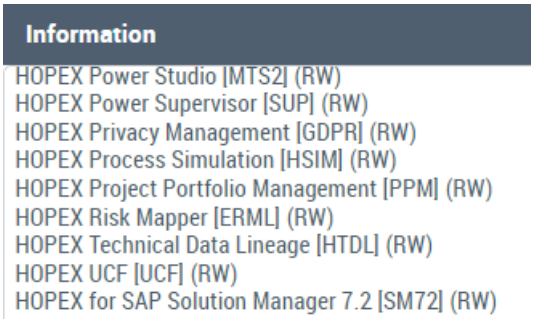
BIG PICTURE: ACCESS MANAGEMENT

Product Access

Product or data accesses are governed by:

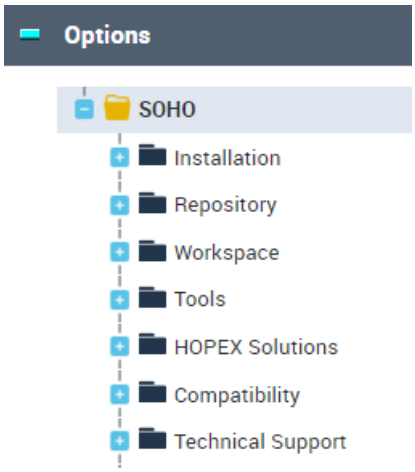
- ***the license file***, which details the available products and their access type (**RW**: Read-Write or **RO**: Read Only)

  ☛ *To access the license file, see Consulting your Licenses.*



- ***the environment options*** for the UI

  ☛ *To access the environment options, see Modifying options at environment level.*



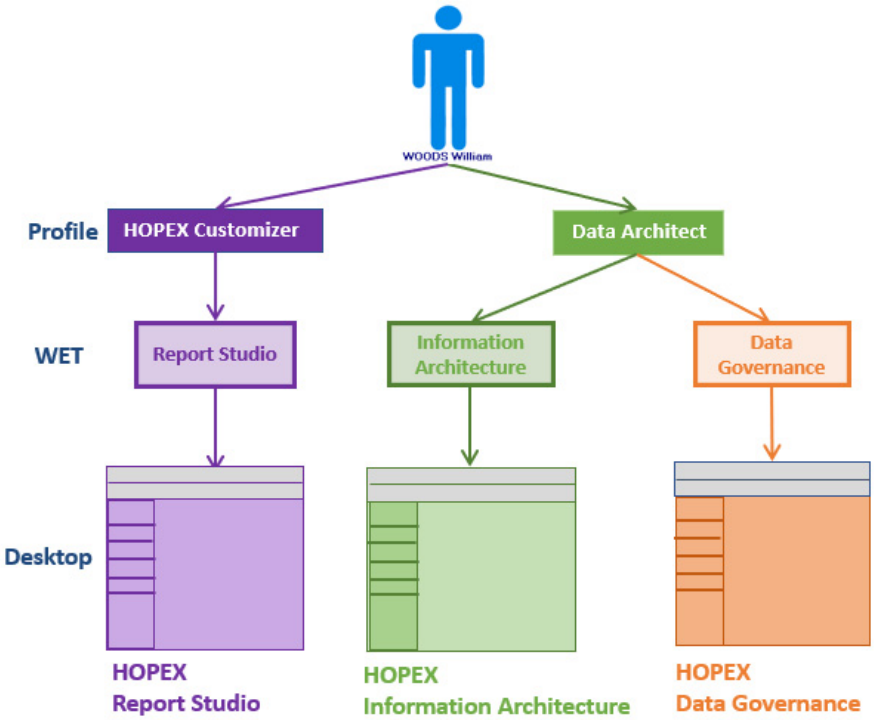
Access Restrictions

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 Create, Reade, Modify, Delete, Search **Permissions**) that is sufficient for the profile
- general UI access (via **Availability**) that is sufficient for the profile
- metamodel or feature access (via the **Profile** options) that is sufficient for the profile
- (optional) dynamic data reading or writing access (via **Data access rules** linked to the profile)

User level

The user properties restrict:

- writing or reading access to specific products (via his/her login **Command Line**, if any)
- metamodel or features access (via the user **Options**)
- static data writing access (via the **Writing access diagram**): the person can modify the objects belonging to his/her writing access area
- (optional) static data reading access (via the **Reading access diagram**): the person has access to the objects belonging to his/her reading access area

Group (used at connexion) level

The group properties restrict:

- specific product writing or reading access (via the 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**.

Options enable in particular to modify the metamodel or features visibility.

- the ***profile*** inherits the option values defined at environment level

  ☛ *To modify the profile options, see Modifying options at profile level.*

- the ***user*** inherits the option values defined at connection profile level

  ☛ *To modify the user options, see Modifying options at user level.*

An ***administrator*** can modify or lock an option at environment level, at profile level, or even at a specific user level.

☛ *To manage user options, see also Managing User Options and Options.*

A ***user*** can modify his/her own options, for example to modify his/her metamodel access or features visibility.

> ☛ *See Options and Extending the Visibility (Metamodel or Advanced Features).*

Customization rule

Customizations at user level (e.g.: data language modification) are also of highest priority, followed in order of priority by those made at profile and environment levels.

MANAGING PRODUCT AND OBJECT ACCESSES

Restricting Product Access 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 a profile access to products, see Products accessible on the license (Command Line).

Example:

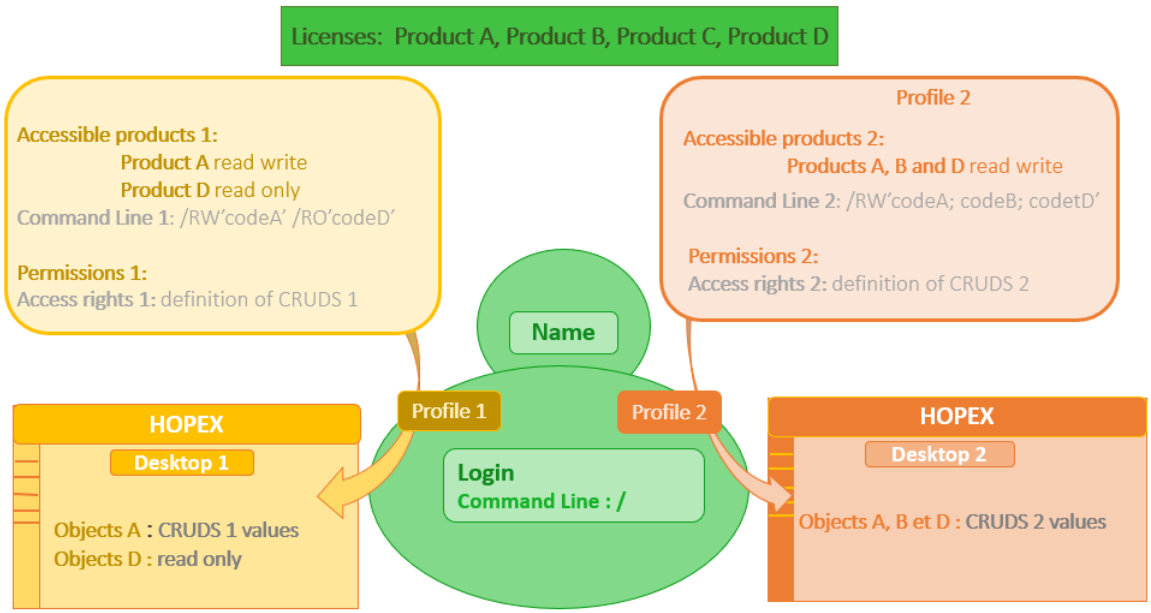
User licenses: Products A, B, C and D.

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 access to product, see Products accessible on the license (Command Line).

Examples:

User licenses: Products A, B, C and D.

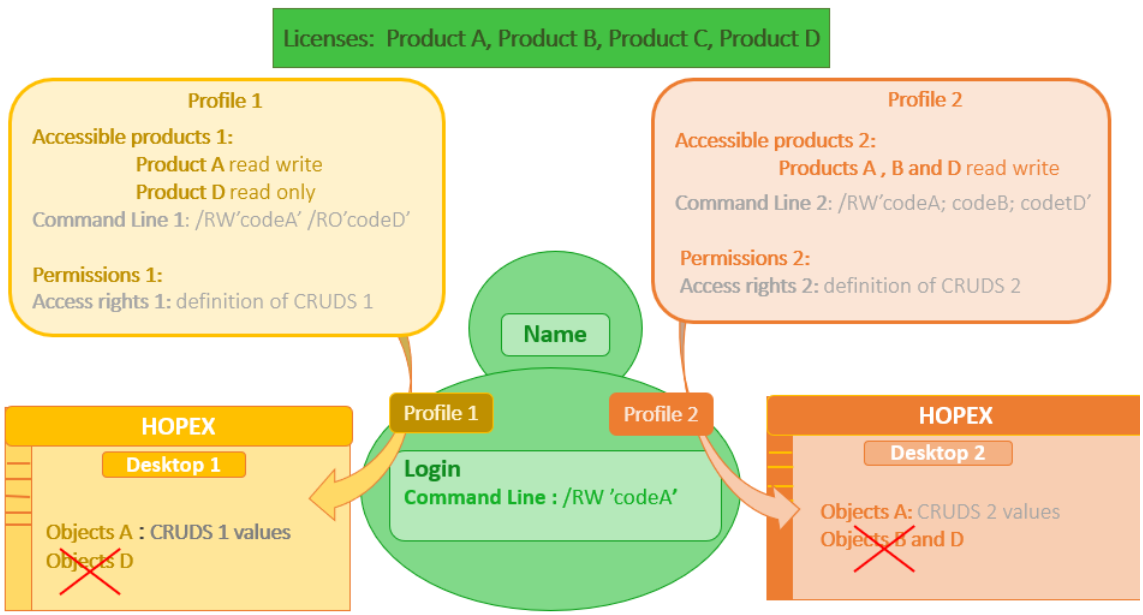
Profile 1 gives reading and writing access to Product A and read only access to product D.

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 Access 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 access to product, see Command line.

Examples:

User licenses: Products A, B, C and D.

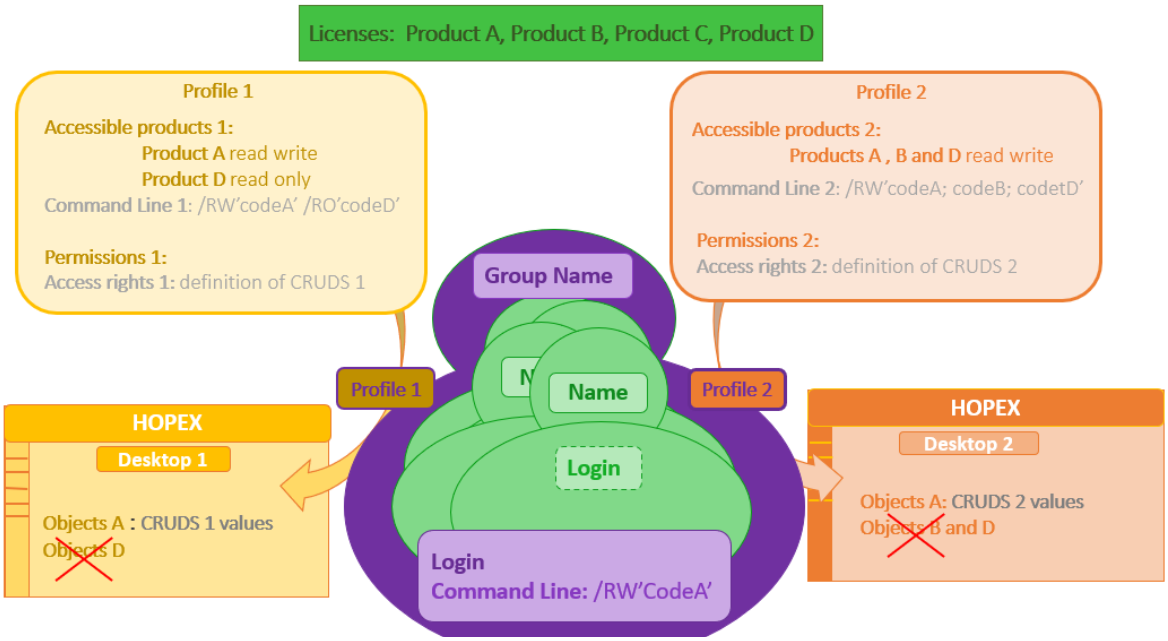
Profile 1 gives reading and writing access to Product A and read only access to product D.

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.

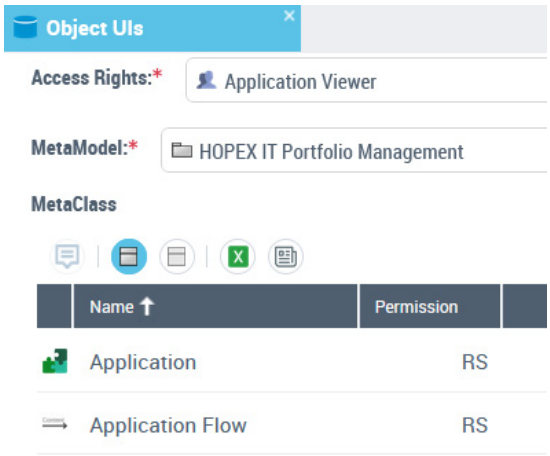


Restricting Object UI Access for a Profile (Permission)

Object UI access of a profile are defined by its associated **Set of UI access rights**.
To manage object UI access, see Managing UI Access.

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 Access for a Profile (Permission)

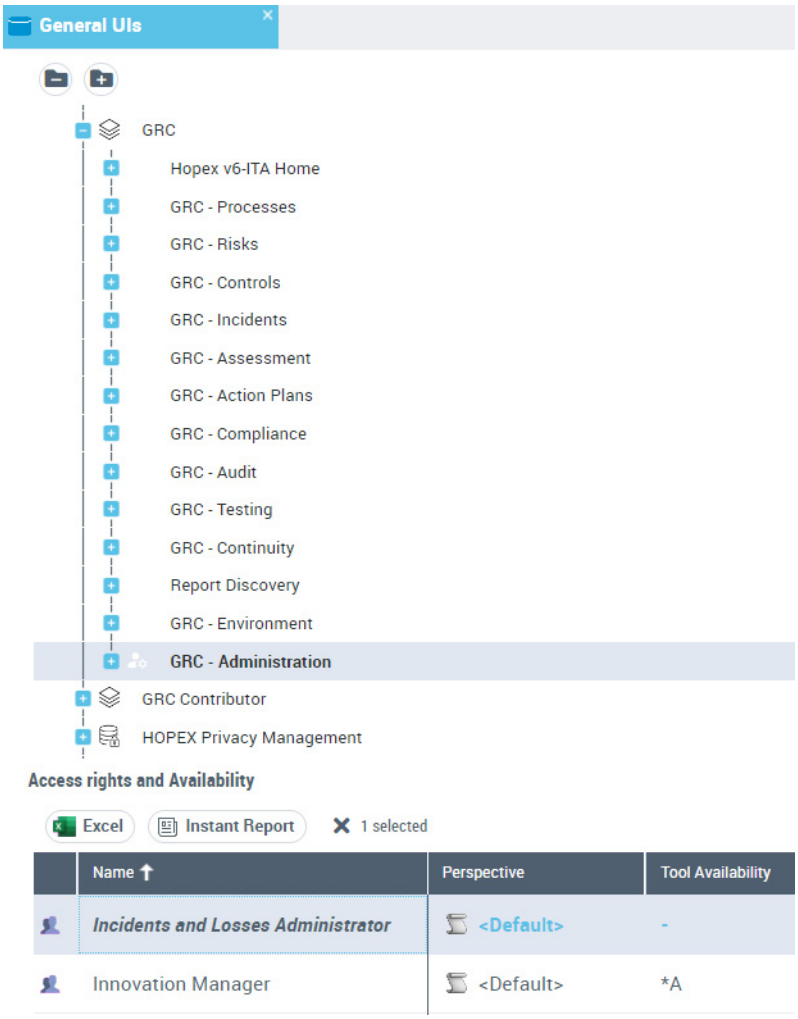
General UI access are managed for a profile. General UIs are classified by category, like:

- desktop
- command category
- command group
- general command
- property page
- tree
- Working Environment Template (WET)

To manage the general UI access, see Managing General UI Access.

Example: the **Administration** navigation menu dedicated to GRC **(Working Environment Template > GRC > GRC -**

Administration) is not available for the **Incident and Losses Administrator** profile.



Restricting Data Access 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 Access Statically

Writing access diagram (authorization) and reading access diagram (confidentiality) define data access 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 access 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, 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** is selected in the Options of the Repository of the environment (Options: **Compatibility > Windows Front-End > Administration**).

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

The HOPEX administrator can mask objects corresponding to 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, which determines the objects that the user (or user group) can see. A user (or user group) can only see objects located in his/her own or lower confidentiality areas.

4

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"
- ✓ "Performance and Health Tests"
- ✓ "Managing Updates"
- ✓ "Managing locks"

INTRODUCTION TO WORKSPACES

Workspace Types

HOPEX gives access either to:

- a public workspace
- a private workspace, or
- a read-only workspace

☛ *See "Working in HOPEX".*

☛ *The workspace type is defined by the WET (Working Environment template) properties associated with the Desktop, see "Connection diagram (with WET)".*

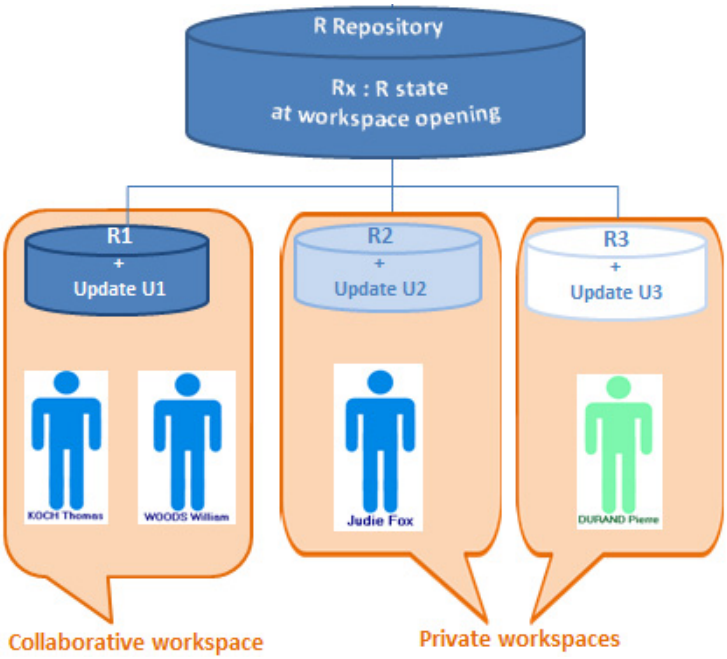
Public Workspace

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. This is the public workspace case.

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

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 at most 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.

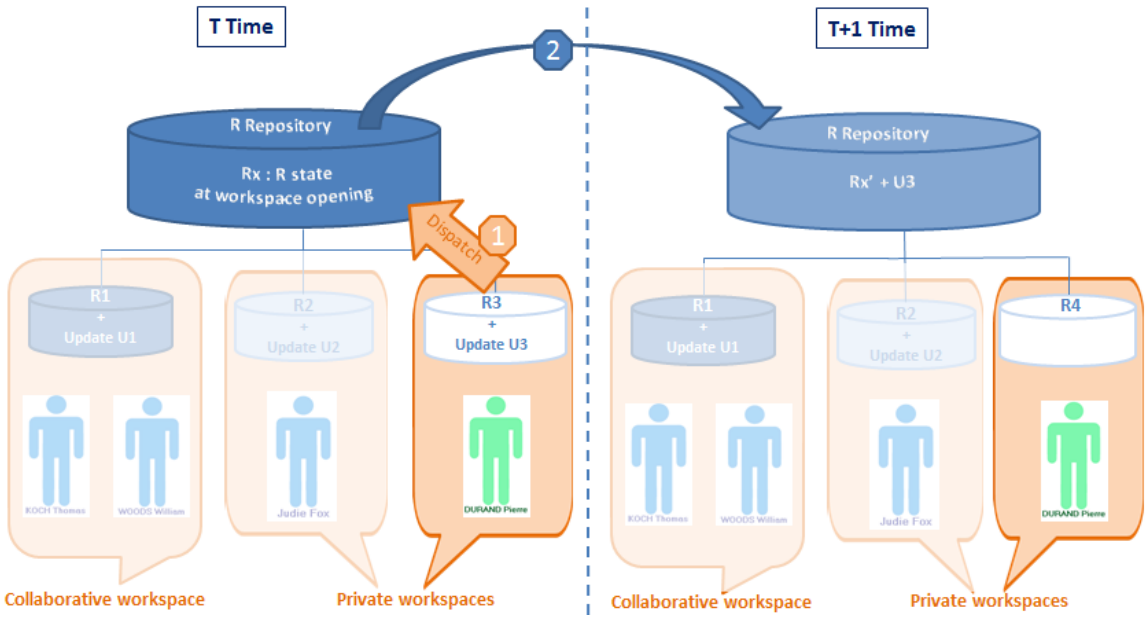
The repository changes from state N to state N+1 with memorization of new data related to the previous situation (state N).

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

Dispatch consists of making public the work carried out in a private workspace.



Dispatch 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:

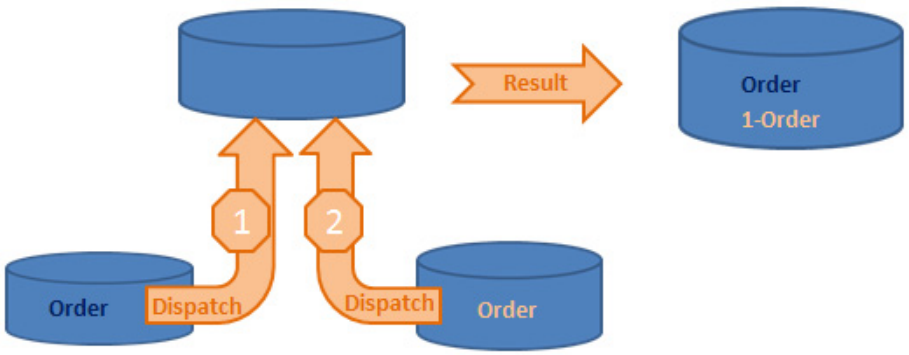
1. In your **HOPEX** desktop, click **Main Menu** .
2. Click **Dispatch**.
   Your modifications are saved in the repository.

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.*

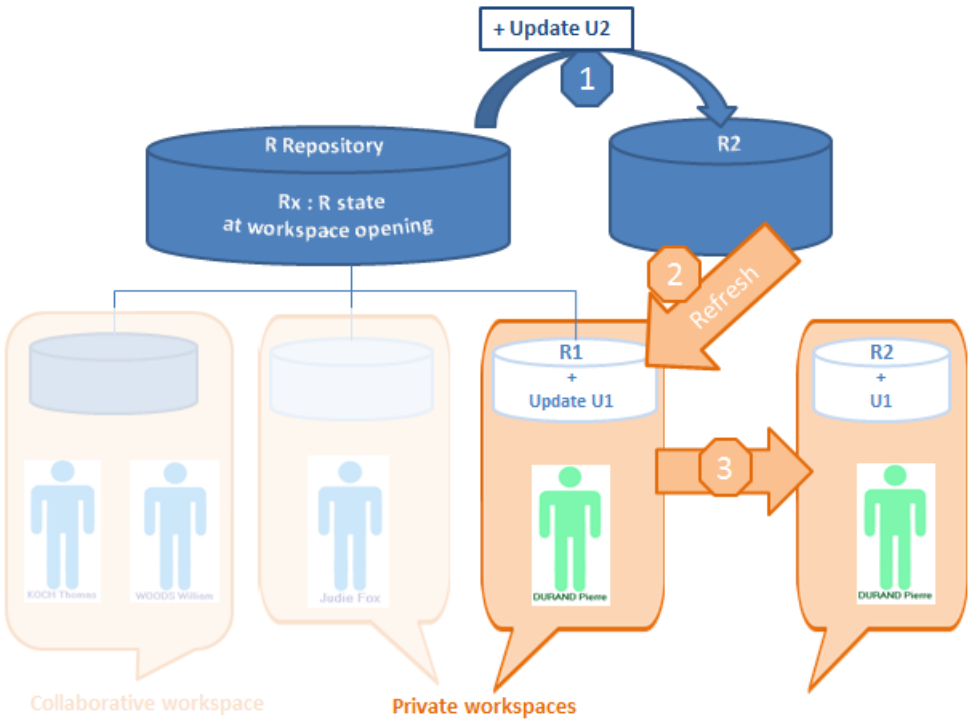
Refreshing allows a user to incorporate repository and system repository changes made by other users, without dispatching current work.

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 (the default is 6 days), **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** .

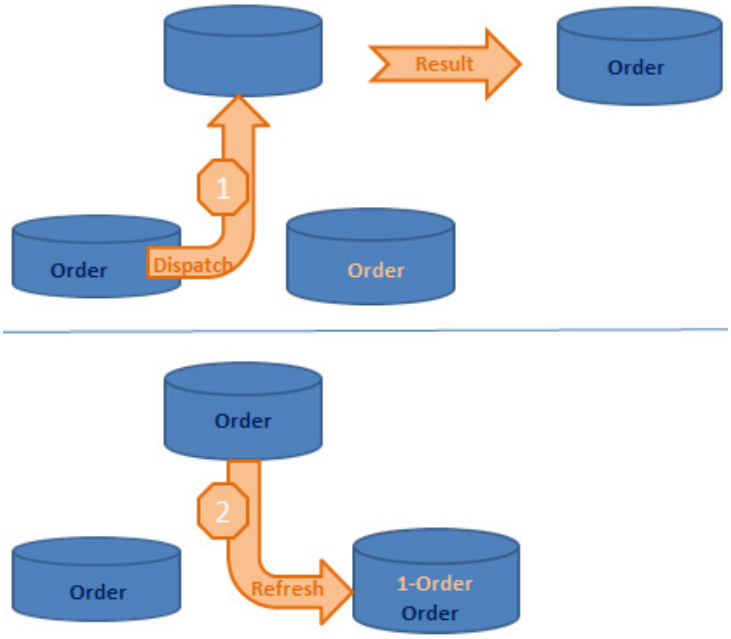
2. Click **Refresh**.

☛ *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. *Discard* of 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.

   ☛ *In the **Main Menu** , select **Export**.*

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:

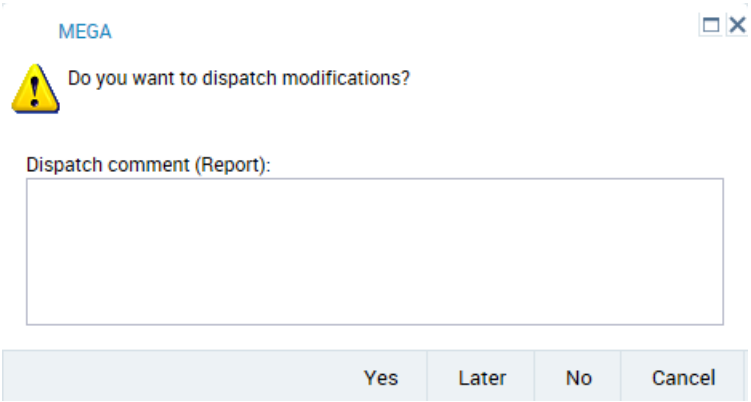
- save in the repository the modifications you have made in your private workspace
- keep the modifications you have made in your private workspace

  ☛ *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 (owner, delay, status).

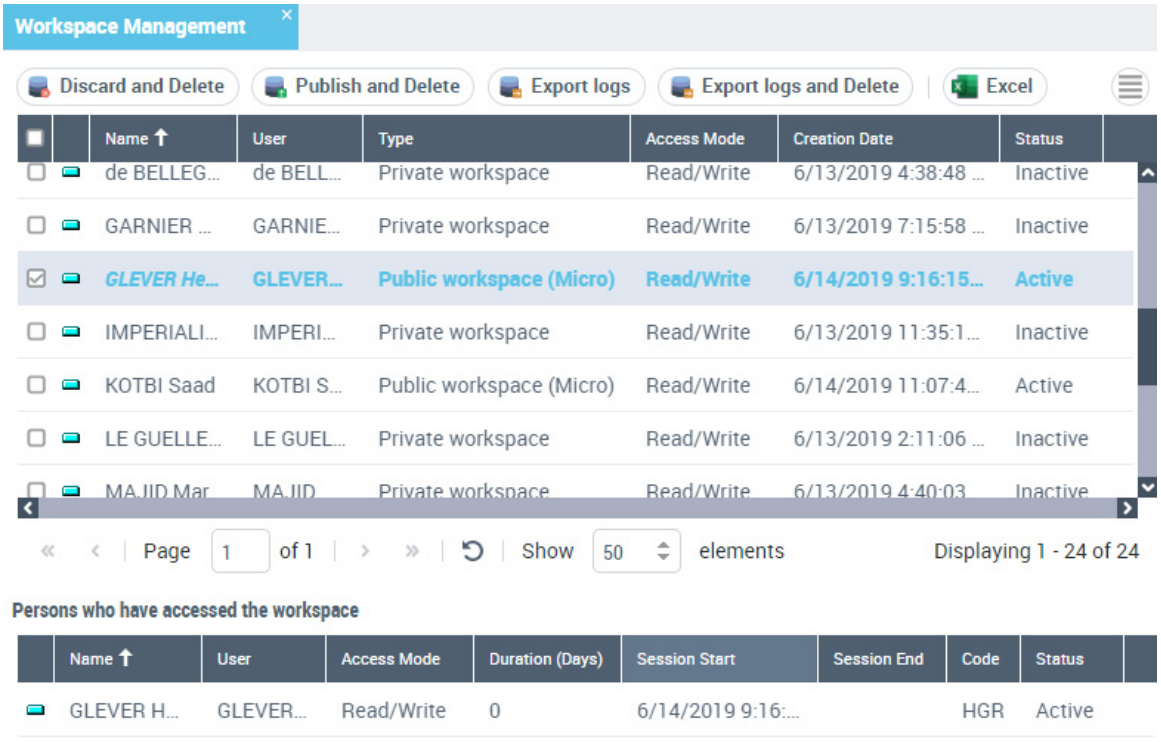
See:

- "Accessing the Management Page for Workspaces"
- "Deleting a Workspace"

Accessing the Management Page for Workspaces

To access the list of current workspaces in an environment:

1. Connect to the **HOPEX Administration** desktop.
   ☛ *See "Connecting to the Administration Desktop".*
2. In the **Administration** tab, click the **Repository Management** pane.
3. Click the **Workspace Management** sub-folder.
   The management page for workspaces currently in progress in the environment appears.



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
- its **Creation** date and time
- the **Status** of the workspace
  - active
  - inactive (in case of a private workspace)

The **Persons who have accessed the workspace** frame details:

- the **User** of the workspace
- the **Access Mode** of the workspace
- its **Duration** in days
- the start date and time of the last session
- the end date and time of the last session
- the user **Status**
  - active
  - inactive

Deleting a Workspace

The **HOPEX** administrator can delete a private workspace when the latter 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 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.: jbandi@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.

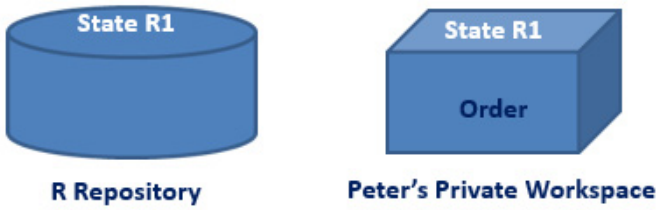
   - **Publish and Delete** if you want to keep the work performed in the workspace.

   All users listed in the **Persons who have accessed the workspace** frame receive a notification e-mail concerning the deleted workspace.

PRIVATE WORKSPACE LIFE: EXAMPLE

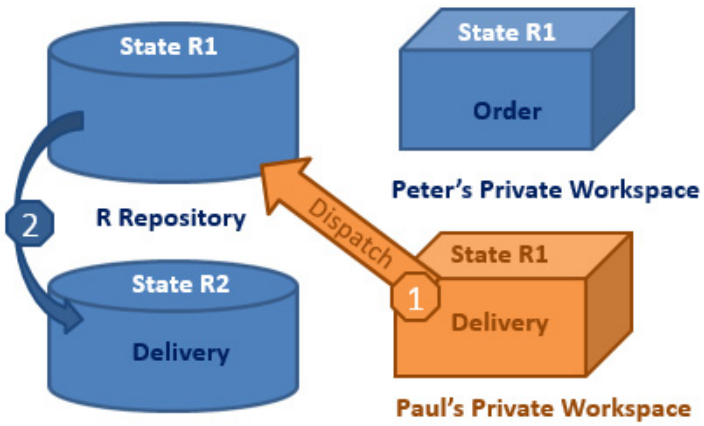
To illustrate how private workspaces work, the following is an example of some steps in the work of several users:

Private workspace 1



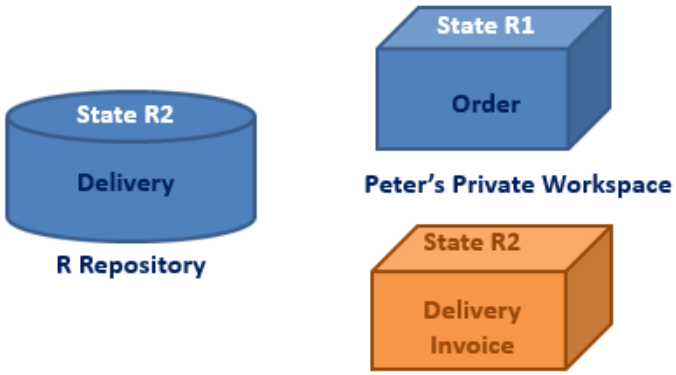
- Peter opens a private workspace, his repository view is state "n" (R1).
- He creates the "Order" message, which he links to the "Customer" org-unit.
- In parallel, Paul dispatches his private workspace...

Private workspace 2



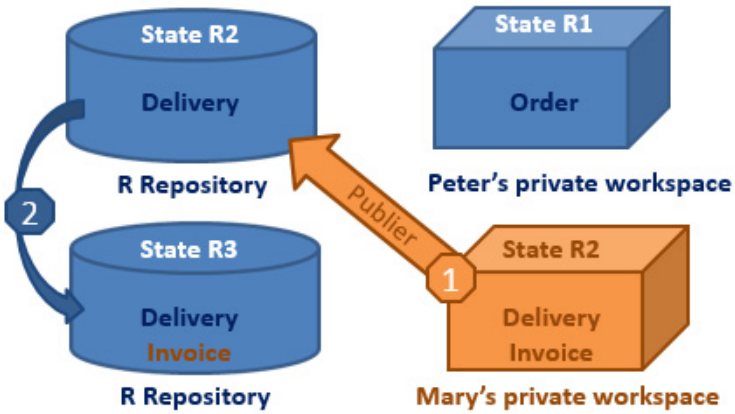
- The private workspace that Paul dispatched created the "Delivery" message, linked to the "Customer" org-unit.
- Paul's dispatch changes the repository to state "n+1" (R2).
- This new message is not seen from Peter's private workspace...

Private workspace 3



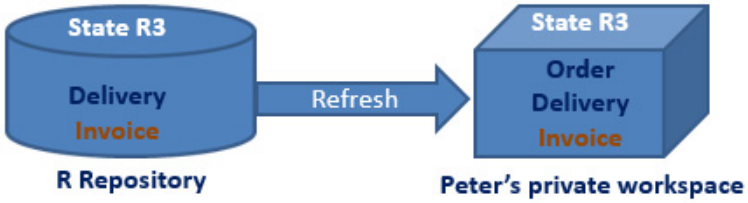
- Mary opens a new private workspace, her repository view is state "n+1" (R2).
- Mary creates the message "Invoice" connected to the "Customer" org-unit...

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.

PERFORMANCE AND HEALTH TESTS

With **HOPEX** you can daily generate a 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 Events 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.
```

The report icon is represented by:

-  if the health report does not include anomalies
-  if the health report includes anomalies

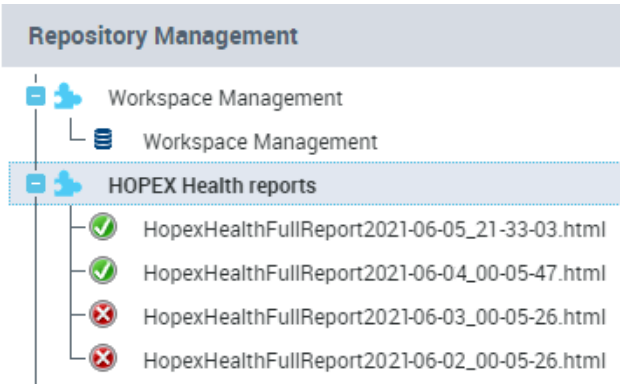
To view HOPEX daily health reports:

☛ *To access the content of the **Repository Management** pane, you must be an advanced user. In **Options > Workspace > Desktop**, the **Display advanced UI** option must be selected.*

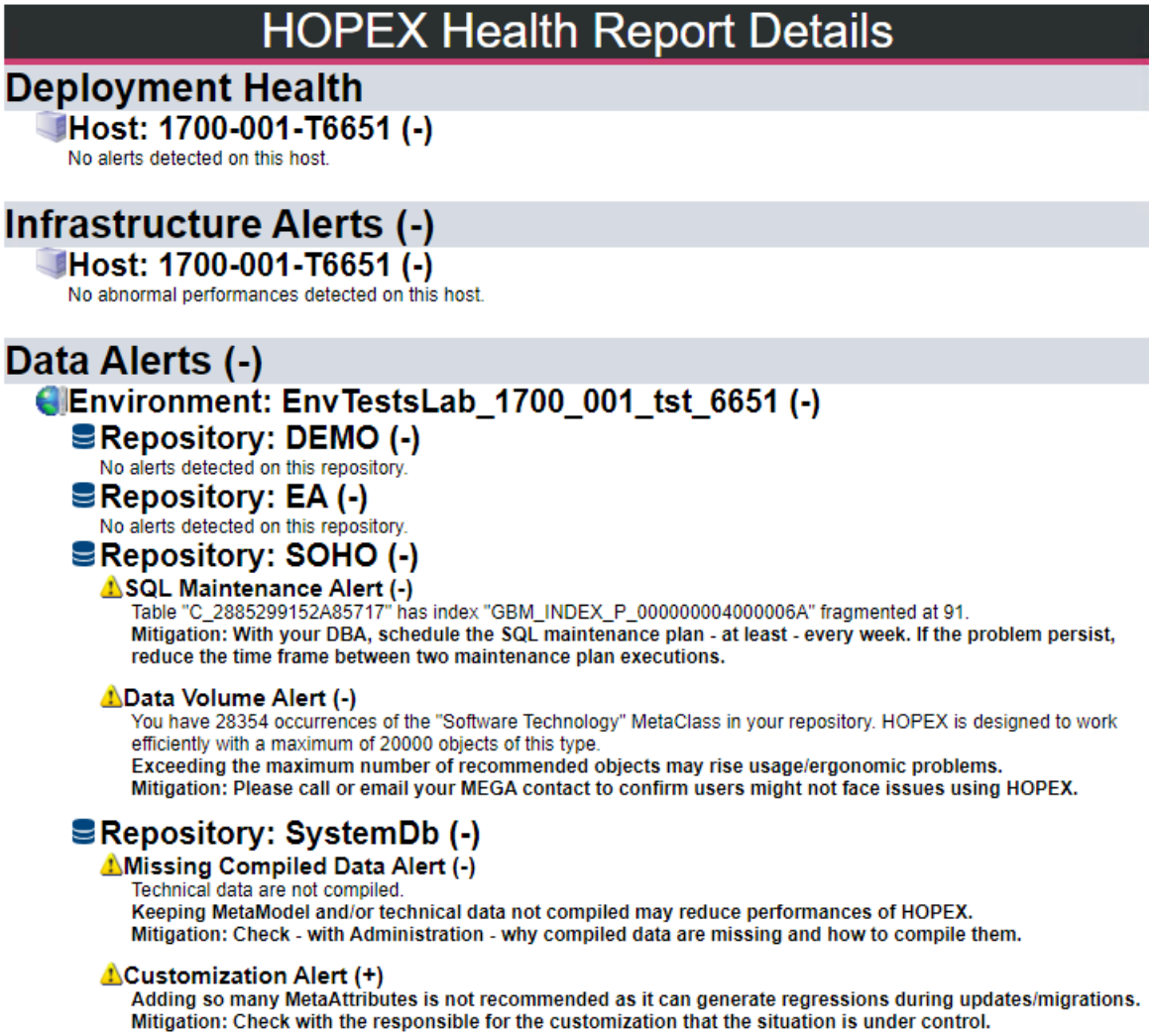
1. Connect to the **Administration** desktop.

   ☛ *See "Connecting to the Administration Desktop".*

2. In the **Repository Management > HOPEX Health reports**, click the report you are interested in (the last report is at the bottom of the list).



The report is displayed in a new browser tab.



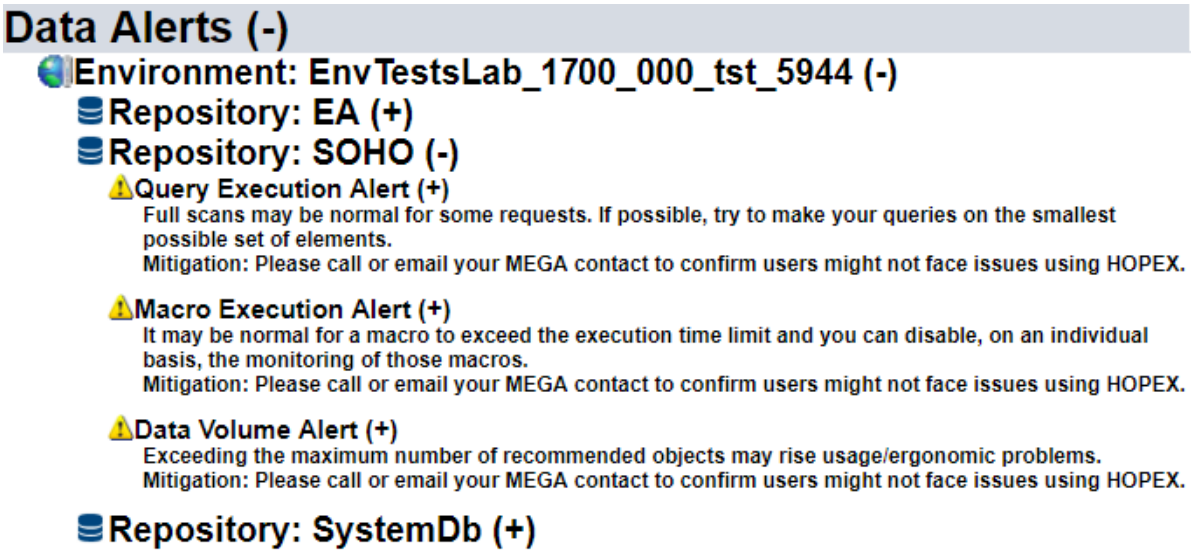
3. Click (+)/(-) beside the name of the machine, environment, repository, or aler to display/hide its details.

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: they create objects, links between objects, diagrams, etc.

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:

Displaying Updates Dispatched in the Repository

To display updates dispatched in the repository:

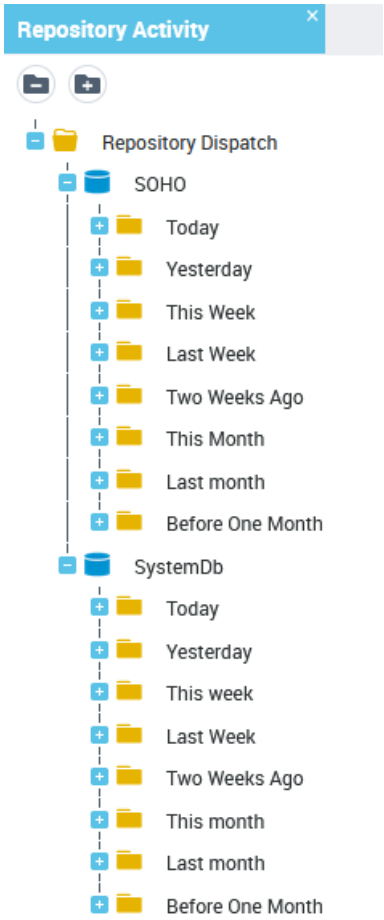
1. Connect to the **Administration** desktop.

☛ *See "Connecting to the Administration Desktop".*

2. In the **Repository Management** pane, click the **Repository Activity** sub-folder.

   ☛ *To access the content of the **Repository Management** pane, you must be an advanced user. In **Options > Workspace > Desktop**, the **Display advanced UI** option must be selected.*

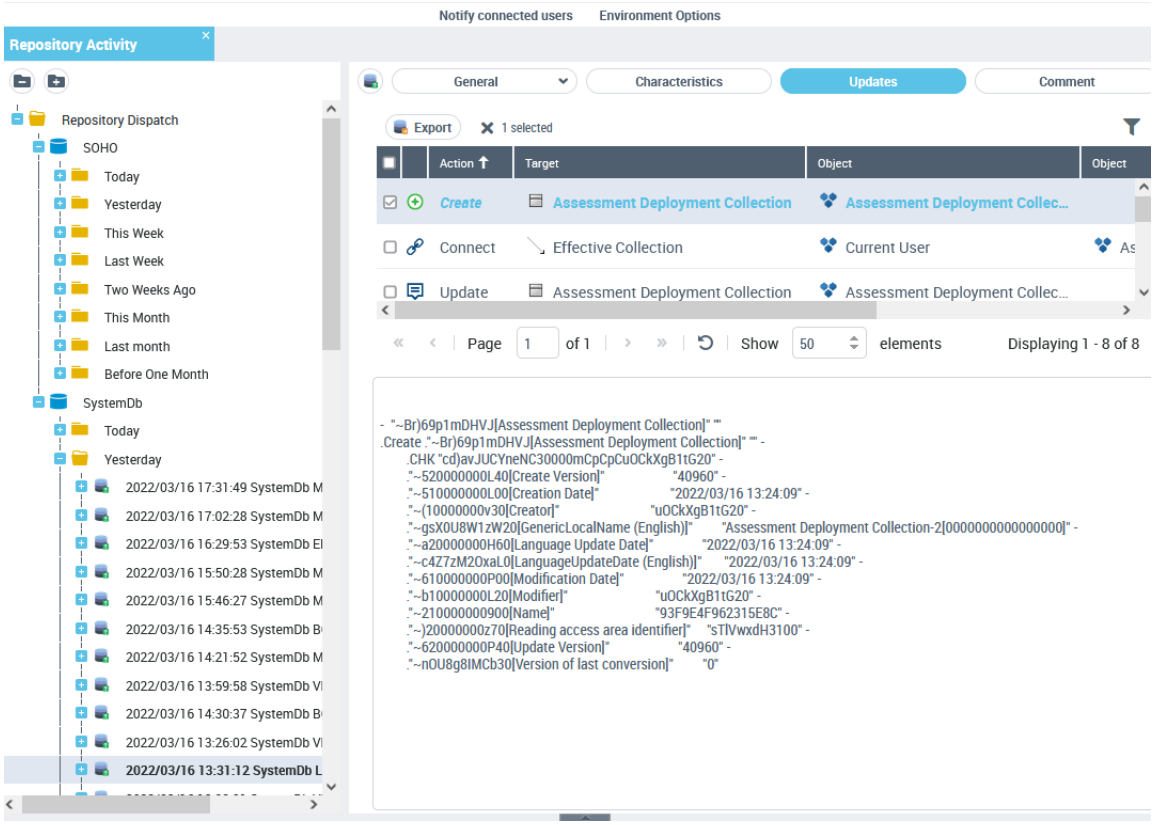
   All dispatches (from private and public workspaces) performed on the current repository and the system repository are detailed in the edit area.
   Dispatches are listed by day, week and month.



3. Expand the folders to access the dispatch you are interested in.
4. Click the dispatch.
   The dispatch property pages are displayed in the edit area.
5. Click **Updates**.
   The **Updates** page details the content of the dispatch in the form of a list of actions displayed in chronological order.

6. Select a row to display the details of the action in the lower frame.

☛ *See "Exporting a Private Workspace Log".*



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 most recent 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. In the environment **Options**, select **Options > Installation > Advanced**.
2. Modify the **Recommended open workspace duration** option value (in day).

Exporting a Private Workspace Log

You can create an export file for a dispatch.

☛ *See private workspace logfile.*

The export file can be exported in format:

- **Text** (.mgr, by default).
- **MEGA XML** (.xmg)
  The exported file is in the form of an XML file containing commands or data (objects and links).

To export the work done in a private workspace in the form of a command file:

1. Access the **Updates** page of the repository dispatch concerned.
   ☛ *See "Displaying Updates Dispatched in the Repository".*
2. Select all of its actions.
3. Click **Export**  .
4. (Optional) If necessary, modify the default export file name and format. Name format of the exported file is "OBJmmdd.mgl", where "mmdd" represents logfile export date month and day.

   ```
   File name format: "OBJmmdd000.mgr"

   where "mmdd" stands for the month and day of the export, and
   "000" a 3-digit number.
   ```

5. Click **Export**.
   The file is downloaded in the download folder of the browser.

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 date and time (GMT0) of the **Lock**, and, if applicable, **Unlock**.
  - 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)

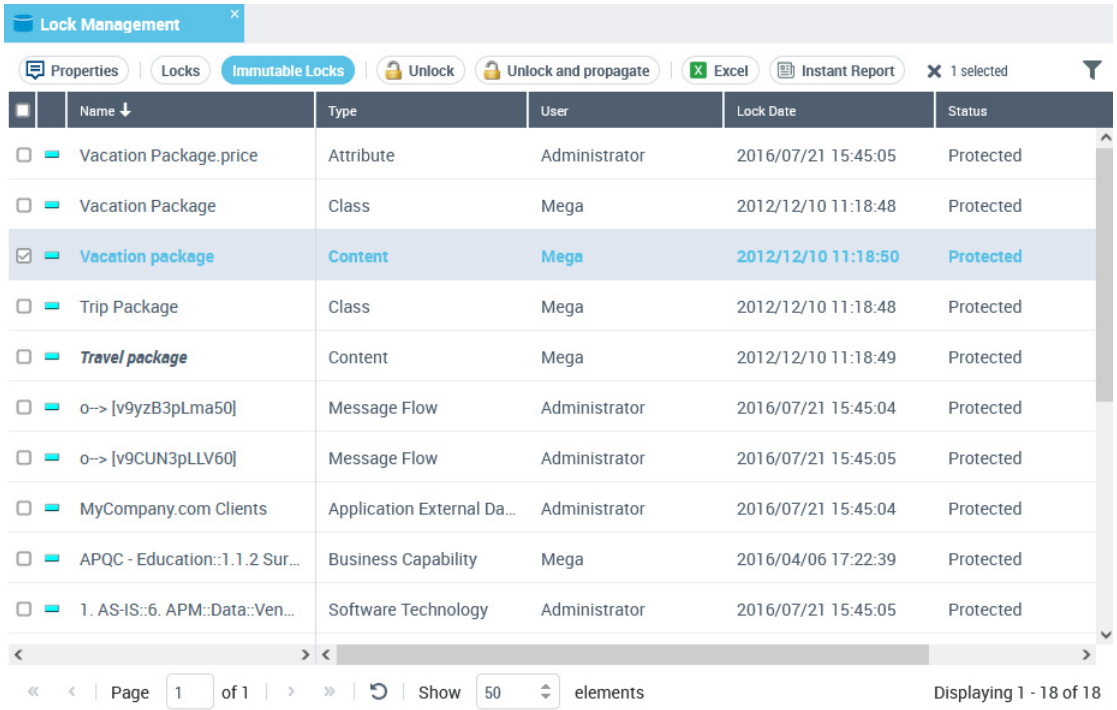
    ☛ *See "Managing immutable locks on objects".*

For each locked object, you can:

- view its properties and access the history of its modifications.

For each object locked with an immutable lock, you can:

- view its properties
- unlock the object to remove its immutability
- unlock the object and propagate to remove its immutability and that of its child locks.



Viewing locks on objects

To view locks from the **Administration** desktop:

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

   ☛ *See "Connecting to the Administration Desktop".*

2. In the **Repository Management** pane, click the **Lock Management** sub-folder.
   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.*

4. To view the history of the locked object modifications:
   - Select the locked object and click **Properties**.
   - Click the object icon and select **History**.

Managing immutable locks on objects

To manage immutable locks from the **Administration** desktop:

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

   ☛ *See "Connecting to the Administration Desktop".*

2. In the **Repository Management** pane, click the **Lock Management** sub-folder.
3. Click **Immutable Locks**.
   The page displays the list of 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.

OBJECTS

The following points are covered here:

- ✓ Importing - exporting a command file
- ✓ Comparing and Aligning Objects Between Repositories
- ✓ Merging Objects
- ✓ Managing UI Access (Permissions) (function available with **HOPEX Power Supervisor**)

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 in HOPEX.*

- in **text format** (.MG*).

  ☛ *For more details on .MG* file syntax, see Command File Syntax.*

- In **MEGA 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 in HOPEX
- Exporting Objects

Importing a command file in 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.

To export a command file from the **Administration** desktop:

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

   ☛ *See Connecting to the Administration Desktop.*

2. In the **Administration** tab, click the **Tools** pane.
   The management tree for tools appears.
3. In the tree, select the **XMG/MGL/MGR > Import** sub-folder.
   The **Hopex File Import - Parameterization** page appears.
4. In the **Command File** field, click **Browse** to browse the folders and select the backup file.

   ☛ *The command file must not exceed 30 MB.*

5. Select the types of **Processing** to be executed:
   You can update:
   - the **Metamodel** (repository structure)
   - the **Technical Data** (*descriptions*, *requests*, as well as *users*).
   - the **Data** (most frequent case)

     ☛ *If the file includes commands that do not match the type you have selected, these commands are ignored.*

6. (If needed) Modify the **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 on success*** *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.*

7. 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 maintained.*

     ☛ *For command files with the MGL extension (log extraction), the absolute identifiers are included in the imported objects. The writing access levels are maintained 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.*

8. 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.

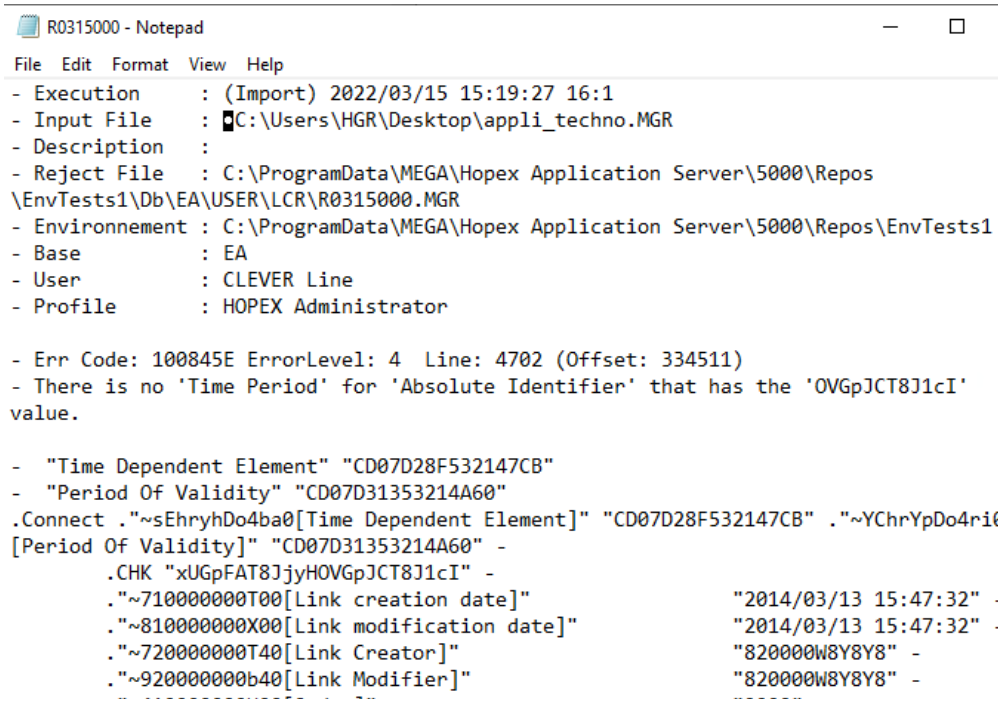
   ☛ *For more details on the main causes of rejects, see Dispatch Conflicts and Rejects When Dispatching.*

9. Click **Import**.
   The report page appears.
   When the import contains errors, a reject report file is generated.

10. (if necessary) 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:

- **plain text**
  The exported file is in the form of an .MGR file.

  ☛ *For more details on .MGR file syntax, see Command File Syntax.*

- **XML MEGA**
  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 70".*

To export **HOPEX** objects from the **Administration** desktop:

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

   ☛ *See Connecting to the Administration Desktop.*

2. In the **Administration > Tools > XMG/MGL/MGR** pane, select **Export**.
   The **Hopex Objects Export - Parameterization** page appears.
3. (If needed) In the **Destination** section, in the **Export File** field, modify:
   - the file format
   - 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 configuration options are selected:
   - **Include Objects of Merging** exports the technical objects resulting from merging objects (_TransferredObject).
   - **Propagate** exports the objects listed together with their dependent objects.
5. In the **Objects to export** section, click **Add objects to list**  .
   The search window 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 in 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 repository archived states

☛ *The objects compared must not be in the same private workspace.*

See:

- Compare and Align Principle
- Compare and Align Warnings
- Comparing and Aligning

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 cont 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 files: in environment options **Options > Tools > Data Exchange > Import/Export Synchronization > MEGA**, select the option **Delete files produced at compare/align on completion of processing**.*

Comparing and Aligning

The compare and align feature is available in all of 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 Connecting to the Administration Desktop or Connecting 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.

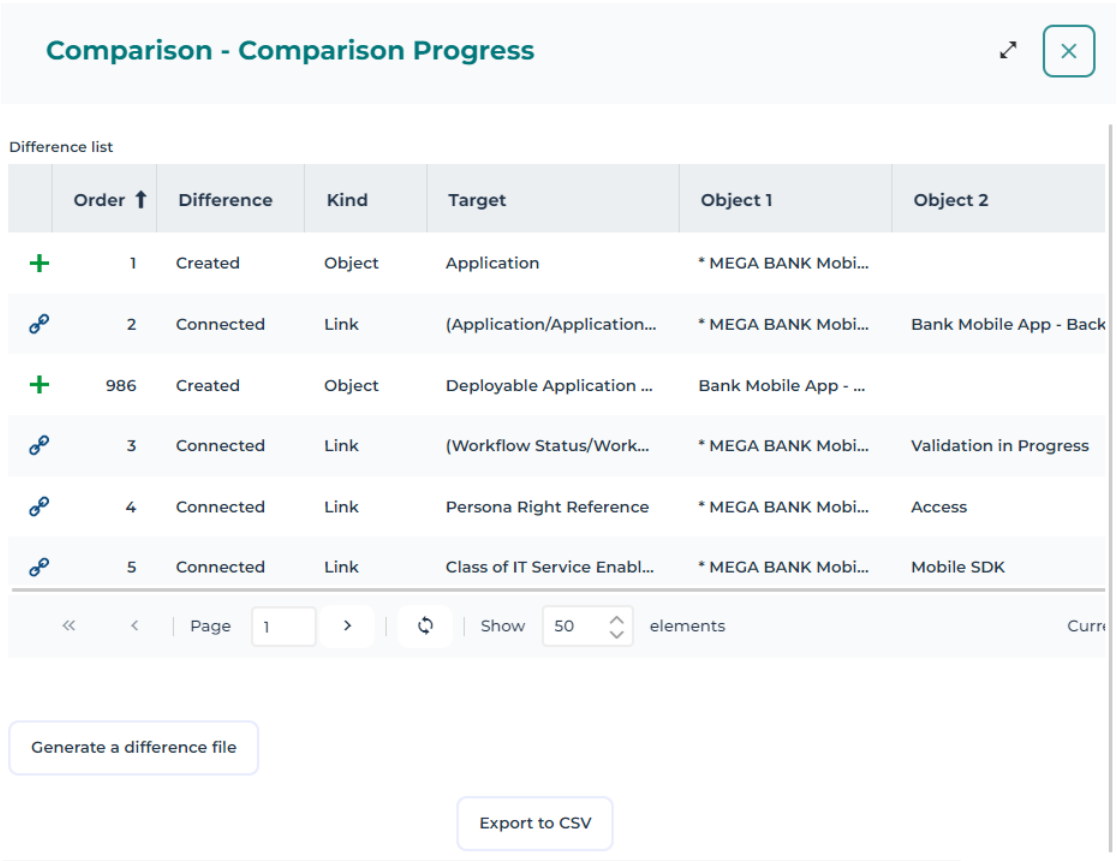
     ☛ *It can be a private workspace of the repository.*
6. (Optional) If required, you can choose to **Compare all repository objects**. Select the option an go to step 10.

   ☛ ***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.



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. To do this, 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 be merged

The **Target** object is the reference object that will be merged with the **Source** object. By default:

- its characteristics are not modified
- the 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 desktop and Solution desktops.

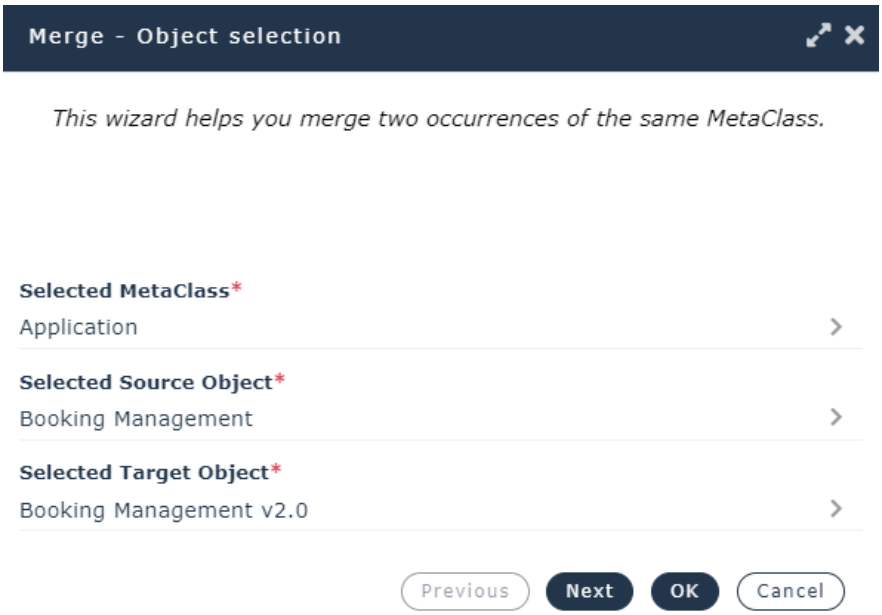
To merge two objects:

1. Connect to **HOPEX** with the required profile.

   See Connecting 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.

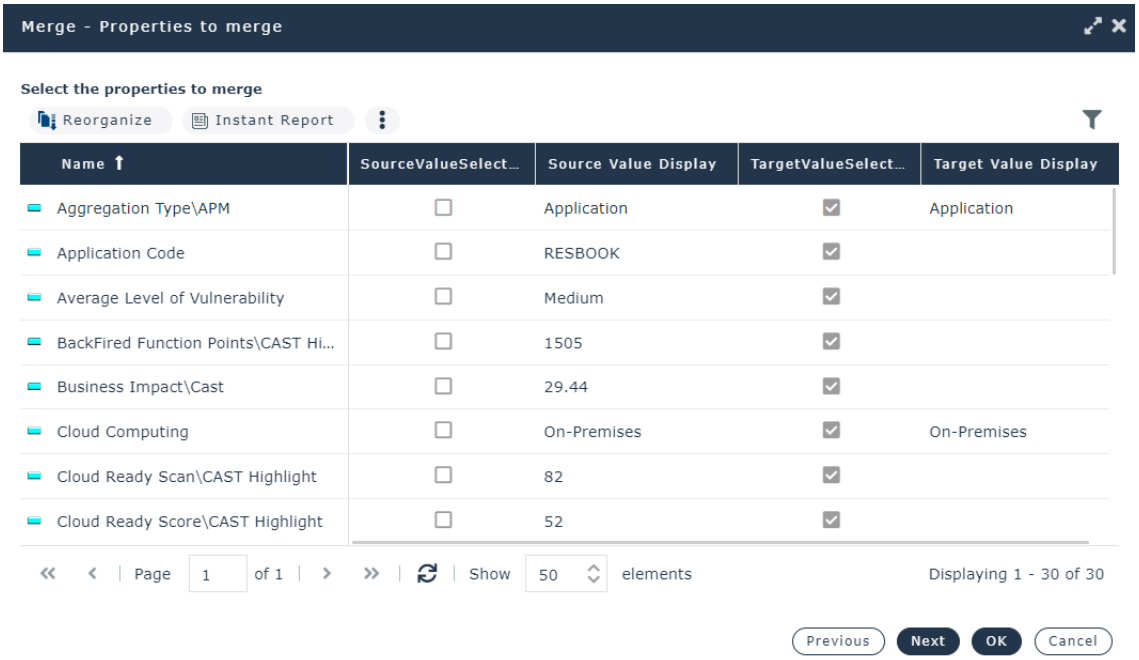
   (private workspace case) To have the right to merge two objects, you must have the right to delete objects.
4. In the **Selected Target object** field, click the arrow and **Select a target object**.
5. Use the search tool to select the target object and click **OK**.

6. Click **Next**.



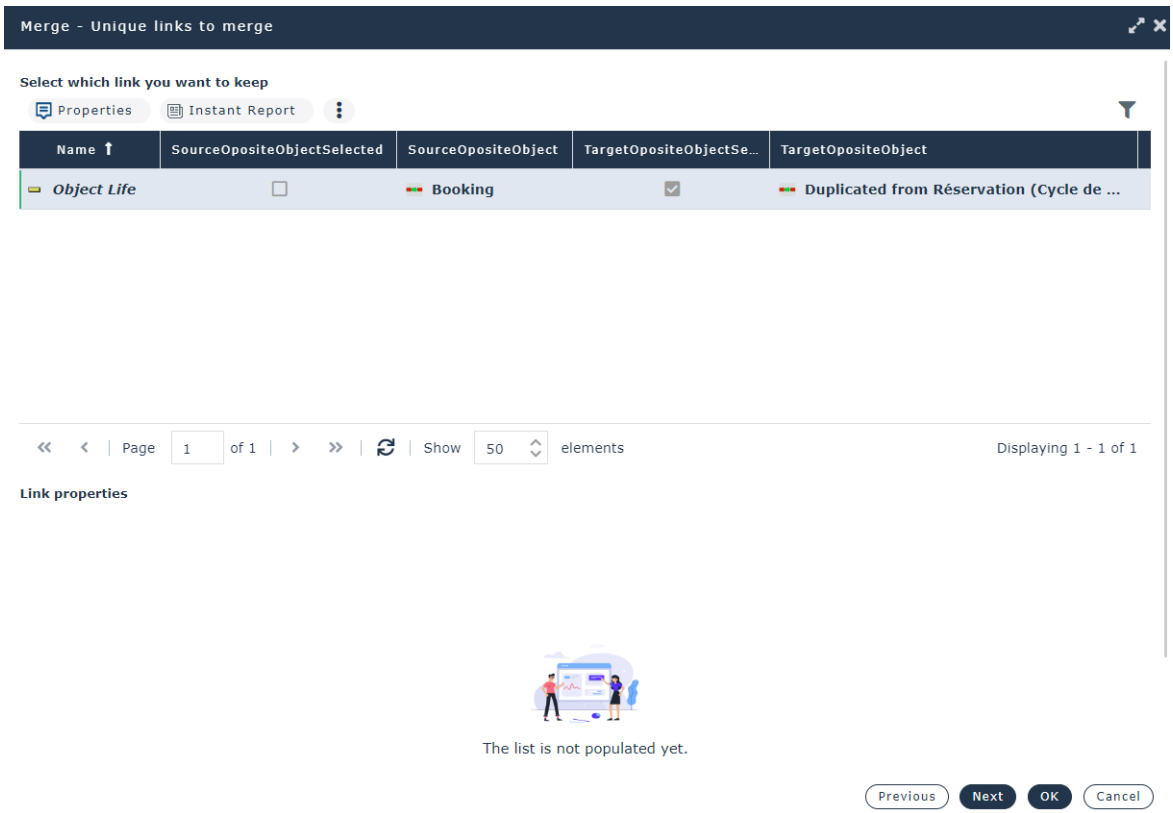
7. Click **Next**.
   The **Properties to merge** window shows the differences found in the characteristic values of both objects.

8. 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.



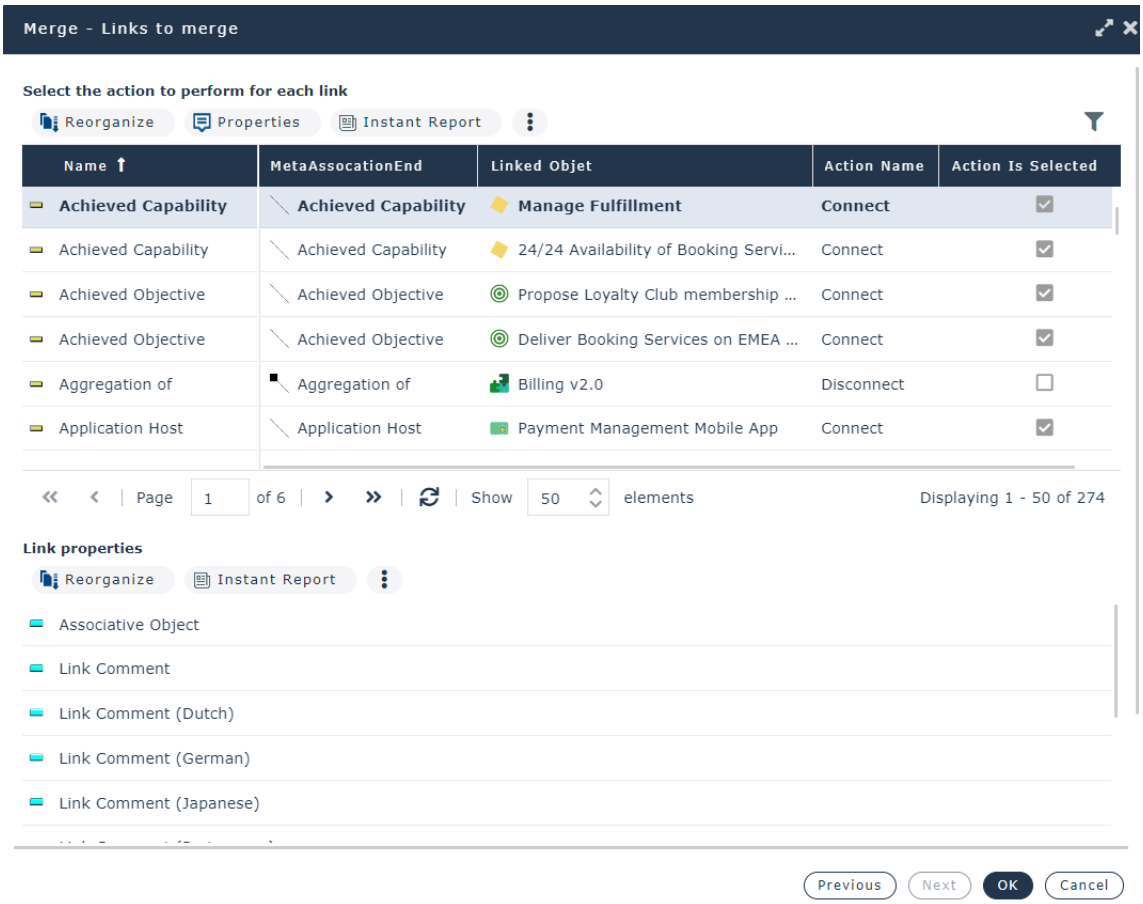
9. Click **Next**.
The **Unique links to merge** window (links that can only exist once for a given object) appears only if the objects to be merged have unique links connecting them to different objects.

Example: a message can have only one super-type.



10. Select the links to be transferred.

11. 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.

12. Click **OK** to start merging.
Once merging is 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 UI ACCESS (PERMISSIONS)

Introduction to UI Access Management (Permissions)

Prerequisites and definitions

UI access management (Permission management) is only available with the **HOPEX Power Supervisor** technical module.

UI access (permissions) of a profile is defined by its associated Set of UI access rights.

You can manage:

- *object UI access*

  📖 *Object UI access defines user rights on creation, reading, update, and deletion on these objects and their tools. By default, object UI accesses have value *CRUD (C: create, R: read, U: update, D: delete, *: default value).*

  ☛ *For information on management of workflow UI accesses, see the HOPEX Power Studio > Customizing Workflows > Managing permissions on Workflows documentation.*

- *general UI access*

  📖 *General UI access defines if tools are available or not. By default, general UI accesses have value *A (A: Available, *: default value)*

To manage UI access you must connect with the **HOPEX Administrator** profile.

☛ *The **HOPEX Administrator - Production** profile does not have access to UI Access management.*

Performance

For optimum performance, after modifying permissions you must compile the permissions.

☛ *Permission compilation is recommended in a production environment, see the HOPEX Administration > Managing Environments > Compiling an environment documentation.*

Accessing the UI Access Management Pages (Permission)

The **Permission** pane enables management of UI access for the complete environment and for each Set of UI access rights:

- **Object UIs** details its access to UI of objects and its access to tools specific to these objects.

  ☛ *See Object UI Access Values.*

  ☛ *See Managing UI Access.*

- **General UIs** details its access to general UIs.

  ☛ *See Object UI Access Values.*

  ☛ *See Managing General UI Access.*

To access the UI access management pages:

1. Connect to the **HOPEX Administration** desktop with the **HOPEX Administrator** profile
   ☛ *See Connecting to the Administration Desktop.*
2. In the **Administration** tab, click the **Permissions** pane.
3. In the **CRUD Management** tree, select the sub-folder:
   - **Object UI access**
   - **General UI access**

Object UI Access Values

Object UI access enables definition of user permissions on the selected metamodel.

- Preceding the value of a permission, the character:
  - * indicates that the value is directly inherited from the default value.
  - - indicates that the value is inherited from an element hierarchically higher in the same profile or sub-profile.
- Value empty means that the user has no permission on the element. The element is not visible to the user.
  When a MetaClass is hidden to a user, it is not available in the repository.

  For example, if the "Package" MetaClass is hidden for a user, this user cannot use packages in modeling work since this object type is not accessible in the interface.

MetaClass occurrence access permissions

By default, the access permission on occurrences of a MetaClass takes value *CRUD:

- C: Create
- R: Read
- U: Update
- D: Delete
- S: available in the quick Search tool

An access permission on occurrences of a MetaClass can take combinations of values:

- **RS**: read and search occurrences of the MetaClass
- **CRUS**: create, read, update, and search occurrences of the MetaClass
- **CRUDS**: create, read, update, delete, and search occurrences of the MetaClass
- **RUS**: read, update, and search occurrences of the MetaClass
- **RUDS**: create, read, update, delete, and search occurrences of the MetaClass
- **R**: read occurrences of the MetaClass
- **CRU**: create, read and update occurrences of the MetaClass
- **CRUD**: create, read, update and delete occurrences of the MetaClass
- **RU**: read and update occurrences of the MetaClass
- **RUD**: create, read, update and delete occurrences of the MetaClass

MetaAssociationEnd access permissions

By default, the access permission on a MetaAssociationEnd takes value *CRUD :

- C: Connect
- R: Read
- U: Update
- D: Disconnect
- M: Mandatory

A permission on a MetaAssociationEnd can take combinations of values:

- R
- CRU
- CRUD
- RU
- RUD

MetaAttribute access permissions

By default, access permission on a MetaAttribute takes value: *RU.

- R: Read
- U: Update
- M: Mandatory

A permission on a MetaAttribute can take combinations of values:

- R: the MetaAttribute is visible
- RU: the MetaAttribute is visible and modifiable
- RUM: the MetaAttribute is visible, modifiable and mandatory

Permissions on a tool

A tool can be available or not.

By default, availability on a tool is: *A.

The permission on a tool can take value:

- A: the tool is available
- <empty>: the tool is not available

Managing UI Access

☛ *For information on management of accesses to user interface workflows, see the **HOPEX Power Studio - Workflows** guide.*

The UI access rights (permissions) of a profile are defined by its associated Set of UI access rights.

For a new Set of UI access rights, by default its access permissions on an object are:

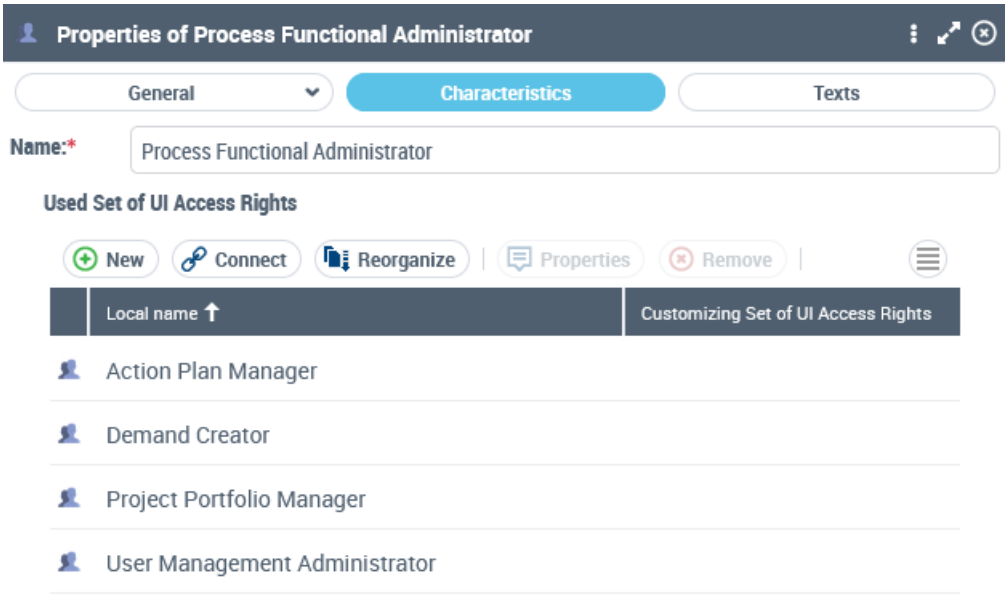
- inherited from the access permissions defined on the Set(s) of UI access rights it uses.

  ☛ *See:*

  Customizing the UI Access (Permissions) of an Existing Profile and *Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile*.

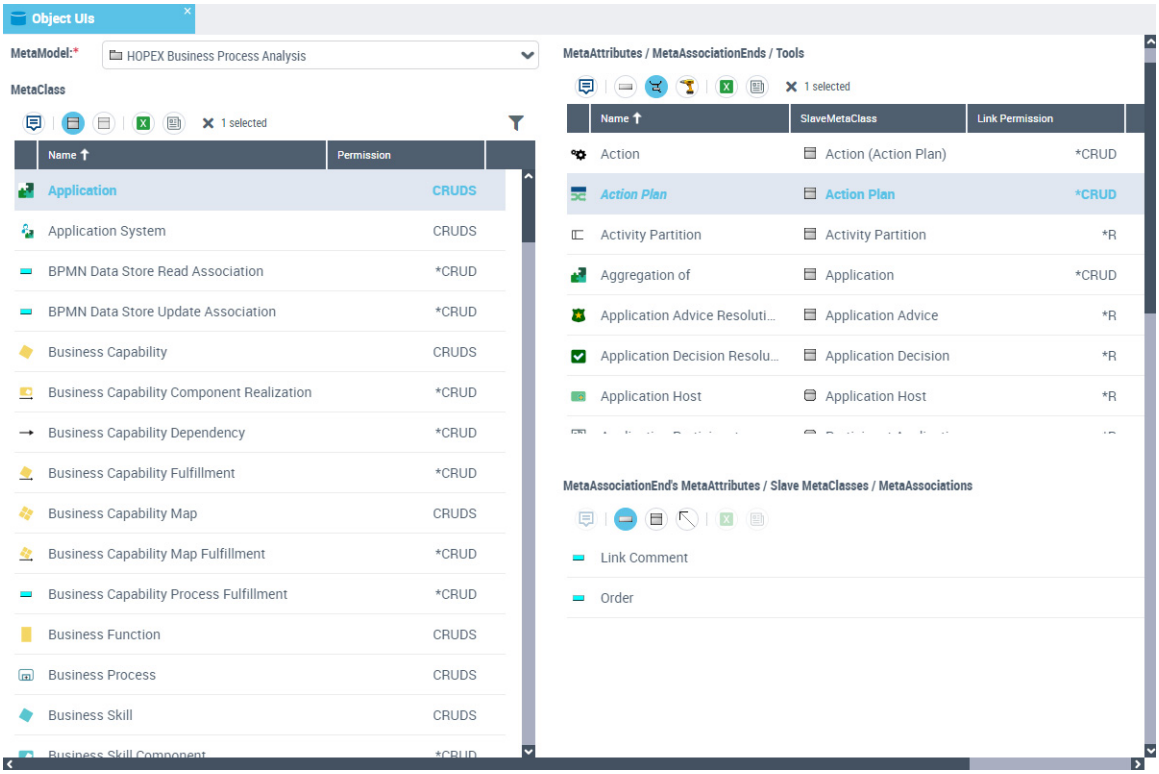
  ☛ ***See Rules on permissions while aggregating Sets of UI access rights.***

  For example the "Auditor/Controller" Set of UI access rights (of the **Auditor/Controller** profile) inherits from the permissions defined on the "Auditor" and "Internal Controller" Sets of UI access rights.



- Inherited from the permissions defined by default (<HOPEX default>), if it does not use any Set of UI access rights.

  ☛ *See Creating a Profile.*



In the **Object UIs** tab:

- the **Access Rights** field enables to select the Set of UI access rights for which you want to view or modify the permissions.
- the **MetaModel** field enables filtering of MetaClasses displayed in the **MetaClass** frame according to the selected MetaModel.
  - "All" value lists all existing MetaClasses.
  - value Extensions lists all MetaClasses that are not stored in standard Metamodels (MEGA Products products)

To define access permissions on objects, see:

- Modifying access permissions on occurrences of a MetaClass.
- Modifying access permissions on MetaAttributes of a MetaClass.
- Modifying access permissions on tools of a MetaClass.
- Modifying access permissions of a link around a MetaClass.
- Modifying access permissions on links around a MetaClass.

Modifying access permissions on occurrences of a MetaClass

To modify access permissions on occurrences of a MetaClass:

1. Access the UI access management pages and select the **Object UI Access**.

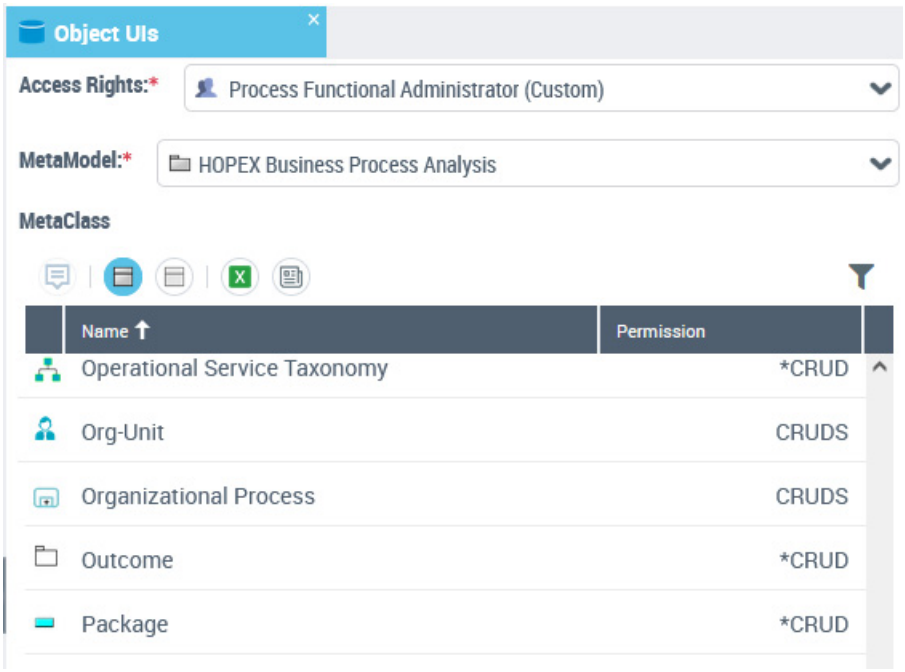
   ☛ *See Accessing the UI Access Management Pages (Permission).*

2. in the **Access Rights** field, use the drop-down menu to select the Set of UI access rights.

   ☛ *<HOPEX Default> defines default access permissions of each MetaClass, MetaAttribute, MetaAssociationEnd and tool.*

3. In the **MetaModel** field, select the MetaModel concerned.
   In the **MetaClass** frame, the listed MetaClasses are filtered according to the selected MetaModel.

   ☛ *By default **Concrete MetaClasses** are displayed, click the **Abstract MetaClass** to display abstract MetaClasses.*

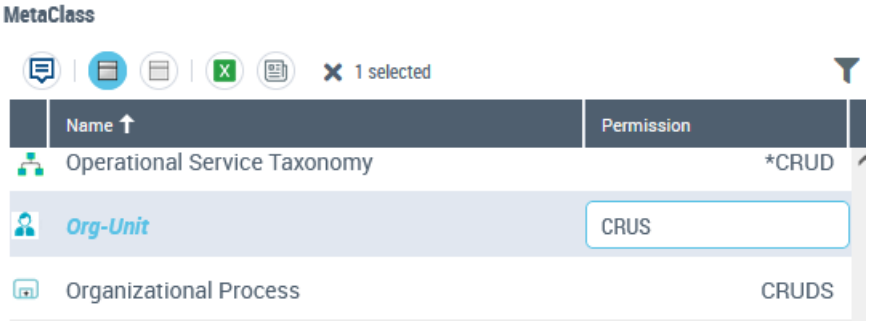


4. In the **MetaClass** frame, select the MetaClass for which you want to modify configuration of access permissions.

   ☛ *By default, its configuration is that inherited from <HOPEX Default>.*

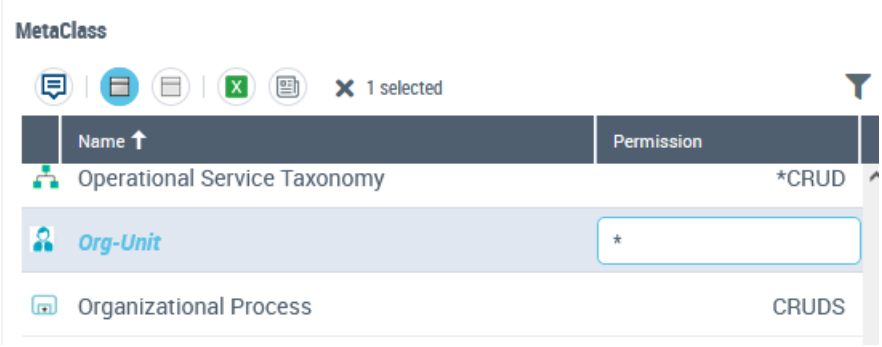
5. In the **Permission** field, enter the new value.

☛ *See MetaClass occurrence access permissions.*

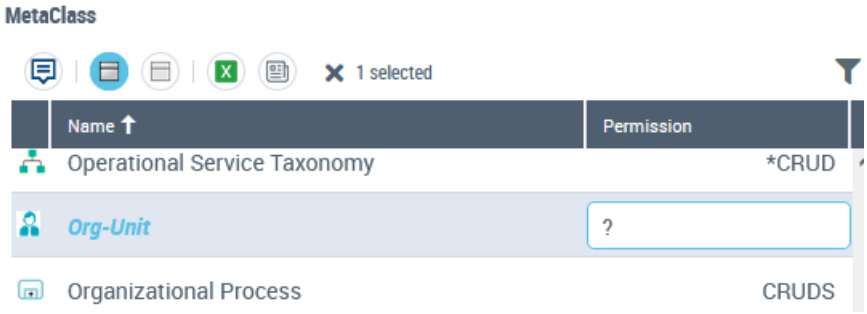


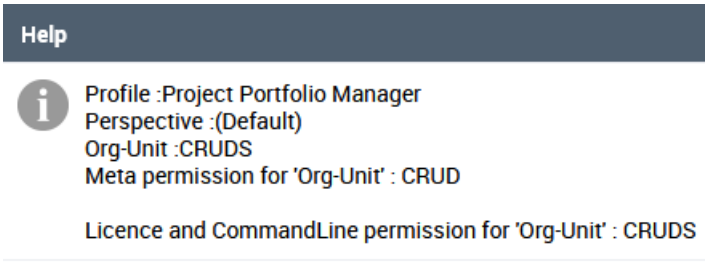
6. Press "Enter".
The value of the MetaClass permission is modified.
In the **MetaAttributes/MetaAssociationEnds/Tools** frame, the values of permissions of elements of the MetaClass are also modified.

☛ *To return to the default value of the permission on the MetaClass, enter the character *.*



☛ *To obtain information on inheritance of the value, enter the character ?.*





For example here:

The permission of **Process Functional Administrator (Custom)** on the **Org-Unit** MetaClass is inherited from the Set of UI Access Rights **Project Portfolio Manager**: CRUDS.

The permission of the **Org-Unit** MetaClass is CRUD, the command line of the **Process Functional Administrator** profile for the **Org-Unit** MetaClass is not restrictive: CRUDS.

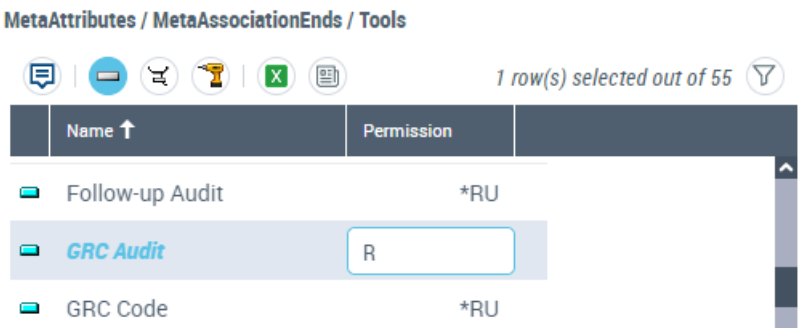
You can also modify the MetaAttributes/MetaAssociationEnds/Tools of a MetaClass, see:

- Modifying access permissions on MetaAttributes of a MetaClass.
- Modifying access permissions on tools of a MetaClass.
- Modifying access permissions of a link around a MetaClass.
- Modifying access permissions on links around a MetaClass.

Modifying access permissions on MetaAttributes of a MetaClass

To modify access permissions of MetaAttributes of a MetaClass:

1. Access the UI access management pages and select the **Object UI Access**.
   ☛ *See Accessing the UI Access Management Pages (Permission).*
2. in the **Access Rights** field, use the drop-down menu to select the Set of UI access rights.
   ☛ *<HOPEX Default> enables to define default access permissions of each MetaClass, MetaAttribute, MetaAssociationEnd and tool.*
3. In the **MetaModel** field, select the MetaModel concerned.
   In the **MetaClass** frame, the listed MetaClasses are filtered according to the selected MetaModel.
4. In the **MetaClass** frame, select the MetaClass concerned.
5. In the toolbar of the **MetaAttributes/MetaAssociationEnds/Tools** frame, click **MetaAttribute** .
   The MetaAttributes of the MetaClass are listed.
6. Select the MetaAttribute for which you want to modify permissions.
7. In the **Permission** field, enter the new value.
   ☛ *See MetaAttribute access permissions.*



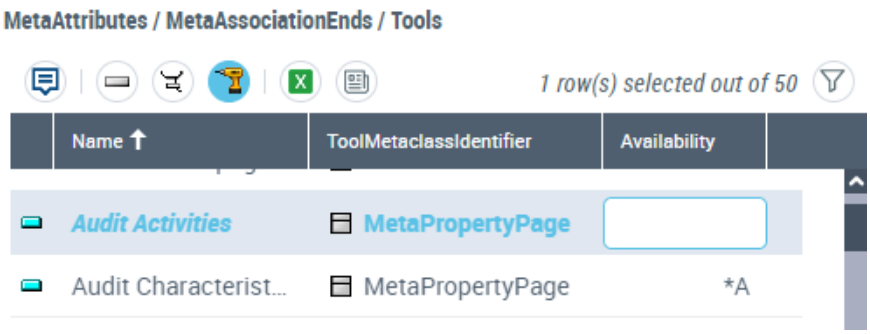
8. Press "Enter".
   The value of the MetaAttribute permission is modified.
   ☛ *To return to the default value, enter the character *.*
   ☛ *To obtain information on origin of an inherited value, enter the character ?.*

Modifying access permissions on tools of a MetaClass

A tool can be available or not.

To modify access permissions on tools of a MetaClass:

1. Access the UI access management pages and select the **Object UI Access**.
   ☛ *See Accessing the UI Access Management Pages (Permission).*
2. in the **Access Rights** field, use the drop-down menu to select the Set of UI access rights.
   ☛ *<HOPEX Default> enables to define default access permissions of each MetaClass, MetaAttribute, MetaAssociationEnd and tool.*
3. In the **MetaModel** field, select the MetaModel concerned.
   In the **MetaClass** frame, the listed MetaClasses are filtered according to the selected MetaModel.
4. In the **MetaClass** frame, select the MetaClass concerned.
5. In the toolbar of the **MetaAttributes/MetaAssociationEnds/Tools** frame, click **Tools** .
6. Select the tool for which you want to modify access permissions.
7. In the **Permission** field, enter the new value.
   ☛ *See Permissions on a tool.*



8. Press "Enter".
   The value of the tool access permission is modified.
   ☛ *To return to the default value, enter the character *.*
   ☛ *To obtain information on inheritance of the value, enter the character ?.*

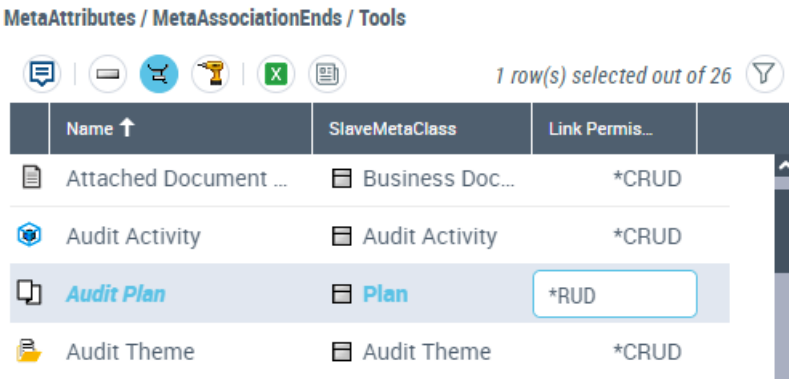
Modifying access permissions of a link around a MetaClass

To modify access permissions of a link around a MetaClass:

1. Access the UI access management pages and select **Access Object UIs**.
   ☛ *See Accessing the UI Access Management Pages (Permission).*
2. in the **Access Rights** field, use the drop-down menu to select the Set of UI access rights.
   ☛ *<HOPEX Default> enables to define default access permissions of each MetaClass, MetaAttribute, MetaAssociationEnd and tool.*

3. In the **MetaModel** field, select the MetaModel concerned.
   In the **MetaClass** frame, the listed MetaClasses are filtered according to the selected MetaModel.
4. In the **MetaClass** frame, select the MetaClass concerned.
5. In the toolbar of the **MetaAttributes/MetaAssociationEnds/Tools** frame, click **MetaAssociationEnd** .
6. Select the MetaAssociationEnd for which you want to modify link access permissions.
7. In the **Permission** field, enter the new value.

   ☛ *See MetaAssociationEnd access permissions.*



8. Press "Enter".
   The value of the link access permission is modified.

   ☛ *To return to the default value, enter the character *.*

   ☛ *To obtain information on inheritance of the value, enter the character ?.*

   See also Modifying access permissions on links around a MetaClass.

Modifying access permissions on links around a MetaClass

You can modify access permissions on:

- the link according to the MetaClass accessed via the link
- one of the MetaAttributes of the link
- one of the MetaClasses accessed via the link

```
Example: You can grant rights to connect (but not to create)
an IT Service to an Application via this same link.
```

To modify access permissions on links around a MetaClass:

1. Select the MetaAssociationEnd.

   ☛ *See Modifying access permissions of a link around a MetaClass, steps 1 to 6.*

2. In the menu bar of the **MetaAttributes of MetaAssociationEnds/ Slave MetaClasses/MetaAssociations**, click **MetaAttribute** , **MetaClass** , or **MetaAssociation** .

3. In the list, select the MetaAttribute, MetaClass or MetaAssociation concerned.
4. In the **Permission** field, modify the permission value.
   - ☛ *See MetaAttribute access permissions.*
   - ☛ *See MetaClass occurrence access permissions.*
5. Press "Enter".
   The value of the access permission is modified.
   - ☛ *To return to the default value, enter the character *.*
   - ☛ *To obtain information on origin of an inherited value, enter the character ?.*

Rules on permissions while aggregating Sets of UI access rights

When a **Set of UI access rights** uses one or several Sets of UI access rights, its permissions are defined by addition of permissions defined on the Sets of UI access rights it uses.

```
Example:

The Sets of UI access rights S1 and S2 are connected to the
Set of UI access rights S3 of the profile P3.

If the permission value on an object A of the Set of UI
access rights S1 is CR and the one of the Set of UI access
rights S2 is RUD, then this permission value on object A for
the Set of UI access rights S3 is CRUD.
```

Attention to default values

A permission value with * means that this value is the default permission value and that it has not been specifically defined. Only those values specifically defined are taken into account in aggregation.

```
Example:

The Sets of UI access rights S1 and S2 are connected to the
Set of UI access rights S3 of the profile P3.

If the permission value on an object A of the Set of UI
access rights S1 is *CRUD and the one of the Set of UI
access rights S2 is R, then this permission value on object
A for the Set of UI access rights S3 is R.
```

Generating a Report on Permissions by Profile

Generating a report on permissions (Administration Desktop)

In the Web Administration desktop, you can generate the **Profile Permissions comparison Report**, which enables to compare the permissions of several profiles.

Report content

All MetaClasses of the selected metamodel appear in the report.

For each MetaClass, the report displays:

- (in rows) all MetaClasses, MetaAttributes of MetaClasses, MetaAssociationEnds of MetaClasses.
- (in columns) permissions for all selected profiles.

To generate an instant report on profile permission comparison:

1. Connect to the **Administration** desktop with **HOPEX Administrator** profile.

   ☛ *See Connecting to the Administration Desktop.*

2. Access the **Profiles** management pages.

   ☛ *See Accessing the User Management Pages.*

3. In the list of profiles, select the profiles for which you want to compare the permissions.

   E.g.: EA Functional Administrator and Data Functional Administrator.

4. In the list toolbar, click **Instant Report**.
5. Select **Profile Permissions comparison Report**.
6. Click **OK**.
7. In the **Parameters** section, in the **Metamodel** pane, click **Connect** and select the Metamodel associated with the profiles you want to compare.

   E.g.: HOPEX IT Portfolio Management.

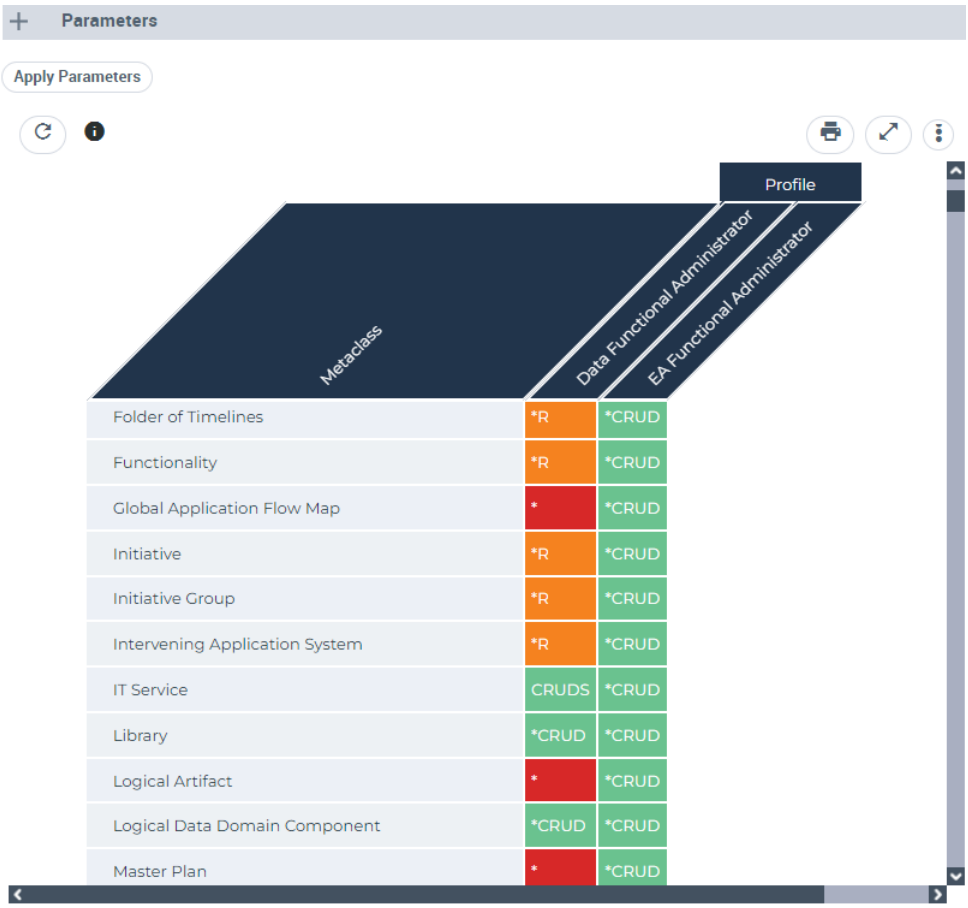
8. In the **Parameters** section, click ^ to reduce the section.
9. Click **Apply Parameters**.

   Attention: when the report has already been generated (the last generation date and time is indicated) with other

parameters, click ⟳ to update the report with the new parameters.

The report is generated as a matrix.

☛ *Generation can take some time, depending on the parameters you have selected.*



10. (If needed) Filter the report according to permission values.

`E.g.: you can display the rows with the "CRUD" value only.`

Generating a report on permissions (HOPEX Studio)

In **HOPEX Studio**, the following Report Templates enable to generate permission related reports:

- **Profile Permission report** enables to generate the detail of permissions for a given profile.
- **Profile Permissions comparison Report** enables to compare permissions of several profiles.
- **Workflow Permissions** enables to generate the detail of permissions for a given workflow.

Report content

All MetaClasses of the selected metamodel appear in the report.

For each MetaClass, the report displays:

- (in rows) all MetaAttributes, Tools, MetaAssociations (and MetaAttributes of MetaAssociations) of the MetaClass.
- (in columns) permissions for all selected profiles.

To generate a report on permissions:

1. In your **HOPEX Studio** desktop (**HOPEX Customizer** profile), access your reports.

   ☛ *See Creating a Report*

2. Click **New** .
3. (Optional) In the **Local Name** field, modify the default report name.
4. In the **Report Template** pane, select the report template concerned.

   ☺ *Use the table filtering tool to easily access the report type.*

5. Click **Next**.
6. Select the report parameters:
   - in the **Profile** pane, click **Connect** and select the profiles concerned.

     ☺ *For a faster result, do not select a large number of profiles.*

   - in the **MetaModel** pane, click **Connect** and select the metamodel concerned.

     ☛ *For the **Workflow Permissions** report template, in the **Workflow** field, click the arrow and select **Connect Worflow Definition**.*

7. Click **OK**.
   The report is generated as a matrix.

   ☛ *Generation can take some time, depending on the parameters you have selected.*

   E.g. the permission comparison report of **Application Portfolio Manager** and **ITPM Functional Administrator**, here

you can see the permissions of some of the MetaAttributes of **Application** MetaClass.

8. (If needed) Filter the report according to permission values.

Managing General UI Access

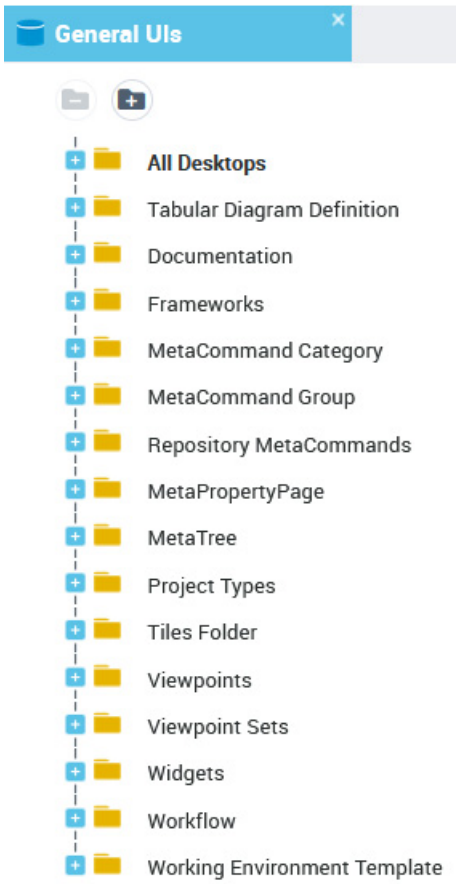
You can manage general UI access for a profile. General UIs are classified by category, like:

- desktop
- command category
- command group
- general command
- property page
- tree
- Working Environment Template (WET)

To manage general UI access:

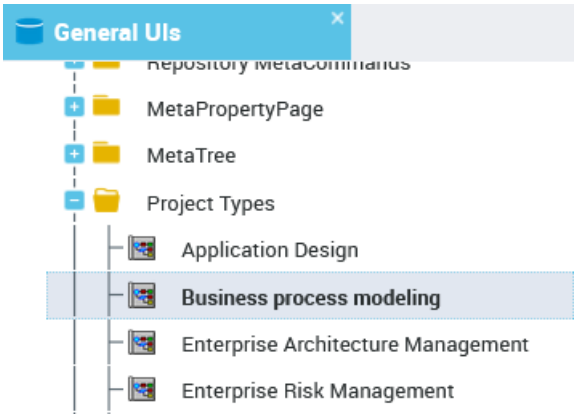
1. Access the UI access management pages and select **General UI Access**.

   ☛ *See Accessing the UI Access Management Pages (Permission).*

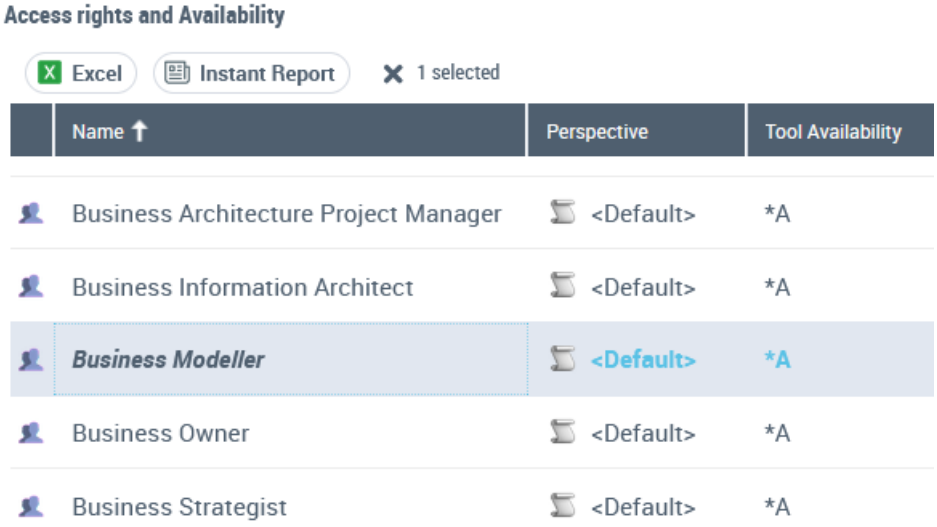


2. Expand the folder of the category concerned.

3. In the list, select the tool concerned.



4. In the **Access rights and Availability** pane, select the Set of UI access rights for which you want to modify access on the tool.
5. In the **Tool Availability** field, enter the availability value.



6. Press "Enter".
The value of tool availability is modified.

> ☛ *To return to the tool availability default value, enter the character *.*
>
> ☛ *To obtain information on origin of an inherited value, enter the character ?.*

SCHEDULING (SCHEDULER)

The **Scheduler** feature of **HOPEX** enables to create Triggers to schedule Job execution. The Trigger creation is performed in **HOPEX Administration** (Administration.exe) application only.

☛ *See HOPEX Administration > Managing the Scheduling (Scheduler) > Creating a Trigger))*

In your **HOPEX** desktop, some profiles (HOPEX Administrator, functional Administrator, HOPEX Customizer) give access to the scheduling list of Triggers (of Jobs).

The following points are covered here:

- ✓ Introduction to the Scheduler
- ✓ Managing Triggers
- ✓ Modifying a Trigger Scheduling

INTRODUCTION TO THE SCHEDULER

Concepts

The Scheduler feature enables to perform tasks defined by MEGA or by an 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).

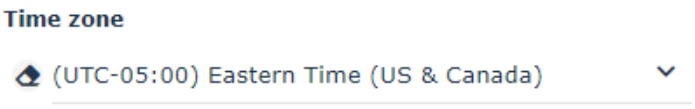
☛ *See Defining the Execution Time Zone.*

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.

   When you configure your Triggers, the execution scheduling is defined in this time zone if you select the **User** execution 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 Execution Time.*

MANAGING TRIGGERS

See:

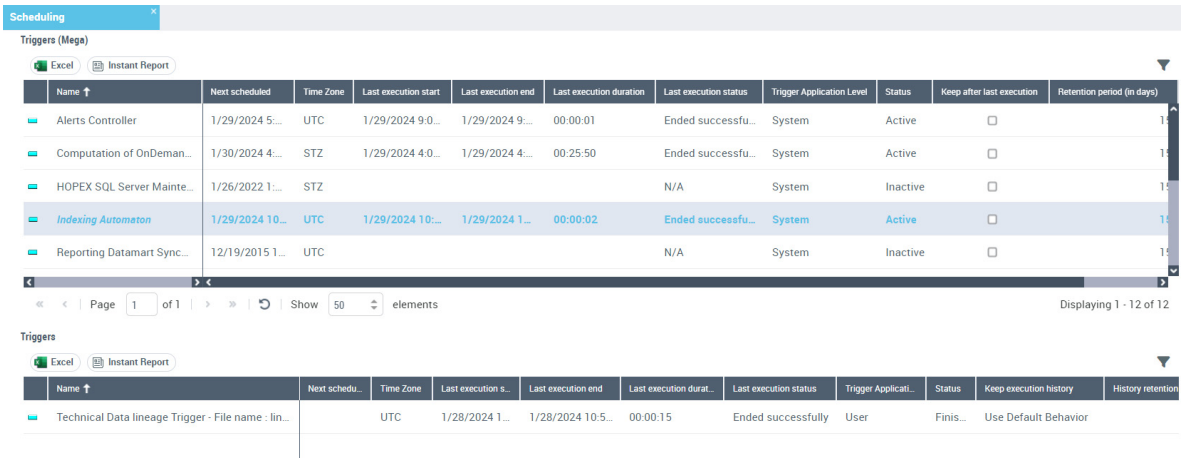
- Accessing Scheduled Triggers
- Managing a Trigger

Accessing Scheduled Triggers

☛ *For detailed information regarding Trigger creation, see HOPEX Administration > Creating a Trigger documentation.*

The Scheduling window displays the following tabs:

- **Triggers (Mega)**
  Triggers provided with HOPEX and available in all the installations. These Triggers are defined on the System repository.
- **Triggers**
  Triggers defined by the HOPEX administrator. These Triggers can be defined on a data repository or on the System repository.



For each scheduled Trigger, it indicates:

- its name
- its next execution date and time
- its time zone

  E.g.: UTC, <name of the user local time>, STZ (Server Time Zone).
- its last execution start/end/duration
- its status (active or inactive)
- if the trace of the trigger is kept after its deletion or not
- its retention period (in days)
- its deletion date

To access the Triggers:

1. Connect to **HOPEX** with one of the required profiles.

   E.g.: HOPEX Administrator, Functional administrator of <Name of the Solution>, HOPEX Customizer.
2. Depending on the desktop:
   - **Web Administration** desktop: select **Tools > Scheduling management > Scheduling**.
   - other desktops: select the **Main menu > Scheduling Management > Scheduling**.

Managing a Trigger

You can:

- update the Trigger scheduling

  ☛ *To modify the job execution dates, times, and frequencies, see Modifying 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.
- display the Trigger properties
  - The **Scheduling** page details the scheduling definition.
  - The **Next execution** page lists all the next executions of the Trigger.
  - The **Characteristics** page enables to keep the Trigger in the list after its last execution and to modify its retention period (by default 15 days).

To manage a Trigger:

1. Access the Trigger management.

   ☛ *See Accessing Scheduled Triggers.*

2. Right-click the Trigger concerned and select:
   - **Update Scheduling**

     ☛ *See Modifying a Trigger Scheduling.*
   - **Activate**/**Deactivate**
   - **Execute**
   - **Delete**
   - **Properties**

MODIFYING 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.*
- the date and time of its first execution
  - ☛ *In a recurrence case, the first execution date is not mandatory.*
  - ☛ *See Defining the First Execution Date of the Trigger.*
- its frequency
  The execution can be unique or recurrent.
  - ☛ *See Defining the Trigger Frequency.*

  If the execution is recurrent:
  - its execution time.
    - ☛ *See Defining the Trigger execution time.*
  - if needed, you can define a recurrence on the execution time, i.e. execute the Trigger several times the scheduled day.
    - ☛ *See Defining a time-based recurrence on the Trigger execution.*
  - the date of its last execution (defined or with no end)
    - ☛ *See Defining the Last Execution Date.*

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 Scheduled Triggers.*
2. Right-click the Trigger concerned and select **Update Scheduling**.
3. 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 First Execution Date of the Trigger

The first execution date of the Trigger can be:

- absolute

  E.g.: on the 04/18/2020 at 18:30:15.

- relative (relative to a reference date)

☛ *In a recurrence case, the first execution date is not mandatory.*

☛ *In a non recurrence case, the first execution date is the unique execution date.*

Defining the first execution date (or unique execution)

To define the first execution date of a Trigger:

1. Access the Triggers.

   ☛ *See Accessing Scheduled Triggers.*

2. Right-click the Trigger concerned and select **Update Scheduling**.
3. In the **Start** section:
   - Use the calendar of the **Start date (absolute)** field to select the first execution date of the Trigger.

     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.*

Defining a relative date for the first execution

You can define a relative date for the first execution, i.e. define the first execution date as:

- (by default) immediately after the Trigger creation, or
- at a later date:
  - a specific number of days after the reference date
  - a specific day of the week after the reference date
  - a specific day of the moth after the reference date

To define the first execution date of a Trigger:

1. Access the Triggers.

   ☛ *See Accessing Scheduled Triggers.*

2. Right-click the Trigger concerned and select **Update Scheduling**.
3. In the **Start** section, select **Relative Date**.
   By default **Reference date/time as soon as possible** is selected: the execution is triggered right after the Trigger creation.

4. To configure a later relative date, clear **Reference date/time as soon as possible**, then in the **Start date (relative)** click ··· and define:
   The **Day of relative date**:
   - In the **Days from reference**, enter the number of days after the reference date, or
   - Select the **Day of week** and use the drop-down list to select the chosen day, or

     `E.g.: Tuesday, the Trigger is executed on the first Tuesday following the reference date.`
   - Select the **Day of month** and use the drop-down list to select the day.

     `E.g.: 15th, the Trigger is executed on the 15th of the month following the reference date.`

   The **Month of relative date**:
   - In the **Months from reference**, enter the number of months after the reference date, or

     `E.g.: 2, the Trigger is executed a couple of months after the reference date.`
   - Select the **Month of year** and use the drop-down list to select the chosen month, or

     `E.g.: June, the Trigger is executed in June following the reference date.`

Defining the Trigger Frequency

A Trigger can be executed uniquely or on a regular basis.

Whatever the frequency chosen, you can perform a first execution as defined in the **Start** section.

Frequency:

- ***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 day of the week

    ```
    E.g.: Monday, Tuesday,..., Sunday
    ```

    You can select several days.
  - the frequency

    ```
    E.g.: every two weeks (N=2)
    ```
- ***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 execution frequency:

1. Access the Triggers.

   ☛ *See Accessing Scheduled Triggers.*
2. Right-click the Trigger concerned and select **Update Scheduling**.
3. In the **Date Recurrence** section, use the drop-down menu of the **Recurrence Type** field to select the frequency.

   ```
   Example: Daily, Monthly, Once, Weekly.
   ```
4. Configure the frequency.
5. (If you want to first execute the Trigger as defined in the **Start** section) Select **Execute at Start date time**.

Defining the Last Execution Date

By default, the Trigger scheduling is endless.

You can define the Trigger last execution date, via:

- an end date, or
- a defined repeat number

To define the Trigger last execution date:

1. Access the Triggers.

   ☛ *See Accessing Scheduled Triggers.*

2. Right-click the Trigger concerned and select **Update Scheduling**.
3. In the **Recurrence End** section, use the drop-down menu of the **Recurrence End Type** to select the end type.

   Example: End Date or Repeat Number.
4. (If you selected End Date) Define the last execution day and time.
   - Use the calendar of the **End date (absolute)** field to select the last execution date of the Trigger.
   - In the **End time** field, set the triggering time (UTC) 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.*

Defining the Execution Time

In case the **Recurrence Type** is "Daily", "Weekly", or "Monthly", you must define the Trigger execution time:

- once: you need to define the execution time only
- several times a day, you must define:
  - the scheduling period (in hours):
  - the start time
  - the end time

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.*

Defining the Trigger execution time

You can define a unique execution time each scheduled execution day.

To set the Trigger execution time:

1. Access the Triggers.

   ☛ *See Accessing Scheduled Triggers.*
2. Right-click the Trigger concerned and select **Update Scheduling**.
3. In the **Time scheduling (for date recurrence)** section:
   - in the **Scheduling type**, keep "Once".
   - in the **Single trigger time**, set the time at which you want to execute the Trigger.

     E.g.: 2:00:00, by default 04:00:00 (in the time zone defined).
4. Click **OK**.

5. Check the scheduling of your execution time.
   - Right-click the Trigger and select **Properties**.
   - Display the **Scheduling** > **Next Executions** page.

   The **Execution Date & Time** table indicates the first execution date and time and the following ones with their corresponding local time.

   ☛ *To define your local time, see Defining your Local Time.*

Defining a time-based recurrence on the Trigger execution

You can schedule the Trigger execution several times each scheduled execution day. Then, you must define:

- the scheduling period (in hours):
  Default period: every 4 hours (04:00:00) each scheduled day.
- the start time of the time-based scheduling
- the end time of the time-based scheduling

To define a time-based recurrence on the Trigger execution:

1. Access the Triggers.

   ☛ *See Accessing Scheduled Triggers.*
2. Right-click the Trigger concerned and select **Update Scheduling**.
3. In the **Time scheduling (for date recurrence)** section, use the drop-down menu of **Scheduling type** field to select "recurrent".
4. Define the recurrence (period, start time and end time of the time-based scheduling):
   - **Scheduling period** (hh:mm:ss format)
   - **Scheduling start time** (hh:mm:ss format)
   - **Scheduling end time** (hh:mm:ss format)

   ```
   E.g.: schedule the Trigger every 30 minutes from 6am to
   10am.
   ```
5. Click **OK**.
6. Check your scheduling configuration regarding the execution time recurrence:
   - Right-click the Trigger and select **Properties**.
   - In the **Scheduling** tab, select the **Next Executions** sub-tab.

   The **Execution Date & Time** table indicates the first execution date and time and the following ones with their corresponding local time.

   ☛ *To define your local time, see Defining your Local Time.*

7

OPTIONS

This chapter presents the various tools and options used to configure and customize **HOPEX**.

The following points are covered here:

INTRODUCTION TO OPTIONS

Option Overview

In the **Administration** desktop, **HOPEX** options can be configured at the following levels:

- environment
- profile
- user

☛ ***Site*** *level options can be modified in the* ***Administration*** *(Windows Front-End) application.*

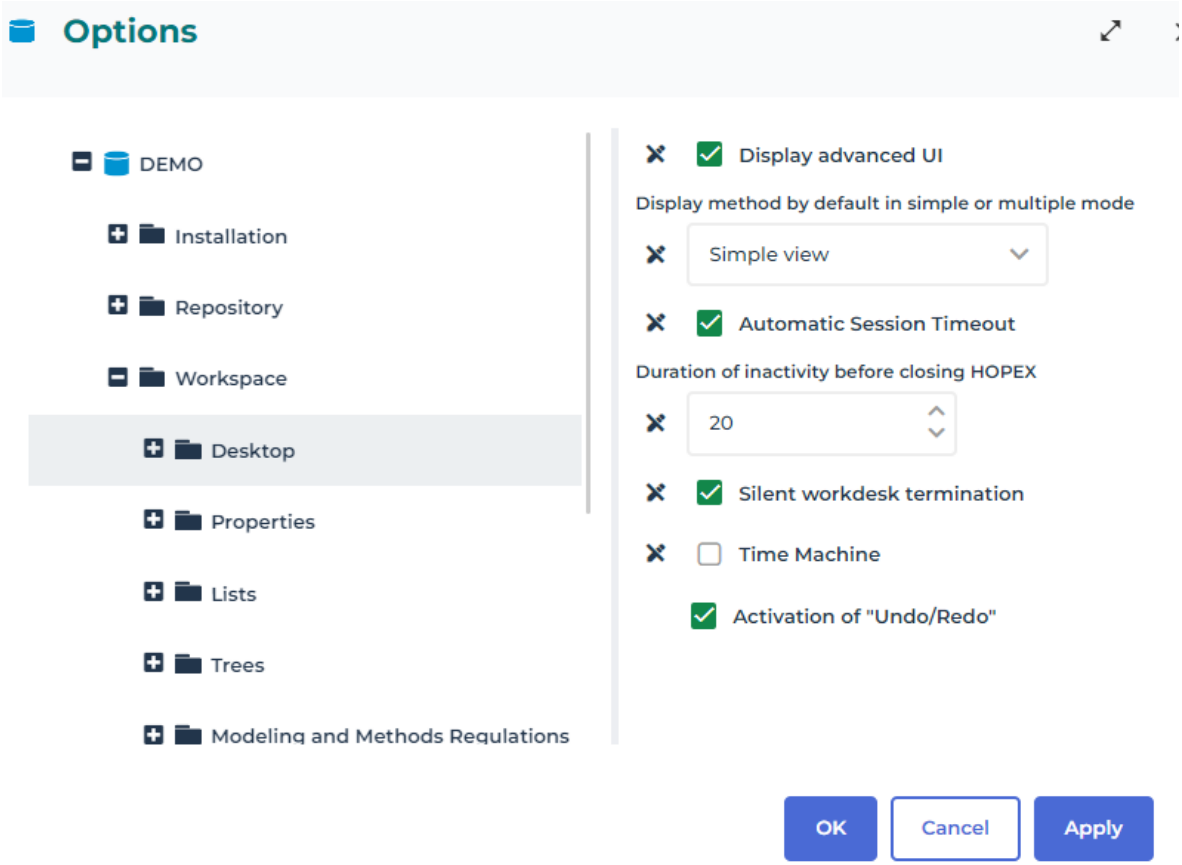
Option levels are governed by an inheritance mechanism.

☛ *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.

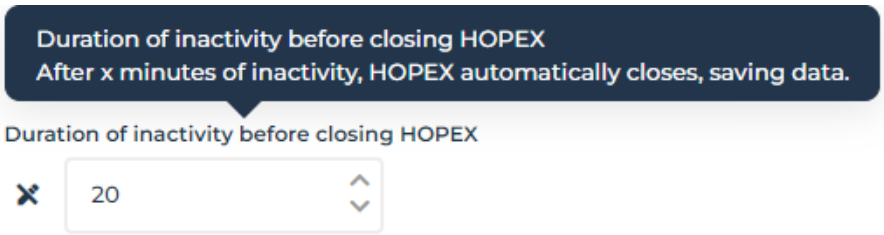
☛ *See Option Groups.*

The right pane enables configuration of the options corresponding to the group selected in the left pane.

Options vary depending on products you have available.

For more details on an option:

- Hold the mouse over the option to display its description in the tooltip.



When the user has a private workspace in progress, you cannot modify his/her options from the **Administration** desktop.

MANAGING OPTIONS

Modifying Options

You can modify options at the following levels:

- environment
- profile (which groups a configuration common to several users)
- 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 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 Connecting to the Administration Desktop.*
2. In the edit area, click **Environment Options**.
   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 profile level

To modify options at the profile level from the **Administration** desktop:

1. Access the Profiles management pages.
   ☛ *See Accessing the User Management Pages.*
2. In the edit area, select the profile concerned.
3. Click **Options**.
   The profile 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.

   Options are modified at profile level.

Modifying options at user level

☛ *A user can modify some of his/her options from the toolbar on his/her desktop Toolbar.*

To modify the options of a user from the **Administration** desktop:

1. Access the user management page.
   ☛ *See Connecting to the Administration Desktop.*
2. Select a **Persons** sub-folder.
3. In the edit area, select the person concerned.
4. Click **Options**.
   The person's Options window opens.
5. Modify the option concerned.
6. 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 user level.

Option Inheritance

Option levels are governed by an inheritance mechanism. An option inherits a value defined at a higher level:

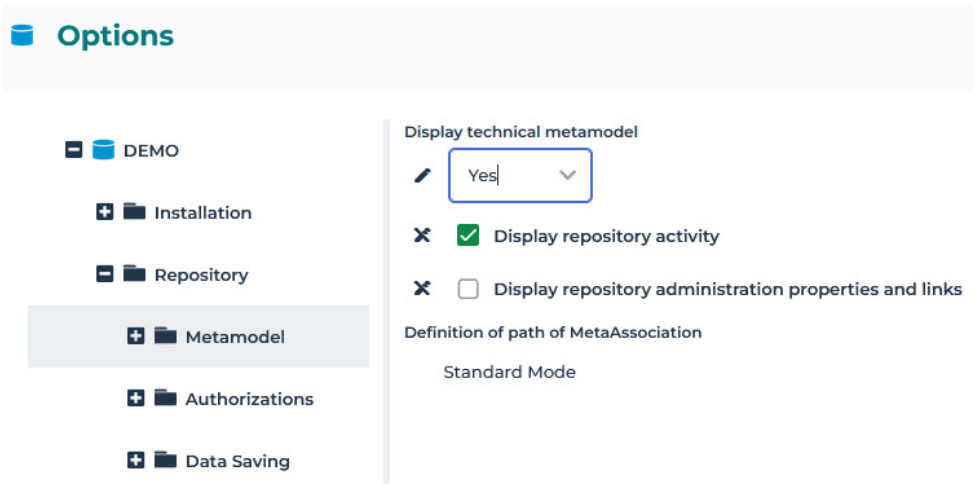
- A user inherits the option values defined at the connection profile level.
- A profile inherits the option values defined at the environment level.
- An environment inherits options defined at the site level.

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.

Reinitializing the value of an option

To reinitialize the value of an option:

1. Access the options.

   ☛ *See Modifying Options.*
2. Click / .

   The value of the option is reinitialized and the icon changes to / .

Controlling 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)
- customization
- 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
- logging

Workspace

Options linked to the user workspace:

- desktop
- properties
- trees
- modeling and method 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**

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 regarding Technical Support access.

Debugging

Options regarding debugging.

Available for HOPEX administrator and functional administrator profiles.

INSTALLATION OPTIONS RELATED TO WEB APPLICATIONS

For detailed information regarding installation options related to Web applications, see the **HOPEX Web Front-End Installation Guide**.

> ☛ *To manage languages in Web applications, see Managing Languages in Web Applications.*

Installation options are not available in your **HOPEX Administration** desktop. They are defined at **HOPEX** site level in **HOPEX Administration** application.

Specifying the Web Applications Access Path

The Web application access path is defined at **HOPEX** site level and cannot be defined from your **HOPEX Administration** desktop.

To specify the Web applications access path:

1. Start **HOPEX Administration**.
2. Right-click the site name and select **Options > Modify**.
   The site options window opens.
3. In the **Options** tree, select **Installation > Web Application**.
4. In the right pane, specify the **Web Application Path** option.

   Example: http://<Server Name>/HOPEX

Specifying SMTP Configuration

The SMTP configuration is defined at **HOPEX** site level and cannot be performed in your **HOPEX Administration** desktop.

You must define the **Electronic mail** options:

- **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.

To specify SMTP configuration:

1. Connect to **HOPEX Administration**.

   ☛ *See **HOPEX Administration > Accessing HOPEX Administration** documentation.*
2. Right-click the site name and select **Options > Modify**.
   The site options window opens.
3. In the **Options** tree, expand the **Installation** folder and select **Electronic Mail**.
4. In the right pane, specify the following options:
   - **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
5. Restart HAS instance:
   - Connect to the **HOPEX Application Server** console.
   - In the navigation menus, select **Installation > HAS Settings**
   - In the right pane, click Save.

   A dialog box alerts you that HAS instance and all its related nodes are going to be restarted and that any connected users will be disconnected.
   - Click **I understand the impacts, restart**.

MANAGING LANGUAGES IN WEB APPLICATIONS

In Web applications, you can modify:

- the interface language
- the data language

On his/her side each user can customize his/her desktop:

- modify his/her interface language

  ☛ *See Modifying the Interface Language*

- switch to another data language

  ☛ *See Modifying the 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 the 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 **HAS console**, stop and start **HOPEX Core Back-End** module.

   💣 **This action disconnects users.**

   ☛ *In **HAS console**: **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 the 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/time format you want to be customized:

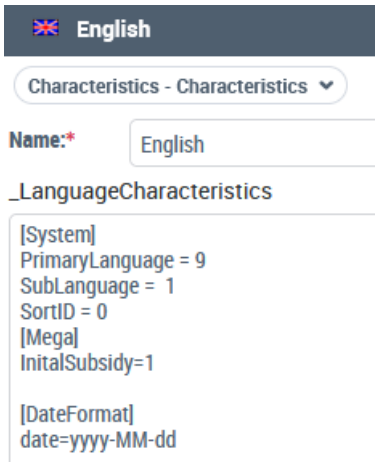
   ```
   [DateFormat]
   Date=<date format>
   time=<time format>
   ```

   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 jul 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, 22
yy	The year with two digits 09, 22
yyyy	The year with four digits 2022

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 **Authorize 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 MEGA 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 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".
   ```

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 and permissions.

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, 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 access — General UI access defines if tools are available or not. By default, general UI accesses have value *A (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 access Object UI access defines user rights on creation, reading, update, and deletion on these objects and their tools. By default, object UI accesses have value *CRUD (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 (Web Front-End specific) 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 MEGA 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 session 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.