MEGA Administration-Supervisor

Web Administrator Guide

HOPEX V2

ABOUT HOPEX ADMINISTRATION

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

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

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**, **HOPEX Power Supervisor**, or **HOPEX Collaboration Manager**). These are indicated by a note.

Presentation of this Guide

This guide concerns the administration of **HOPEX** from the **HOPEX Administration** desktop (Web Front-End).

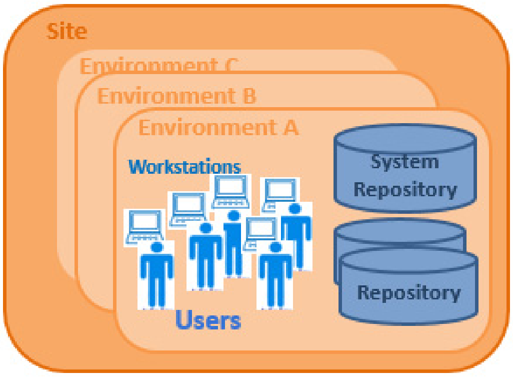
> ☛ *To perform **HOPEX** administration tasks from the **HOPEX Administration** application (Windows Front-End), see the HOPEX Administration - Supervisor guide.*

The following points are covered here:

- "Web Administration Desktop", page 5: access to and description of the **HOPEX** Administration desktop.
- "Managing Users", page 15: creation of users, user groups and their profiles.
- "Managing workspaces", page 117: principle of private workspaces, dispatch and refresh private workspaces, and lock management.
- "Managing objects", page 147: 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", page 307: description of the syntax used in command files.
- "Managing Options", page 169: access to options, user level options and language management.
- "Glossary", page 181: 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. A user:
  - has a specific workspace in each repository.
  - has a specific configuration and is authorized to access specific product functions and repositories in the environment.

WEB ADMINISTRATION DESKTOP

The 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, LDAP servers), repositories (workspaces, locks, repository, repository snapshots) and permissions (UI accesses).

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.

The points covered here are:

CONNECTING TO THE ADMINISTRATION DESKTOP

From the **Administration** desktop, you can in particular perform the following administration operations:

- user management
- permission management (UI access)
- repository management

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 "The Administration profiles provided", page 26.*

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

To connect to the **Administration** desktop:

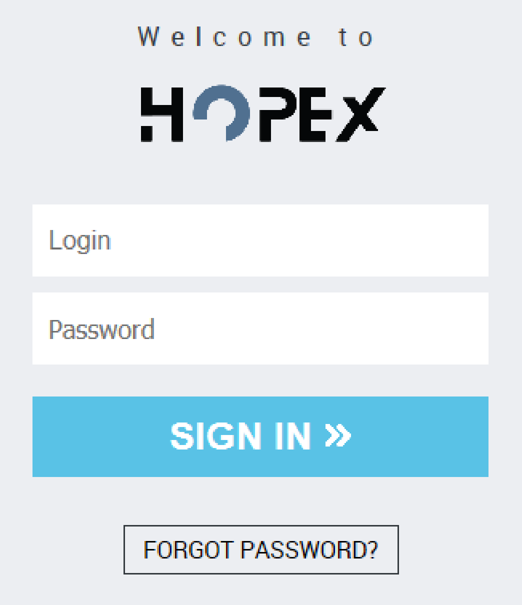
1. Start the **HOPEX** application using its HTTP address.

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

   The connection page appears.

2. In the **Login** field, enter your identifier.

   `Example: Mega is the login of the` **`HOPEX`** `administrator Mega.`



3. (If you have a password) In the **Password** field, enter your password.

   > ☛ *If you have lost your password, click **Forgot Password**, see "Reinitializing Your Password", page 9.*

4. In the drop-down menu for environments, select your work environment.

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

5. Click **SIGN IN**.
   When you have been authenticated, a new dialog box appears.
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. 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.*

8. 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 "The Administration profiles provided", page 26*

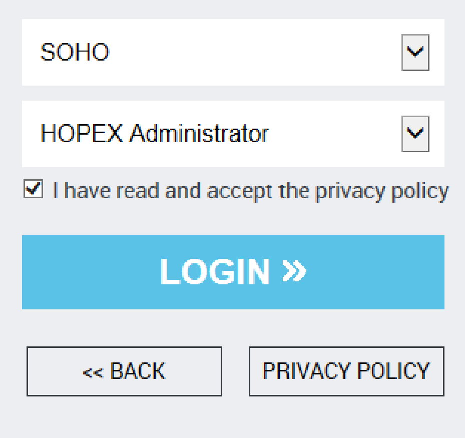
   > ☛ *If you have only one profile (administration), this is automatically taken into account and the profile selection field does not appear.*

9. In the drop-down menu for applications, select the **Administration (Web Front-End)** application.

   > ☛ *If you can access only the **Administration (Web Front-End)** application with the profile selected, this is automatically taken into account and the application selection field does not appear.*

10. Click **Privacy Policy**, read the confidentiality policy, then select **I have read and accept the privacy policy**.
    The **Login** 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.*



SOHO

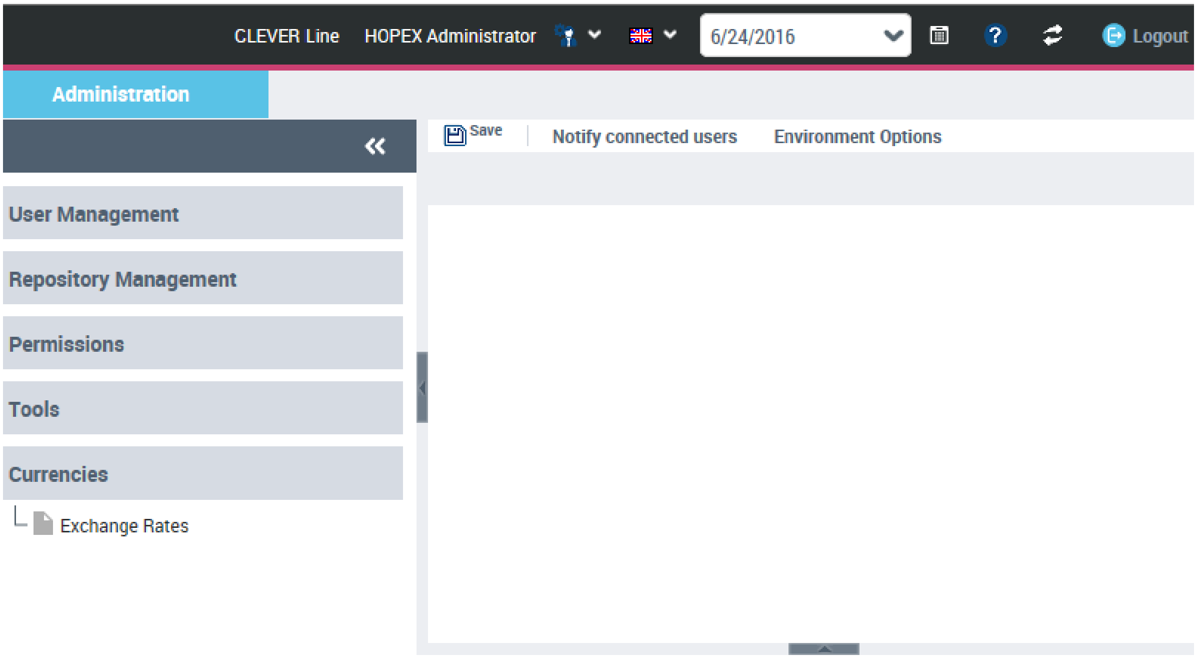
HOPEX Administrator

☑ I have read and accept the privacy policy

11. Click **LOGIN**.

☛ *Click **BACK** if you want to return to the authentication dialog box.*

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



☛ *See "Administration Desktop Description", page 10.*

REINITIALIZING YOUR PASSWORD

If you have lost your password, you can reinitialize it (MEGA authentication case).

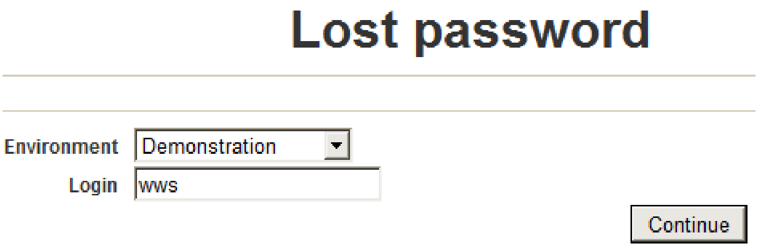
☛ *See "Authentication mode", page 38.*

To reinitialize your password:

1. Open the connection page.

   ☛ *See "Connecting to the Administration Desktop", page 6.*

2. Click **Forgot Password**.
   The **Lost password** page appears.



Lost password

Environment: Demonstration

Login: wws

3. In the **Environment** field, select your work environment.

   ☛ *If you have access to only one environment, this is automatically selected and this field does not appear.*

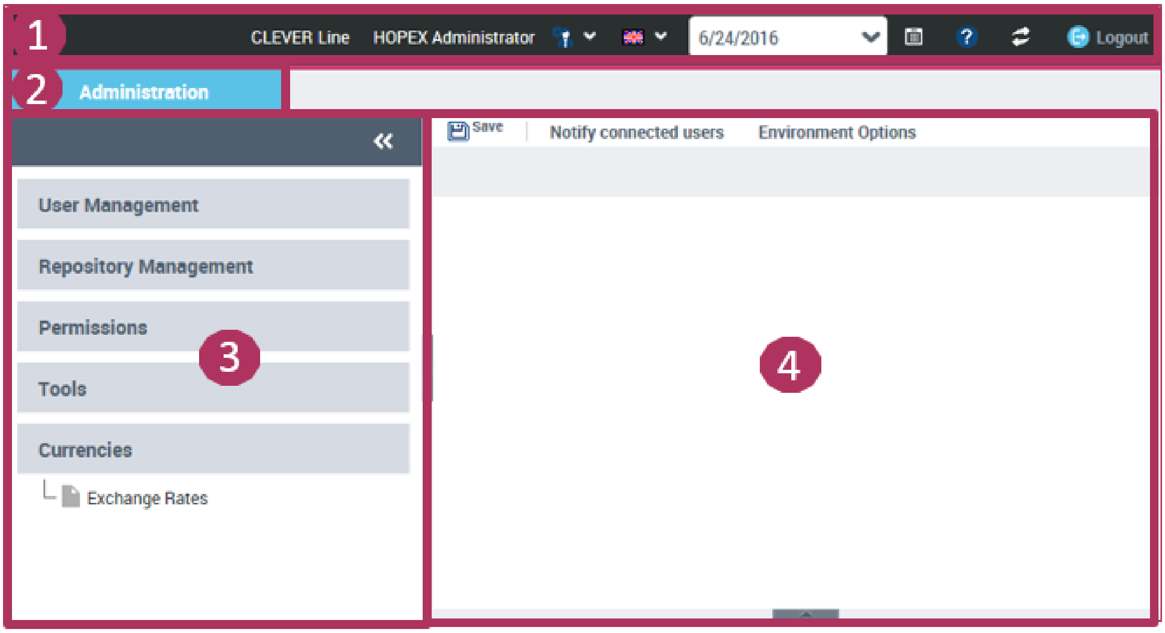
4. In the **Login** field, enter your login.
5. Click **Continue**.
6. Answer the security question.
7. Click **Reinitialize**.
   An e-mail containing a link with limited validity period is sent to you.
8. Click this link.
   The **Modify Password** page appears.
9. Enter your password and answer the security question.

   ☛ *By default, a password must contain between 8 and 16 characters, with at least one letter, at least one digit and at least one special character, see "Modifying password definition rules", page 113*

10. Click **Apply**.

Administration Desktop Description

To access the **Administration** desktop, see "Connecting to the Administration Desktop", page 6.

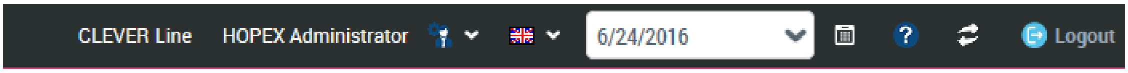


1, Toolbar, 2: Administration tab, 3: Navigation panes, 4: Edit area

The **Administration** desktop includes:

- a toolbar.
  - ☛ *See "Toolbar", page 10.*
- an **Administration** tab that contains panes and trees to select the objects to manage.
  - ☛ *See "Navigation panes and trees", page 12.*
- an edit area to manage objects.
  - ☛ *See "Edit area", page 14.*

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:

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

    ☛ *Your password must contain between 8 and 16 characters, with at least one letter, at least one figure and at least one special character.*

  - modify your options

    ☛ *For information on options available at user level, see "Available Option Groups (User Level)", page 175.*

  - modify the theme of your desktop

    ☛ *The theme used in the Web applications also defines the theme used in the reports. To customize reports, see the **HOPEX Common Features** guide - Customizing Reports chapter.*

  - manage your alerts

    ☛ *See the **HOPEX Common Features** guide - Communicating in **HOPEX** chapter.*

  - obtain information on your licenses
  - diagnose the installation

    ☛ *This information simplifies error diagnostics. It can help explain application slow response time.*

  - download the HOPEX system information report

    ☛ *See "System Information Access Option (Web user)", page 176.*

  - reinitialize your personal parameters
  - access the documentation
- modify the interface data language

  ☛ *To manage languages, see "Managing Languages in Web Applications", page 178.*

- display data as it was at a prior date, with the **Time Machine**

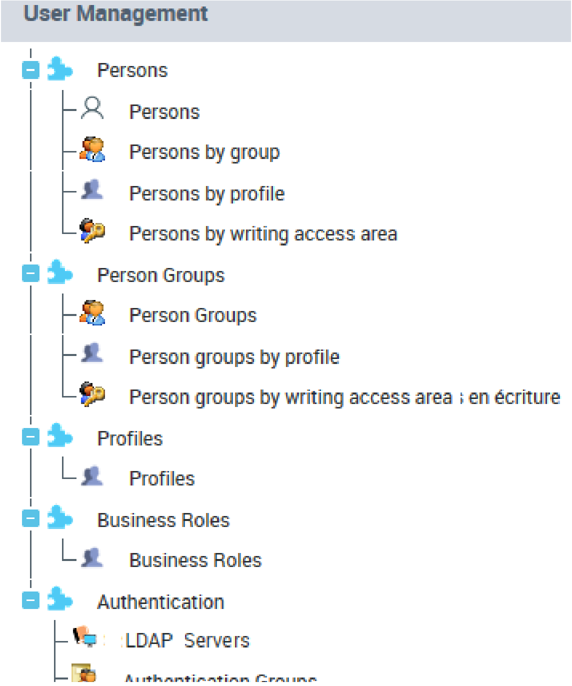
  17/06/2016

- 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*:



User Management

- Persons
  - Persons
  - Persons by group
  - Persons by profile
  - Persons by writing access area
- Person Groups
  - Person Groups
  - Person groups by profile
  - Person groups by writing access area ; en écriture
- Profiles
  - Profiles
- Business Roles
  - Business Roles
- Authentication
  - LDAP Servers
  - Authentication Groups

- the *persons*

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

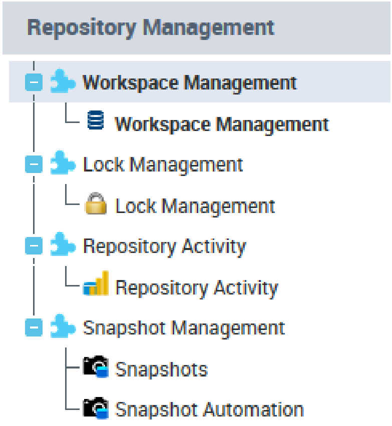
- the *person groups*

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

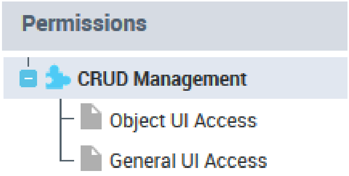
- the *profiles*
- the *business roles*
- the *LDAP servers*

  ☛ *The **LDAP Servers** folder is available only if you are connected with a user with the HOPEX Administrator profile (example: **Administrator**), see "The Administration profiles provided", page 26* *and that LDAP authentication is the user default authentication mode, see "Defining default authentication mode to LDAP", page 103.*

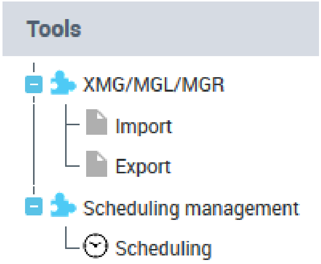
- the **Repository Management** pane to manage the *workspaces*, the *locks*, the *repository* and the *snapshots*



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



- the **Tools** pane to:
  - import or export objects with the Excel import/export wizard
  - import or export objects in different formats
  - import Visio diagrams
  - manage scheduling



- **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:

- save your updates (**Save** 💾)
- notify connected users by e-mail (**Notify connected users**)
- manage the environment options (**Environment Options**)

MANAGING USERS

The **Administration** desktop is equipped with tools required for user management.

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:

Actions to be Performed 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", page 16
- "Compulsory Actions to be Performed to Define a User", page 17
- "Compulsory Actions to be Performed to Define a User Group", page 18
- "Optional Actions to be Performed to Define a User", page 18
- "Other Actions to Set or Manage a User", page 19
- "Checking the Configuration of Persons", page 19

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 Users", page 81.*

  ☛ *See "Creating a Person Group", page 91.*

To connect to **HOPEX** a user select 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 Login Characteristics", page 79), the products accessible to this user are at the intersection of values of the Command Line attribute of the user login and profile.

- the applications and the desktops which the user is going to access.

  ☛ *See "Connection schema: Person - Profile - Application", page 21.*

  ☛ *See "Connection schema: Person - Profile - Application - Desktops", page 22.*

- the UI access rights (permissions) of the user

Assigning a profile to a person defines:

> ☛ *See "Assigning a Profile to a Person", page 56.*

- 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 be Performed to Define a User

To create a user who can connect to **HOPEX** you must:

- define the name of the person

  > ☛ *See "Creating Users", page 81.*

- define the login of the user

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

  > ☛ *See "Defining the Login of a Person", page 86.*

  > ☛ *The login of the user is created automatically on creation of the person, see "Creating Users", page 81 (If necessary, see "Creating the Login of a Person", page 85).*

  > ☛ *The login status must be active so the person can connect, see "Status (Login)", page 38.*

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

  > ☛ *See "Creating Users", page 81.*

  > ☛ *See "Defining a Person", page 83.*

  > ☛ *The e-mail address is necessary, for example, for distributing documents, receiving notifications and questionnaires, or when a Web user lost his/her password.*

- assign a profile to a 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", page 56.*

Compulsory Actions to be Performed 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", page 91.*

- 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 created automatically on creation of the person group, see "Creating a Person Group", page 91.*

  ☛ *See "Defining the Login of a Person Group", page 97.*

- 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 her/him to the profiles assigned to the person group.*

  ☛ *See "Assigning a profile to a person group", page 58.*

  ☛ *See "Performing a mass assignment of profiles to a person group", page 59.*

Optional Actions to be Performed to Define a User

According to the selected options you must:

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

  ☛ *The e-mail address is necessary, for example, for distributing documents, receiving notifications and questionnaires, or when a Web user lost his/her password.*

  ☛ *See "Defining a Person", page 83.*

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

  ☛ *See "Defining a Person", page 83.*

  ☛ *See "Connecting a Person to a Writing Access Area", page 88.*

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

  ☛ *See "Defining a Person", page 83.*

  ☛ *See "Connecting a Person to a Reading Access Area", page 89.*

- define if the person belongs to a person group.

  ☛ *See "Defining a Person", page 83.*

Other Actions to Set or Manage a User

You can:

- define the telephone number and initials of the person

  ☛ *See "Defining a Person", page 83.*

- define the data language of the Web user

  ☛ *See "Defining a Person", page 83.*

- 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", page 86.*

  ☛ *See "Configuring a Profile", page 52.*

- modify user authentication mode

  ☛ *See "Defining the Login of a Person", page 86.*

- make the user inactive.

  ☛ *See "Defining the Login of a Person", page 86.*

  ☛ *See "Preventing User Connection", page 89.*

Checking the Configuration of Persons

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", page 69.*

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", page 20
- "Connection schema: Person - Profile - Application", page 21
- "Connection schema: Person - Profile - Application - Desktops", page 22
- "Connection schema: Person - Profile - Application - Specific Desktops", page 24
- "The Administration profiles provided", page 26
- "Profile Properties", page 29

Description of a profile

The description of a profile includes:

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

☛ *See "Profile Properties", page 29.*

Definition of the profile

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

Example: Application Portfolio Manager, Enterprise Architect).

The profile defines:

- the applications and the desktops which the user is going to access.

  ☛ *See "Connection schema: Person - Profile - Application", page 21.*

  ☛ *See "Connection schema: Person - Profile - Application - Desktops", page 22.*

  ☛ *See "Defining applications accessible to profile users", page 53* and *"Defining application desktops accessible to profile users", page 54.*

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

  ☛ *See "Managing UI Access", page 235.*

- access rights restricted to certain products

  ☛ *See "Products accessible on the license (Command Line)", page 29.*

  💣 **If a user already has restricted access rights to products (see "Viewing Login Characteristics", page 79), the products accessible to this user are at the intersection of values of the Command Line attribute of the user login and profile.**

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:

☛ *See "Assigning a business role to a person", page 65.*

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

Connection schema: Person - Profile - Application

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

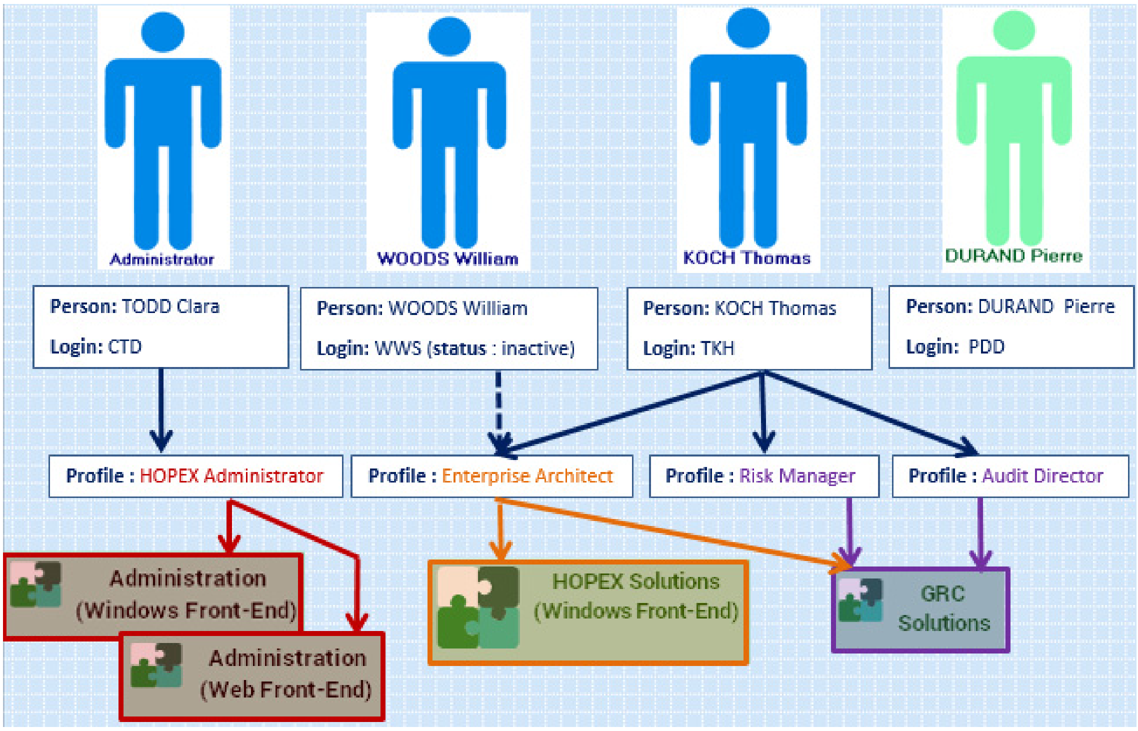
- a login

  ☛ *See "Creating Users", page 81.*

  ☛ *The login status must be active so the person can connect, see "Status (Login)", page 38.*

- at least one profile.

  ☛ *See "Assigning a Profile to a Person", page 56.*



In the above 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 Solutions (Windows Front-End)** or **GRC Solutions** applications.
- 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**.

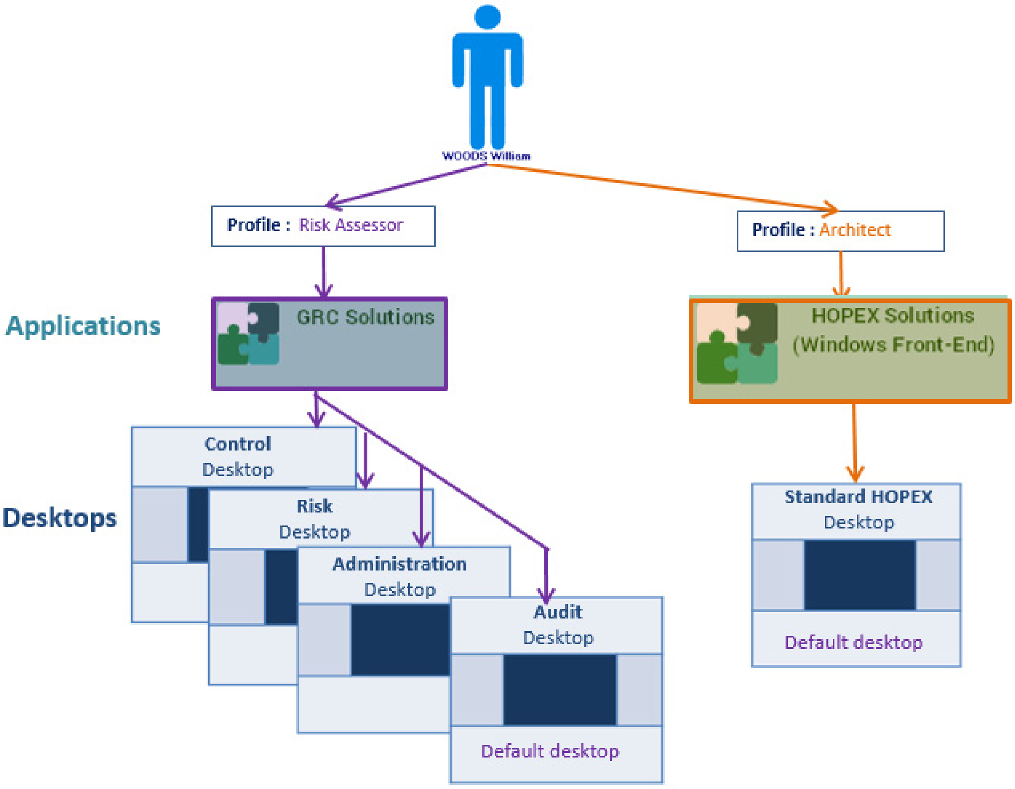
Connection schema: Person - Profile - Application - Desktops

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 supplied by **MEGA**, **MEGA** recommends you create a new profile; see "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50.*

☛ *To enable access to only certain desktops of the application, see "Connection schema: Person - Profile - Application - Specific Desktops", page 24.*



Example:

The **GRC Solutions** application is linked to the **Risk Assessor** profile and the **HOPEX Solutions (Windows Front-End)** application is linked to the **Architect** profile.

No desktops of the **GRC Solutions** or **HOPEX Solutions (Windows Front-End)** application are directly linked to the **Risk Assessor** and **Architect** profiles.

The user William WOODS, who has the **Risk Assessor** and **Architect** profiles, has access to all the **GRC Solutions** and **HOPEX Solutions (Windows Front-End)** applications.

Connection schema: Person - Profile - Application - Specific Desktops

A user can connect to applications 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:

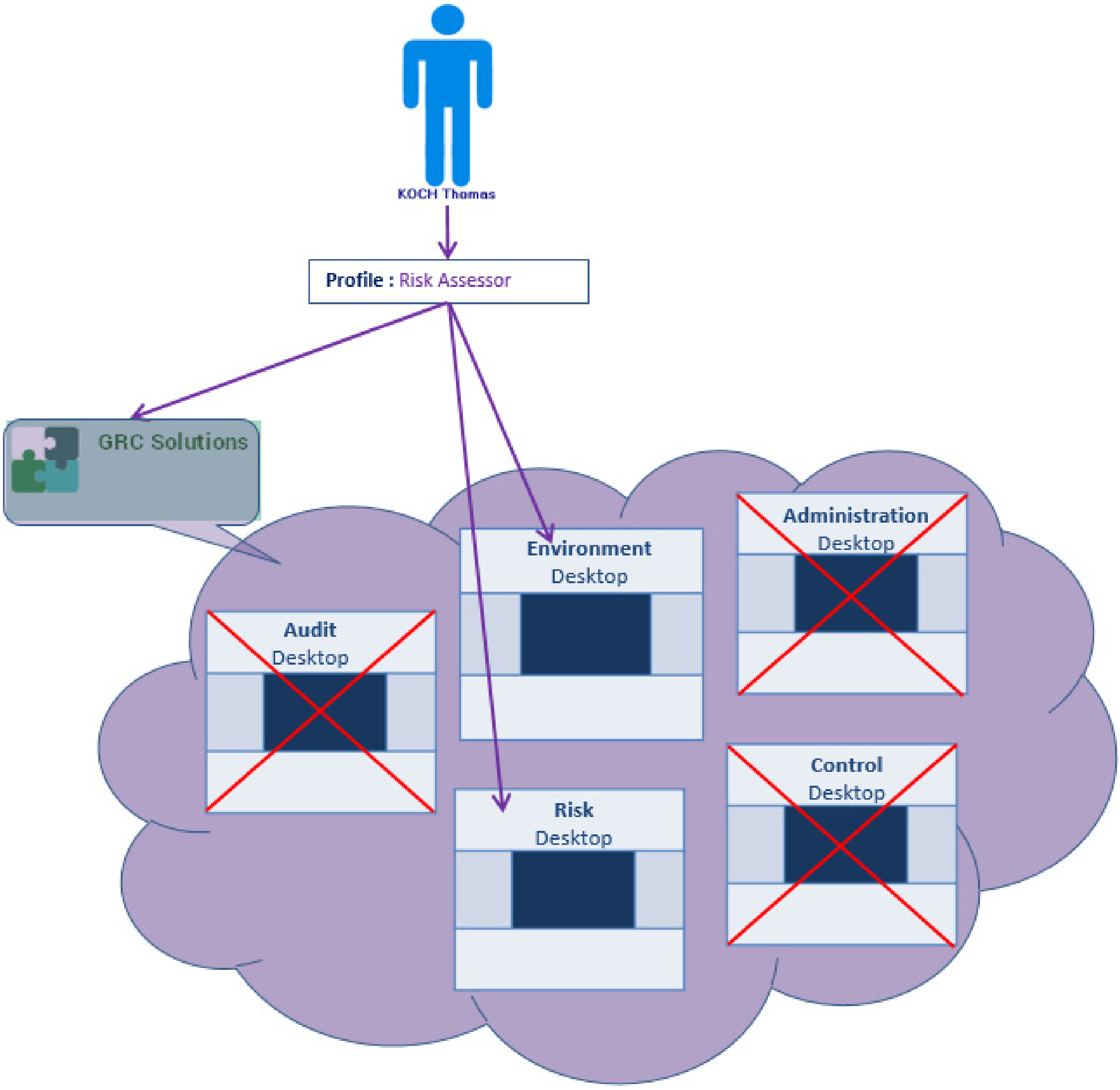
> ☛ *To modify a profile delivered by* ***MEGA****, you must have rights to modify* ***HOPEX*** *data. Alternatively, you can create a new profile, see "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50.*

- the application containing the desktops.

> ☛ *See "Defining applications accessible to profile users", page 53.*

- the desktops to which you want users of the profile to connect.
  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 application desktops accessible to profile users", page 54.*



Example:

The **Risk Assessor** profile is connected:

- to the **GRC Solutions** application which contains in particular the "Audit", "Environment" and "Administration" desktops.

- to the "Risk" and "Environment" desktops of the "GRC Solutions" application.

User Thomas KOCH with the **Risk Assessor** profile can connect only to the "Risk" and "Environment" desktops of the **GRC Solutions** application. The "Audit", "Control" and "Administration" desktops are not authorized.

The Administration profiles provided

Administration profiles are supplied 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", page 26.*
  - **HOPEX Administrator - Production**

    ☛ *See "HOPEX Administrator - Production profile", page 27.*
- Administration (Web Front-End), with exclusive access to the **Web Administration** desktop:
  User Management Web Administrator

  ☛ *See "User Management Web Administrator profile", page 28.*
- functional Administration (Web Front-End), with access to the **Web Administration** desktop and to Solution-specific desktops:
  <Solution name> functional Administrator

  Example: **ITPM functional Administrator** gives access to Environment, ITPM, and Administration desktops.

  ☛ *See "Functional Administrator profile of a Solution", page 28.*

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

☛ *See "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50 and "Configuring a Profile", page 52.*

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 - Supervisor guide.*

- **Profiles**

  ☛ *See "Managing Profiles", page 48.*

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

  ☛ *See "Creating and Managing Users", page 81.*

- *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", page 91.*

- **Business Roles**

  ☛ *See "Managing Business Roles", page 61.*

- **Permissions**

  ☛ *See "Managing UI Access (Permissions)", page 233.*

- an LDAP server

  ☛ *Available if the default authentication mode is set to LDAP, see "Defining Default Authentication Mode", page 102.*

  ☛ *See "LDAP Authentication", page 104.*

It also allows to perform tasks linked to:

- **Repository management**:
  - workspace management

    ☛ *See "Managing workspaces", page 117.*

  - repository activity management

    ☛ *See "Managing Updates", page 138.*

  - lock management

    ☛ *See "Managing locks", page 142.*

  - snapshot management

    ☛ *To create a repository snapshot, see the **HOPEX Collaboration Manager - Repository Snapshots** guide.*

- **Tools** such as:
  - XMG/MGL/MGR file import/export

    ☛ *See "Importing a command file in HOPEX", page 148.*

    ☛ *See "Exporting Objects", page 150.*

  - Scheduler use

    ☛ *See **HOPEX Power Studio - Scheduler** guide.*

HOPEX Administrator - Production profile

The **HOPEX Administrator - Production** profile is the equivalent of the **HOPEX Administrator** profile without permission management rights.

User Management Web Administrator profile

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

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

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

  ☛ *See "Creating and Managing Users", page 81.*

- *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", page 91.*

- **Business Roles**

  ☛ *See "Managing Business Roles", page 61.*

It also gives access to management of:

- **LDAP servers**

  ☛ *Available if the default authentication mode is set to LDAP, see "Defining Default Authentication Mode", page 102.*

  ☛ *See "LDAP Authentication", page 104.*

- **Locks**.

  ☛ *See "Managing locks", page 142.*

Functional Administrator profile of a Solution

Each **<Solution name> functional Administrator** gives access to the Administration desktop and to Solution-specific desktops.

From an administration point of view, the **<Solution name> Functional Administrator** profile allows, in particular, to manage:

- **Profiles**

  ☛ *See "Managing Profiles", page 48.*

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

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

  ☛ *See "Creating and Managing Users", page 81.*

- *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", page 91.*

- **Business Roles**

  ☛ *See "Managing Business Roles", page 61.*

It also gives access to:

- Scheduler use.

  ☛ *See **HOPEX Power Studio - Scheduler** guide.*

- **LDAP server** management.

  ☛ *Available if the default authentication mode is set to LDAP, see "Defining Default Authentication Mode", page 102.*

  ☛ *See "LDAP Authentication", page 104.*

Profile Properties

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

☛ *See "Introduction to Profile Management", page 20.*

☛ *To assign a profile to a person or a person group, see "Assigning a Profile to a Person", page 56 and "Assigning a profile to a person group", page 58.*

☛ *To manage profiles, see "Managing Profiles", page 48.*

Name

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

Products accessible on the license (Command Line)

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 found out the product code, see on line documentation: **Concepts > Products**.*

💣 **If a user already has access rights restricted by the Command Line attribute on his/her Login (see "Viewing Login Characteristics", page 79), 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 products for which he/she 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.***

Assignable

The **Assignable** attribute defines if the profile is assignable to a Login or not. Certain profiles are created to aggregate other profiles.

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

☛ *The default value is "No".*

Administrator profile

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

- grant administrator profile 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".

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 an Existing Profile / Creating a Profile from an Existing Profile", page 50.*

- "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.

_GUIName

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

MetaPicture

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

Working Environment Template

The working environment template defines the appearance of the desktop.

Profile used

The **Profile used** page contains the profiles used to define the current profile by aggregation of these profiles.

☛ *See "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50.*

Persons and Person Groups

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

Available applications

The **Available Applications** page is used to define the applications to which the current profile gives access.

☛ *See "Defining applications accessible to profile users", page 53.*

Available desktops

The **Available Desktops** page is used to define a **Working Environment Template**, which gives access to a specific desktop.

In cases where a **Working Environment Template** 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 application desktops accessible to profile users", page 54.*

Terminology

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

☛ *See "Associating a terminology with a profile", page 54.*

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", page 55.*

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", page 40.*

The following points are detailed here:

- introduction:
  - "Users Delivered", page 34
  - "User: Definition", page 34
- properties:
  - "Person Properties", page 35
  - "Person Login Properties", page 37
- access:
  - "Accessing the User Management Pages", page 69
- characteristics:
  - "Viewing Person Characteristics", page 76
  - "Viewing Login Characteristics", page 79

Users Delivered

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

- persons indispensable to the system:
  - ***Administrator***, with Login "System"

    ☛ *The "Administrator" user cannot be deleted. It has no profile (it has all rights) and no password is assigned at installation.*

    ☛ *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) and no password is assigned at installation.*
- a person given by way of example:
  - ***Mega***, with Login "Mega"

    ☛ *The "Mega" user can be deleted (not recommended). The "Mega" user has the "HOPEX Administrator" profile, which allows to manage repositories and users. No password is assigned to "Mister Guide" at installation.*

User: Definition

For each environment, a user has:

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

  ☛ *see "Viewing Person Characteristics", page 76.*
- 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 "Person Login Properties", page 37.*
- a **user code** which enables naming of user associated files, for example the work repository.

  ☛ *see "Person Login Properties", page 37.*
- 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", page 29.*

  ☛ *see "Managing Profiles", page 48.*

  ☛ *see "Assigning a Profile to a Person", page 56.*
- **options**

  ☛ *see "Managing Options", page 169.*

- (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", page 65.*

Only a user with a **HOPEX Administrator**, **Web user Administrator** , or **Functional Administrator for a Solution** profile (or with equivalent rights) can configure and modify user properties.

☛ *see "The Administration profiles provided", page 26.*

Person Properties

☛ *To consult properties of a person, see "Viewing Person Characteristics", page 76.*

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.

```
Example: DURAND Pierre
```

Image

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

E-mail address

The person e-mail address is useful, for distribution of reports (MS Word) for example.

It is mandatory for password change in Web mode and for receipt of questionnaires for example.

```
Example: pdurand@mega.com
```

Telephone number and initials

The telephone number and initials of the person are optional.

```
Example: +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/Web application) 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** is selected in **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 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 "Person Login Properties", page 37.*

Belongs to a Person Group

A person can:

- belong to a group

  ☛ *See "Creating a Person Group", page 91.*

- have the **Belongs to a person group** attribute selected
  When the "Belongs to a person group" attribute of the person is selected, the person belongs to a dynamic group (LDAP group or group connected to a macro).

  ☛ *See "Defining a dynamic person group with LDAP", page 94.*

  ☛ *See "Defining a dynamic person group with a Macro", page 94.*

  When the "Belongs to a person group" attribute of the person is 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 (LDAP group or groups connected to a macro): the person belongs to the default group.

☛ *See "Default connection group", page 43.*

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 her/him.

Profile assignment

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

The profile determines:

- the objects and tools to which the person has access

  ☛ *See "Managing UI Access (Permissions)", page 157.*

- the Web applications to which the person can connect.
- repository access
- access to products

  ☛ *See "Description of a profile", page 20.*

  ☛ *See "Assigning a Profile to a Person", page 56.*

Object assignments

Objects are assigned 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 **Assignment > Assignment of profiles** page.

☛ *See "Managing Business Roles", page 61.*

☛ *See "Assigning a business role to a person", page 65.*

Person Login Properties

To:

- create the login of a person, see "Creating Users", page 81 or "Creating the Login of a Person", page 85.
- consult login characteristics, see "Viewing Login Characteristics", page 79.
- configure the login of a person, see or "Defining the Login of a Person", page 86.

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.

```
Example: PDD
```

Login Holder

The login holder is the person associated with the login.

`Example: 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)", page 29.*

💣 ***If*** **a user is connected to a profile and the user and profile each 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.**

Authentication mode

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 "Defining Default Authentication Mode", page 102.*

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", page 102.*

- **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 "Windows Authentication", page 104.*

- **LDAP**
  Passwords are managed and stored in the LDAP server of the enterprise. The directory configuration is stored in options.

  The **HOPEX** user is authenticated at the LDAP server level.

  > ☛ *For more details, see "LDAP Authentication", page 104.*

- **Custom**
  This authentication is managed by an external authentication module or SSO. This authentication mode is specific to Web connection to Web applications.

  > ☛ *See the **Web connection overloading and configuration EN** technical article.*

Windows identifier

> ☛ *This field only appears when the **Authentication Mode** is "Windows", see "Authentication mode", page 38.*

The **Windows Identifier** of a user enables connection of a **HOPEX** user to a Windows user, see "Associating a Windows user with a HOPEX user manually", page 104.

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

LDAP server

> ☛ *This field only appears when the **Authentication Mode** is "LDAP", see "Authentication mode", page 38.*

The **LDAP Server** is the server with which the **HOPEX** user is authenticated in LDAP authentication mode.

This server contains the LDAP directory in which the **HOPEX** user is registered.

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", page 41
  - "Belonging to a Person Group", page 42
  - "User Groups Delivered", page 42
- properties:
  - "Person Group Properties", page 42
  - "Properties of a Person Group Login", page 45
- access:
  - "Accessing the User Management Pages", page 69
- characteristics:
  - "Viewing Person Group Characteristics", page 78
  - "Viewing Login Characteristics", page 79

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", page 16.*

  ☛ *see "Description of a profile", page 20.*
- connect to the application with their **login**, but with access rights defined on the **login** of the group.

  ☛ *see "Properties of a Person Group Login", page 45.*
- share the assignments defined for the group.

  ☛ *See "Assigning a profile to a person group", page 58.*
- share the personal characteristics defined for the group.

  ☛ *see "Person Group Properties", page 42.*

  💣 **When a person belongs to a person group, the person cumulates the profiles assigned to her/him 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 on creation of the person.

  ☛ *See "Creating Users", page 81.*
- connect more than one person to a person group simultaneously:

  ☛ *See "Connecting one or more persons to a person group", page 93.*

A user group is a group of persons with a login.

☛ *see "Properties of a Person Group Login", page 45.*

Belonging to a Person Group

A person can:

- belong to a group

  ☛ *See "Creating Users", page 81.*

  ☛ *See "Creating a Person Group", page 91.*

  ☛ *See "Connecting one or more persons to a person group", page 93.*

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

  ☛ *See "Belongs to a Person Group", page 36.*

  When the "Belongs to a person group" attribute of the person is selected, the person belongs to a dynamic group (LDAP group or group connected to a macro).

  ☛ *See "Defining a dynamic person group with LDAP", page 94.*

  ☛ *See "Defining a dynamic person group with a Macro", page 94.*

  When the "Belongs to a person group" attribute of the person is 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 (LDAP group or groups connected to a macro): the person belongs to the default group.

  ☛ *See "Default connection group", page 43.*

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 her/him to the profiles assigned to the person group she/he belongs to.*

User Groups Delivered

A user group is a group of persons with a login.

By default at installation, the "Guests" person group with the Login "Guests" is created in the environment.

At installation, Guests is defined as default connection group (see "Default connection group", page 43).

Person Group Properties

☛ *For information on a person group, see:*

"Managing Person Groups Rather than Persons", page 41,
"User Groups Delivered", page 42,
"Viewing Person Group Characteristics", page 78, and
"Defining the Login of a Person Group", page 97.

Name

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

```
Example: 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. This is used to restrict access to the products of the group and make the group inactive.

The user that belongs to the group connects with his/her own login, but with repository access rights defined on the login of the group.

☛ *For more details, see "Properties of a Person Group Login", page 45.*

💣 **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.*

☛ *By default, at installation "Guests" is the default connection group.*

☛ *See "Person Properties", page 35.*

Person group types

A person can belong to:

- a static group
  Persons are explicitly connected to the group.
  ☛ *See "Defining a Person Group", page 92.*
- a dynamic group
  The group computes group persons on the fly.
  Examples of dynamic groups:
  - LDAP groups (case of LDAP authentication)
    ☛ *See "Defining a dynamic person group with LDAP", page 94.*
  - 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", page 94.*

LDAP dynamic group

An LDAP group is an organization within a directory. It is often characterized by type OU.

```
Example: the LDAP Quality group has the unique identifier
(Distinguished Name):

OU=Quality,OU=UNIVERSITE,OU=FRANCE,DC=fr,DC=mega,DC=com
```

All persons belonging to this organization belong to the LDAP group.

LDAP groups represent a list of persons distributed by organization. Users belonging to an LDAP group use configuration available on the group:

- HOPEX repository connection
- access to roles

The LDAP group defines a group or organization in the LDAP directory or Active Directory. It contains a list of users authorized to connect to the application concerned with the group configuration.

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/Web application) via the **Data language** option.*

Assignment - 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 profile determines the following for the person group:

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

> ☛ *See "Description of a profile", page 20.*

- the objects and tools accessible

> ☛ *See "Managing UI Access (Permissions)", page 157.*

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", page 58.*

Properties of a Person Group Login

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

To:

- create a person group, see "Creating a Person Group", page 91.
- consult login characteristics, see "Viewing Login Characteristics", page 79.
- define the login of a person group, see "Defining the Login of a Person Group", page 97.

User code

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

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

```
Example: SUPPOR
```

Login Holder

The login holder is the person group associated with the login.

```
Example: 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.**

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)", page 29.*

💣 ***If* a user is connected to a profile and the user and profile each 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.**

Authentication mode

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 "Defining Default Authentication Mode", page 102.*

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

- **HOPEX**

  Passwords are managed and stored in the **HOPEX** repository.

  This is default authentication mode.

  ☛ *For more details, see "Authentication in HOPEX", page 102.*

- **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 "Windows Authentication", page 104.*

- **LDAP**
  Passwords are managed and stored in the LDAP server of the enterprise. The directory configuration is stored in options.

  The HOPEX user is authenticated at the LDAP server level.

  > ☛ *For more details, see "LDAP Authentication", page 104.*

- **Custom**
  This authentication is managed by an external authentication module or SSO. This authentication mode is specific to Web connection to Web applications.

  > ☛ *See the **Web connection overloading and configuration EN** technical article.*

Windows Login

> ☛ *This field only appears when the **Authentication Mode** is "Windows", see "Authentication mode", page 38.*

The **Windows Login** of a user enables connection of a **HOPEX** user to a Windows user, see "Associating a Windows user with a HOPEX user manually", page 104.

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

LDAP server

> ☛ *This field only appears when the **Authentication Mode** is "LDAP", see "Authentication mode", page 38.*

The **LDAP Server** is the server with which the **HOPEX** user is authenticated in LDAP authentication mode.

This server contains the LDAP directory in which the **HOPEX** user is registered.

MANAGING PROFILES

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

The *profiles* are managed in the **HOPEXAdministration** desktop.

☛ *See "Introduction to Profile Management", page 20.*

📖 *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:

- "Introduction to Profiles", page 48
- "Creating a Profile", page 49
- "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50
- "Viewing Profile Characteristics", page 50
- "Configuring a Profile", page 52
- "Checking a profile compliancy with connection regulation", page 56
- "Assigning a Profile to a Person", page 56
- "Assigning a profile to a person group", page 58
- "Deleting a Profile", page 60

You can also:

- copy a profile
- manage a profile
  - manage the modeling rules of the profile
  - compare and align profiles

To:

- modify profile options

  ☛ *see "Managing Options", page 169.*

- manage metamodel filters at profile level

  ☛ *see "Managing UI Access", page 159.*

Introduction to Profiles

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

```
Example: Application Portfolio Manager, Enterprise
Architect).
```

A profile enables definition of the same connection rights to a set of users:

- applications accessible

  ☛ *See "Defining applications accessible to profile users", page 53.*

- desktops accessible

  ☛ *See "Defining application desktops accessible to profile users", page 54.*

- access rights to UIs (permissions).

  ☛ *See "Managing UI Access", page 159.*

- the same options.

  ☛ *See "Viewing Profile Characteristics", page 50.*

- access rights restricted to certain products

  ☛ *See "Products accessible on the license (Command Line)", page 38.*

  💣 **If a user already has access rights restricted by the Command Line attribute on his/her Login (see "Viewing Login Characteristics", page 79), the products accessible to this user are at the intersection of values of the Command Line attribute of the user login and profile.**

You must assign each person (or person group) at least one profile so that this person can connect to a **HOPEX** application.

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

Assigning a profile to a person (or person group) defines:

- the repository concerned by the assignment
- the repository access rights
- (optional) the validity period of the assignment
- (optional, with read-only access to the repository) connection repository snapshot

  ☛ *See "Assigning a Profile to a Person", page 56.*

  ☛ *See "Assigning a profile to a person group", page 58.*

Creating a Profile

To connect, a user must have at least one profile assigned (by assignment of a profile to the person or the person group to which the person belongs).

Users with the same profile share common characteristics: options, authorized products, access rights to repositories, UIs and data.

To create a profile:

1. Access the Profiles management pages.

   ☛ *See "Accessing the User Management Pages", page 69.*

2. In the **Profiles** page, click **New** ⊕.
3. In the profile creation dialog box that appears, 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. Click **OK**.
   The new profile appears in the list of profiles.
   You must:
   - define profile UI access

     ☛ *See "Managing UI Access", page 159.*

     ☛ *You can use configuration of UI access defined on an existing profile, see "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50.*
   - configure the profile.

     ☛ *See "Configuring a Profile", page 52.*

Customizing an Existing Profile / Creating a Profile from an Existing Profile

You can create a profile by aggregation of existing profiles.

To customize a profile for which you do not have modification rights, you can create a new profile from this profile.

☺ ***To customize a profile provided by MEGA, MEGA recommends you create a new profile from this existing profile.***

To customize a profile for which you do not have modification rights:

1. Create a new profile.

   ☛ *See "Creating a Profile", page 49.*
2. In the properties pages of the new profile, select **Used Profile**.
3. Right-click your **Profile** and select **Connect > Sub-Profile**.
4. (Optional) In the query field, enter the characters you want to find.
5. Click **Find** 🔍.
6. In the results list, select the profile you want to customize.

   ☛ *You can aggregate several profiles.*
7. Click **Connect**.
   The profile you have created inherits all accesses defined on the profile you have connected. You can customize these accesses.

Viewing Profile Characteristics

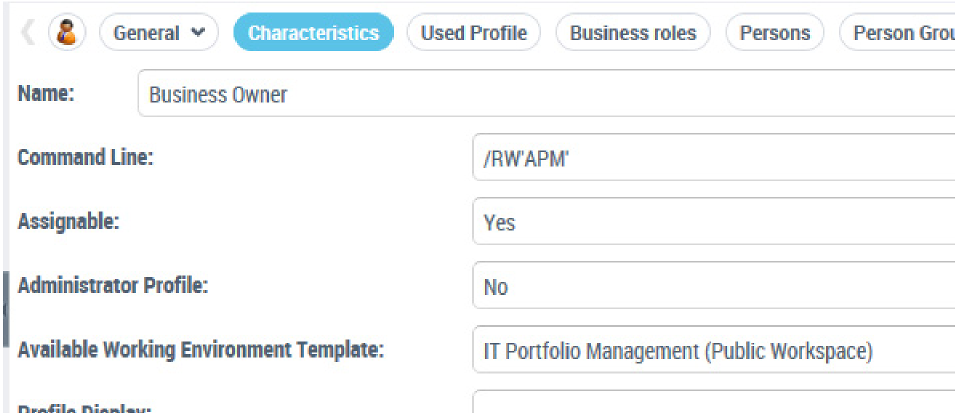
To view profile characteristics:

1. Access the user management pages.

   ☛ *See "Accessing the User Management Pages", page 69.*
2. Select the **Profiles** sub-folder.
3. In the edit page, select the profile.

4. In the toolbar, click **Properties** .
   The profile **Properties** dialog box opens.

   ☛ *For detailed information on characteristics of a profile, see "Profile Properties", page 29.*



Name: Business Owner

Command Line: /RW'APM'

Assignable: Yes

Administrator Profile: No

Available Working Environment Template: IT Portfolio Management (Public Workspace)

Profile Display:

☛ *See "Configuring a Profile", page 52.*

Configuring a Profile

From the profile properties window you can define:

☛ *See "Profile Properties", page 29.*

- 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.*
- the profile display name in the interface.

  ☛ *See step 7.*
- the profile icon in the interface.

  ☛ *See step 8.*
- perform a mass profile assignment to persons

  ☛ *See "Performing a Mass Profile Assignment to Persons", page 57.*

  ☛ *See "Performing a mass assignment of profiles to a person group", page 59.*
- applications accessible to users of the profile

  ☛ *See "Defining applications accessible to profile users", page 53.*
- desktops accessible to users of the profile

  ☛ *See "Defining application desktops accessible to profile users", page 54.*
- the terminology associated with the profile

  ☛ *See "Associating a terminology with a profile", page 54.*
- object types available

  ☛ *See "Defining the object types available for a profile", page 55.*
- the sub-profiles used to define the profile.

  ☛ *See "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50.*

To check that the profile complies with the connection regulation:

- see "Checking a profile compliancy with connection regulation", page 56.

Configuring profile characteristics

To configure profile characteristics:

1. Access the properties of the profile.

   ☛ *See "Viewing Profile Characteristics", page 50.*

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)", page 29.*

3. (Optional) In the **Assignable** field, modify the attribute value via the drop-down menu. By default, the profile is not assignable.

   ☛ *See "Assignable", page 30.*

4. (Optional) In the **Administrator Profile** field, modify the attribute value.

   ☛ *By default, the profile is not an administrator profile.*

   ☛ *See "Administrator profile", page 30.*

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", page 30.*

6. (Optional) In the **Profile Status** field, modify the attribute value.

   ☛ *By default, the profile is active.*

7. (Optional) In the **_GUIName** field, enter the profile name displayed in the interface.
8. (Optional) In the **MetaPicture** field, click the arrow and select **Query 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**.

Defining applications accessible to profile users

☛ *To modify a profile provided by **HOPEX**, you must create a new profile; see "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50.*

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

☛ *See "Connection schema: Person - Profile - Application", page 21.*

All desktops connected to the application are then accessible. To enable access to only certain desktops of the application, see "Defining application desktops accessible to profile users", page 54.

☛ *See "Connection schema: Person - Profile - Application - Desktops", page 22.*

To define applications available for a profile:

1. Access the properties pages of the profile.

   ☛ *See "Viewing Profile Characteristics", page 50.*

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

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

Defining application desktops accessible to profile users

A user can connect to applications 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 "Connection schema: Person - Profile - Application - Specific Desktops", page 24.*

To do this, you must connect to the profile:

- the application containing the desktops.

  > ☛ *See "Defining applications accessible to profile users", page 53.*

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

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

  > ☛ *To modify a profile supplied by **HOPEX**, **HOPEX** recommends you create a new profile; see "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50.*

To define application desktops available for a profile:

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

> ☛ *See "Defining applications accessible to profile users", page 53.*

1. Access the properties pages of the profile.

   > ☛ *See "Viewing Profile Characteristics", page 50.*

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

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", page 50.*

2. Select **Terminology**.
3. In the toolbar, click **Connect** .
   The business roles query tool appears.
4. (Optional) In the second field, enter the characters to find.

5. Click **Find** 🔍.
6. In the query results, select the terminology you want to connect.

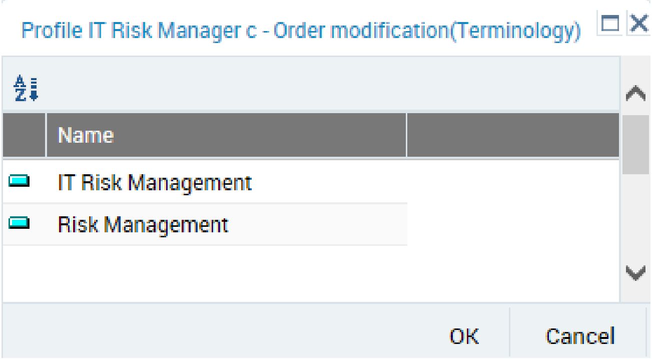
   ☛ *You can select several terminologies.*
7. Click **Connect**.
   The terminology is connected to the profile.

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", page 50.*
2. Select **Terminology**.
3. In the toolbar, click **Reorganize**.
4. Drag and drop to place the priority terminology at the top.



Profile IT Risk Manager c - Order modification(Terminology)

Name
IT Risk Management
Risk Management

```
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", page 50.*
2. Select **Available Types**.
3. Select **Available Objects**.
4. In the toolbar, click **Connect**.
   The object type query tool appears.
5. (Optional) In the query tool, in the first field, select the object type category.

6. (Optional) In the second field, enter the characters to find.
7. Click **Find** 🔍.
8. In the query result, select the object types to make available for the profile.
9. Click **Connect**.
   The object types selected are made available for the profile.

Checking a profile compliancy 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", page 69.*

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
- the repository access rights 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.

☛ *The repository snapshot creation function is available with **HOPEX Collaboration Manager.***

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

☛ *To create a repository snapshot, see the **HOPEX Collaboration Manager - Repository Snapshots** guide.*

See:

- "Assigning a Profile to a Person", page 57
- "Performing a Mass Profile Assignment to Persons", page 57
- "Mass assignment of profiles to persons", page 58

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", page 58*

> ☛ *To assign a profile to a person from the user management page, see "Mass assignment of profiles to persons", page 58).*

To assign a profile to a person:

1. Access the properties of the person.

   > ☛ *See "Viewing Person Characteristics", page 76.*

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. (optional) 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) In the **Data access** field, click the drop-down menu to restrict access to read-only data.

   > ☛ *By default, access to repositories is "read/write".*

7. (optional, with read-only access to the repository) In the **Connection Snapshot** field, select a connection repository snapshot.
8. (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.
9. 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", page 58.*

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", page 69.*

2. In the edit area, select the profile you want to connect to persons.
3. In the edit area, click **Connect** 🔗 .
4. (Optional) In the query field, enter the characters to find.

5. Click **Find** 🔍 to run the query.
   The list of persons to whom you can assign the profile appears.
6. In the result list, select the persons to whom you want to assign the profile.
7. Click **Connect**.
   The selected profile is assigned to the selected persons, on the current repository, without a validity limit.

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", page 69.*
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. 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.
6. Select the profiles that you want to assign to the selected persons.
7. Click **OK**.
   The selected profiles are assigned to the persons selected 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", page 58
- "Performing a mass profile assignment to person groups", page 59
- "Performing a mass assignment of profiles to a person group", page 59

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 Person Group Characteristics", page 78.*

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. In the **Repository** field, click the drop-down menu and select the repository to which the profile is assigned.

   ☛ *You can select one repository or all the repositories.*

5. In the **Data access** field, click the drop-down menu and select the data access mode.
6. By default, assignments do not have a validity limit. If you must 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", page 69.*

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. (Optional) In the query field, enter the characters to find.
6. Click **Find** 🔍 to run the query.
   The list of person groups to whom you can assign the profile appears.
7. In the result list, select the person groups to whom you want to assign the profile.
8. Click **Connect**.
   The selected profile is assigned to the selected person groups, on the current repository, without a validity limit.

Performing a mass assignment of profiles to a person group

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

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

   ☛ *See "Accessing the User Management Pages", page 69.*

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

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", page 69.*

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

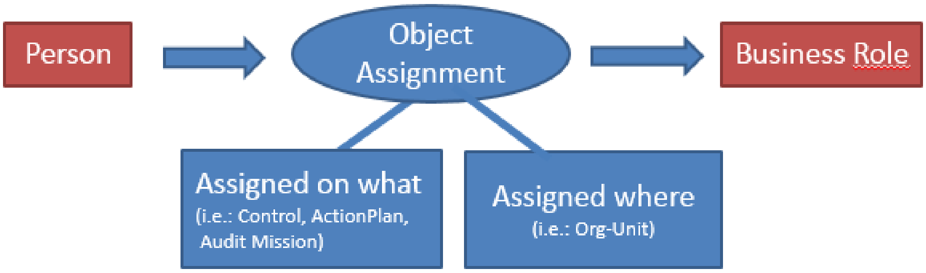
   ☛ *You can select more than one.*

3. Click **Delete** ⊗.
   The delete objects dialog box opens.
4. Click **Delete**.
   The profile is deleted from the environment

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", page 61
- "Creating Business Roles", page 62
- "Defining a Business Role", page 63
- "Assigning a business role to a person", page 65
- "Transferring responsibilities to a person", page 66
- "Duplicate the Responsibilities of a Person", page 67
- "Deleting a Business Role", page 68

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", page 69.*

2. Click **New** ⊕ .
   The business role creation dialog box 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", page 62.*

   > ☛ *To define the business role, see "Defining a Business Role", page 63.*

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", page 69.*

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", page 65.*

To define a business role:

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

   ☛ *See "Accessing the User Management Pages", page 69.*

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 MetaClasses query tool appears.

   - (Optional) In the second field, enter the characters to find.
   - Click **Find** 🔍.
   - In the query 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 MetaClasses query tool appears.

   - (Optional) In the second field, enter the characters to find.
   - Click **Find** .
   - In the query 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 find.
   - 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.

8. Click **Save** .

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

   ☛ *See "Assigning a business role to a person", page 65.*

Assigning a business role to a person

A business role can be assigned to a person:

- for a specific object

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

  ☛ *See "Assigning an object to a person", page 65 step 5.*

- to a given geographical location

  Example: David Oldfield is Risk Manager at London Branch.

  ☛ *See "Assigning an object to a person", page 65 step 6.*

- to a given geographical location for a specific object

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

  ☛ *See "Assigning an object to a person", page 65 steps 5 and 6.*

See:

- "Assigning an object to a person", page 65
- "Mass assignment of objects to persons", page 66

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", page 66*

☛ *To assign an object to a person from the user management page, see "Mass assignment of objects to persons", page 66.*

To assign an object to a person:

1. Access the properties of the person.

   ☛ *See "Viewing Person Characteristics", page 76.*

2. In **Assignments,** click **Object Assignments**.
3. Click **New** ⊕.
4. In the **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", page 63.*

   In the query dialog box:

   - (if necessary) in the first field, select the object type to find.
   - (optional) in the **Find object** field, enter the characters to find.
   - 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", page 63.*

   In the query dialog box,

   - (if necessary) in the first field, select the object type to find.
   - (Optional) in the second field, enter the characters to find.
   - 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", page 69.*
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 **Connect** 🔗.
7. (Optional) Using the query wizard:
   - (if necessary) in the first field, select the object type to find.
   - (Optional) in the second field, enter the characters to find.
   - 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", page 67.*

To transfer the responsibilities from one person to another:

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

   ☛ *See "Accessing the User Management Pages", page 69.*
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 characters to find.
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", page 69.*

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 characters to find.
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", page 63).**
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", page 69.*
2. Select the business role you want to delete.

   ☛ *You want to select one or more business roles.*
3. Click **Delete** ⊗.
   The business role deletion dialog box appears.
4. Click **Delete**.
   The business role is deleted from the environment.

Access to User Management

See:

- "Accessing the User Management Pages", page 69.
- "Viewing Person Characteristics", page 76.
- "Viewing Person Group Characteristics", page 78.
- "Viewing Login Characteristics", page 79.

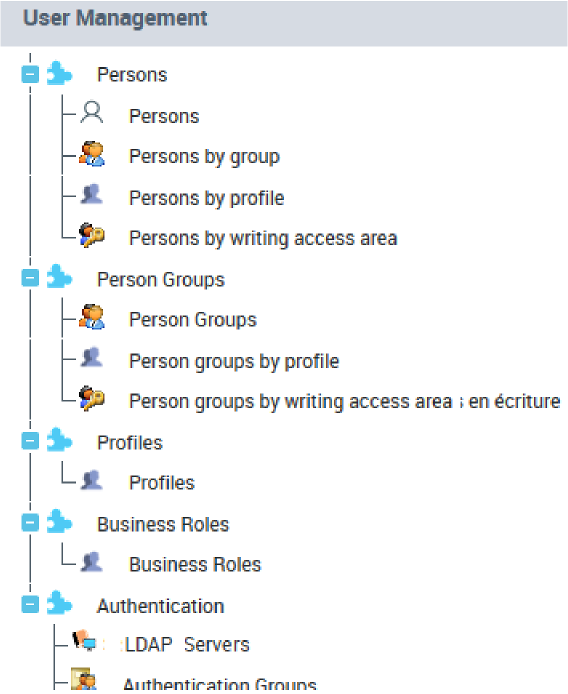
Accessing the User Management Pages

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

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

   ☛ *See "Connecting to the Administration Desktop", page 6.*

2. In the **Administration** tab, click the **User Management** pane.
   The user management tree appears.



3. In the user management tree, click on a sub-folder for:
   - **Persons** to manage persons and logins

     ☛ *See "Actions performed from the Persons management page", page 71.*
   - **Person Groups** to manage the persons who belong to the same person group

     ☛ *See "Actions performed from the Person Group page", page 72.*
   - **Profiles** to manage profiles

     ☛ *See "Managing Profiles", page 48.*

     ☛ *See "Profile Properties", page 29.*
   - **Business Roles** to manage the business roles

     ☛ *See "Managing Business Roles", page 61.*
   - **LDAP Servers** to manage the LDAP servers.

     ☛ *See "LDAP Authentication", page 104.*

   The management page selected appears.

See:

- "Managing persons who have an identical characteristic", page 70
- "Managing a group of persons who have a specific characteristic", page 70
- "Actions performed from the Persons management page", page 71
- "Actions performed from the Person Group page", page 72

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", page 72
- "Accessing the list of person who belong to the same group", page 72
- "Accessing the list of persons connected to a specific writing access area", page 73
- "Accessing the list of persons connected to a specific reading access area", page 73
- "Accessing the list of persons who have or do not have a login", page 73

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", page 74
- "Accessing the list of person groups connected to a specific writing access area", page 74
- "Accessing the list of person groups connected to a specific reading access area", page 75

Actions performed from the Persons management page

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

- create users

  ☛ *See "Creating Users", page 81.*

- create logins

  ☛ *See "Creating the Login of a Person", page 85.*

- access a person using his/her name

  ☛ *"Accessing a person using his/her name", page 74*

- configure the characteristics of a person

  ☛ *See "Defining a Person", page 83.*

- check the configuration of a person

  ☛ *See "Checking the Configuration of Persons", page 19.*

- configure the characteristics of a login

  ☛ *See "Defining the Login of a Person", page 86.*

- delete users

  ☛ *See "Deleting a user", page 90.*

- modify the properties of users

  ☛ *See "Modifying User Properties", page 88.*

- assign a profile to a person

  ☛ *See "Assigning a Profile to a Person", page 57 and "Mass assignment of profiles to persons", page 58.*

- assign an object to a person

  ☛ *See "Assigning an object to a person", page 65 and "Mass assignment of objects to persons", page 66.*

- Transferring the Responsibilities of a Person

  ☛ *See "Transferring responsibilities to a person", page 66.*

- duplicate the responsibilities of a person

  ☛ *See "Duplicate the Responsibilities of a Person", page 67.*

- initialize and manage the password of a Web user

  ☛ *See "Managing the Password of a Web User", page 112.*

- connect a person to a writing access area

  ☛ *See "Connecting a Person to a Writing Access Area", page 88.*

- connect a person to a reading access area

  ☛ *See "Connecting a Person to a Reading Access Area", page 89.*

- access user options

  ☛ *See "Modifying options at user level", page 172.*

- import persons from an LDAP directory

  ☛ *See "Importing persons from an LDAP server", page 109.*

- filter persons.

  ☛ *See "Accessing the list of persons who have or do not have a login", page 73 or "Accessing a person using his/her name", page 74.*

Actions performed from the Person Group page

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

- create user groups

  ☛ *See "Creating a Person Group", page 91.*

- define the properties of a person group

  ☛ *See "Defining a Person Group", page 92.*

- configure the characteristics of a login

  ☛ *See "Defining the Login of a Person Group", page 97.*

- assign a profile to a person group

  ☛ *See "Assigning a profile to a person group", page 58.*

- connect a person group with a writing access area

  ☛ *See "Connecting a Person Group with Access to a Writing Area", page 95.*

- connect a person group with a reading area access

  ☛ *See "Connecting a person group with access to a reading area", page 96.*

- define a person group

  ☛ *See "Deleting a Person Group", page 99.*

- modify user group properties

  ☛ *See "Modifying User Group Properties", page 98.*

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", page 69.*

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", page 71.*

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", page 69.*

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 LDAP 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", page 72.*

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", page 69.*
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", page 71.*

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", page 69.*
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", page 71.*

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", page 69.*

2. Select a **Persons** sub-folder.
3. In the edit area, click in the field of the **Login** column and select:
   - **Filters > Display specified values only**

     The persons who have a login are listed.
   - **Filters > Display unspecified 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", page 69.*
2. Select a **Persons** sub-folder.
3. In the edit area, click in the field of the **Name** column and in the **Filters** 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", page 69.*
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", page 72.*

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", page 69.*
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", page 72.*

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:

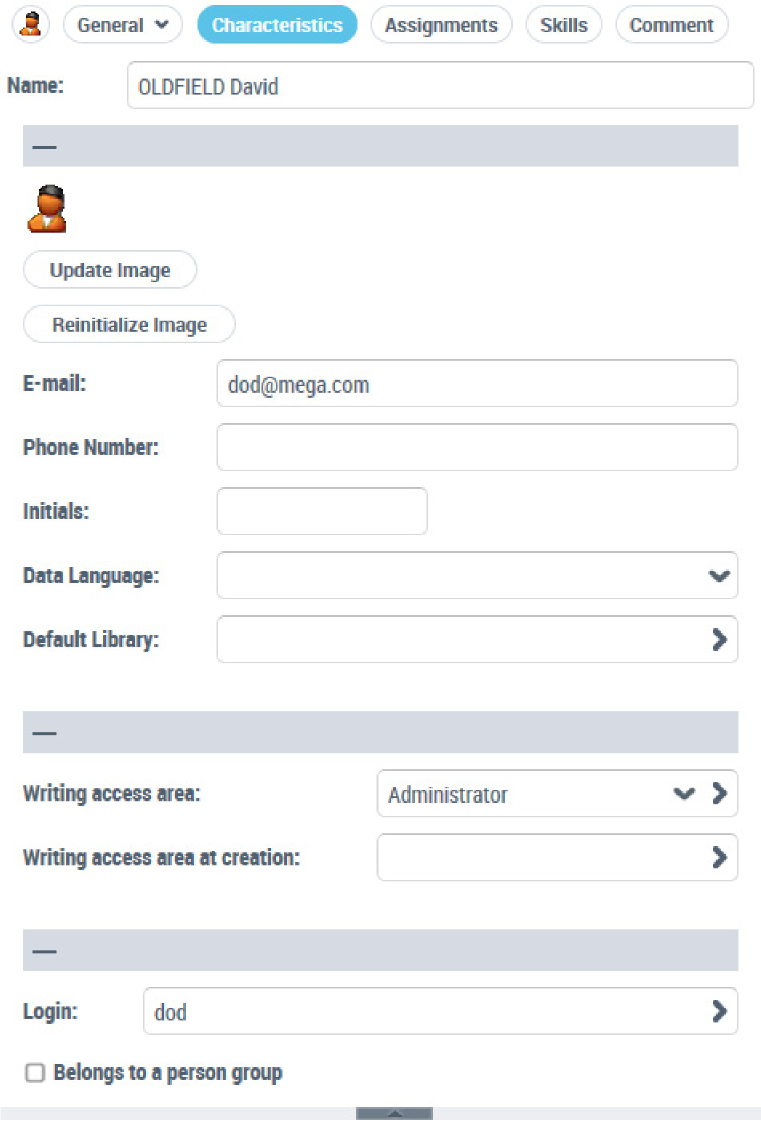
1. Access the user management page.

   ☛ *See "Accessing the User Management Pages", page 69.*

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", page 72.*

Viewing Person Characteristics



Name: OLDFIELD David

E-mail: dod@mega.com

Phone Number:

Initials:

Data Language:

Default Library:

Writing access area: Administrator

Writing access area at creation:

Login: dod

☐ Belongs to a person group

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", page 83, "Creating Users", page 81 and "Assigning a Profile to a Person", page 56 (or "Performing a Mass Profile Assignment to Persons", page 57).*

To view person characteristics:

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

   > ☛ *See "Accessing the User Management Pages", page 69.*

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", page 73 and "Accessing a person using his/her name", page 74.*

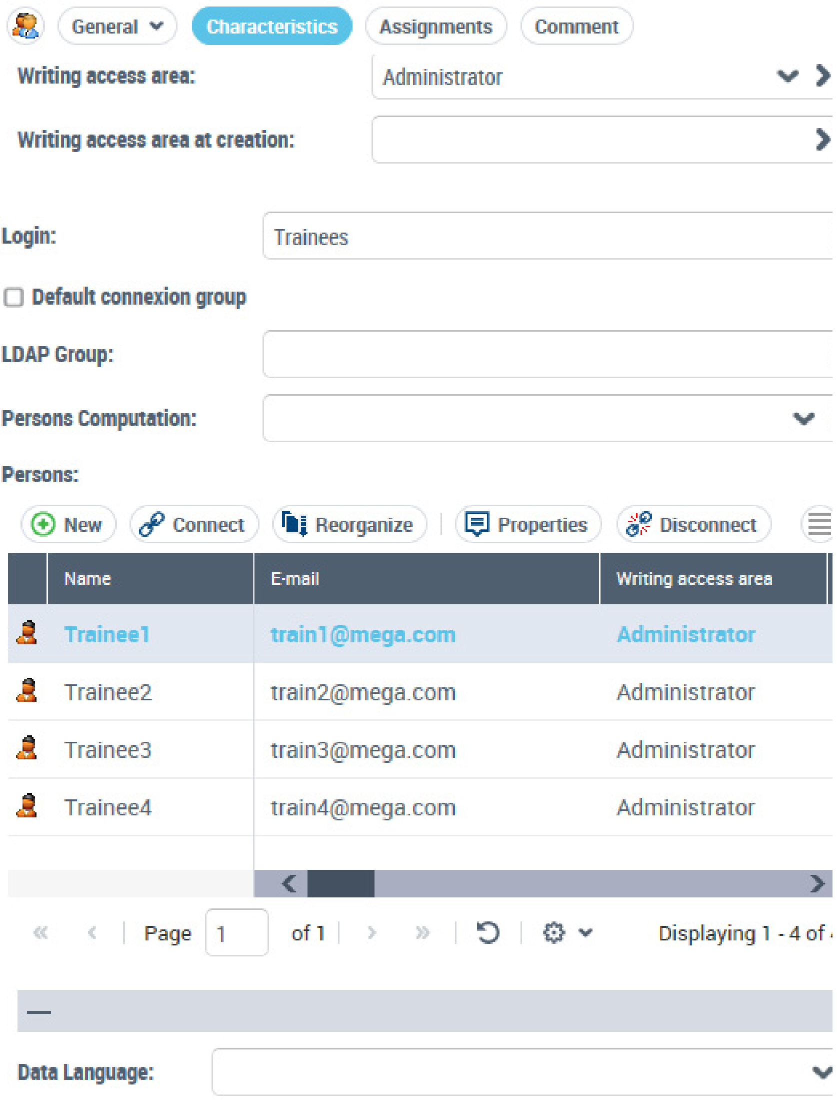
   > ☛ *You can modify the e-mail and the login of a person directly in this page (with a click in the corresponding field).*

3. In the Persons list, select the person.
4. In the toolbar, click **Properties** .
   The **Properties** dialog box of the person opens.
5. Click:
   - the **Characteristics** tab to define or modify the person properties.

     > ☛ *See "Person Properties", page 35.*

     > ☛ *See "Defining a Person", page 83.*
   - **General > History** to display the actions performed on the person.
   - **Assignments** to display and assign profiles to the person.

Viewing Person Group Characteristics



Writing access area: Administrator

Writing access area at creation:

Login: Trainees

□ Default connexion group

LDAP Group:

Persons Computation:

Persons:

	Name	E-mail	Writing access area
	Trainee1	train1@mega.com	Administrator
	Trainee2	train2@mega.com	Administrator
	Trainee3	train3@mega.com	Administrator
	Trainee4	train4@mega.com	Administrator

Page 1 of 1 Displaying 1 - 4 of

Data Language:

To view person group characteristics:

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

   ☛ *See "Accessing the User Management Pages", page 69.*

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 LDAP group or associated macro and it comments.

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

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

3. In the toolbar, click **Properties** 🗨.
   The **Properties** dialog box of the person group opens.
4. Click:
   - **Characteristics** to define or modify the person group properties.

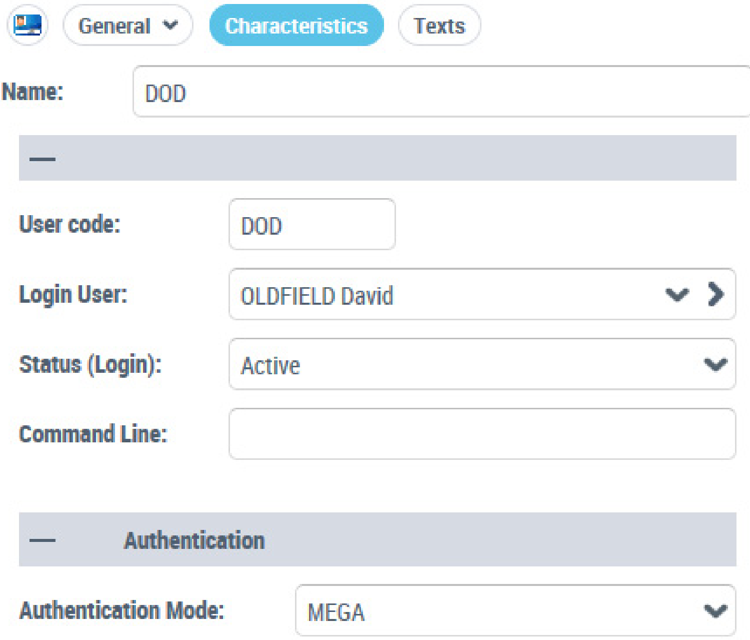
     ☛ *See "Person Group Properties", page 42.*

     ☛ *See "Defining a Person Group", page 92, "Defining a dynamic person group with LDAP", page 94, "Defining a dynamic person group with a Macro", page 94.*
   - **General > History** to display the actions performed on the person group.
   - **Assignments** to display the profiles assigned to the person group.

Viewing Login Characteristics

☛ *For detailed information on characteristics of a login, see "Person Login Properties", page 37.*

☛ *To configure a login, see "Defining the Login of a Person", page 86.*



Name: DOD

User code: DOD

Login User: OLDFIELD David

Status (Login): Active

Command Line:

Authentication Mode: MEGA

To view login characteristics:

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

   ☛ *See "Accessing the User Management Pages", page 69.*

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 "Actions to be Performed to Define a User", page 16.

☛ *To manage person groups, see "Managing Person Groups Rather than Persons", page 41 and "Creating and Managing a Person Group", page 91.*

The following points are covered here:

- configuration:
  - "Creating Users", page 81
  - "Defining a Person", page 83
  - "Creating the Login of a Person", page 85
  - "Defining the Login of a Person", page 86
  - "Modifying User Properties", page 88
  - "Connecting a Person to a Writing Access Area", page 88
- management:
  - "Checking the Configuration of Persons", page 19
  - "Connecting a Person to a Writing Access Area", page 88
  - "Connecting a Person to a Reading Access Area", page 89
  - "Preventing User Connection", page 89
  - "Deleting a user", page 90
  - "Creating and Managing a Person Group", page 91
  - "Managing User Options", page 100

For information on managing business roles for persons, see:

- "Assigning a business role to a person", page 65
- "Transferring responsibilities to a person", page 66
- "Duplicate the Responsibilities of a Person", page 67

Creating Users

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

☛ *Instead of creating users one by one, you can import a list of persons. This list can for example come from an LDAP server (see "Synchronization with a company directory", page 104).*

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", page 35.*

☛ *For detailed information on characteristics of a login, see "Person Login Properties", page 37.*

☛ *To import users from an LDAP directory, see "LDAP Authentication", page 104.*

You can create the person as follows:

- not predefined
- predefined with one of the following criteria:
  - the group to which the person belongs
  - a profile
  - a writing access area
  - a reading access area (if reading access management is activated)

To complete the configuration of the person, see "Defining a Person", page 83.

To create a user:

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

   ☛ *See "Accessing the User Management Pages", page 69.*

2. You can create:
   - either a non-predefined person:
   Select the **Persons** sub-folder then in the edit area go to step 4.
   - or a person predefined with a characteristic:
   Select the sub-folder:

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

     Persons by profile *to create a person and automatically assign this person the profile that you are going to select.*

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

     Persons by reading access area *(available if reading access management is activated) to create a person automatically connected to the reading access area that you are going to select.*

3. In the edit area, select the group, the profile, the writing access area or the reading access area that you want to connect to the person.
4. Click **New** ⊕.
   The **Creation of Person - Characteristics** dialog box opens.
5. In the **Name** field, enter the name of the person.

   ```
   Example: DUBOIS Guillaume
   ```

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

6. In the **E-mail** field, enter the e-mail address of the person.

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

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

   ☛ *If you do not enter the Login, it will automatically take 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. (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".*

9. (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.*

10. Click **Next**.
The **Creation of Person - profiles** dialog box opens.

> ☛ *If step 2 you have selected **Person by profile**, go directly to step 13.*

> ☛ *If necessary, you can assign profiles to the user at a later time, see (or "Assigning a Profile to a Person", page 56). Go directly to step 13.*

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

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

> ☛ *You can assign more than one profile to the person.*

13. Click **OK**.

The user appears and is added to the list of users 👤.

> ☛ *To define the characteristics of the user, see "Defining a Person", page 83*

> ☛ *You must configure the login of the user, see "Defining the Login of a Person", page 86.*

Defining a Person

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

> ☛ *For more information on properties of a person, see "Person Properties", page 35.*

> ☛ *To check the configuration of a person, see "Checking the Configuration of Persons", page 19.*

> ☛ *To assign:*

a profile to a person (mandatory), see "Assigning a Profile to a Person", page 56.

an object to a person (if needed), see "Assigning a business role to a person", page 65.

From the profile properties window of a person, you can define:

- name of the person

  ☛ *See step 1.*

- image of the person

  ☛ *See step 2.*

- e-mail address of the person

  ☛ *See step 3.*

- telephone number and initials of the person

  ☛ *See step 4.*

- data language of the Web user

  ☛ *See step 5.*

- default library to store objects created by the person

  ☛ *See step 6.*

- writing access area of the user

  ☛ *See step 7.*

- reading access area of the user

  ☛ *See step 7.*

- the login of the person

  ☛ *See step 8.*

- if the person belongs to a person group.

  ☛ *See step 9.*

To define a **Person**:

1. Access the properties of the person.

   ☛ *See "Viewing Person Characteristics", page 76.*

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

   ☛ *To delete the image, click **Reinitialize Image**.*

3. In the **E-mail** field, enter the e-mail address of the person.

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

4. (Optional) Enter the **Phone Number** and the **Initials** of the person.
5. (Web specific, optional) In the **Data Language** field, you can define a specific data language for this user.
   - Click the arrow and select **Query Language**.
   - In the query wizard, select the data language (objects) and click **OK**.

   ☛ *If the field is not specified, the default data language is the interface language defined in environment options (**Options/ Installation/User Management**: **Data Language**).*

   ☛ *See "Managing Languages in Web Applications", page 178.*

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", page 88.*
   - 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", page 89.*
   - 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", page 85.*
9. (optional) If necessary select **Belongs to a Person Group**
10. Click **Save** 💾.
    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:

- an administration desktop, the login of the person is automatically created.
  This person can connect to **HOPEX**.
- other desktops, for example to add it to an organizational 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 Person Characteristics", page 76.*
2. In the **Login** field, click the arrow and select **Create Login**.
   The **Creation of Login** dialog box 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**.*

   Example: GDS

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

   Example: GDS

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

Defining the Login of a Person

From the Login properties window, you can:

☛ *See "Person Login Properties", page 37.*

- define the login name, the user code associated with the login and the login holder

  ☛ *See step 1.*

- modify user status (inactive)

  ☛ *See step 2.*

- restrict user access to certain products

  ☛ *See step 4.*

- modify user authentication mode

  ☛ *See step 4.*

To define the login of a person:

1. In the login properties pages, display **Characteristics**.

   ☛ *See "Viewing Login Characteristics", page 79.*

   - 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 serves as a basis for naming user private workspaces.*

   - 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)", page 38.*

3. (Optional) In the **Command Line** field, define the products available to which the user has access.
   To restrict 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 **HOPEX Business Process**

Analysis and **HOPEX IT Portfolio Management** modules to a user, enter:

```
/RW'HBPA;APM'
```

☛ *To determine the product code, see the on line documentation:* ***Concepts > Products****.*

💣 ***If* a user is connected to a profile and the user and profile each 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 (on his/her login) and profile.**

4. (Optional) In the **Authentication Mode** field, click the arrow and modify the authentication mode. The default value is "MEGA".

   ☛ *See "Authentication mode", page 38.*

5. Click **Apply**.

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", page 35.*

    ☛ *See "Viewing Person Characteristics", page 76.*

    ☛ *See "Defining a Person", page 83.*
- login:
  - its name
  - user code

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

    ☛ *See "Person Login Properties", page 37.*

    ☛ *See "Viewing Login Characteristics", page 79.*

    ☛ *See "Defining the Login of a Person", page 86.*

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", page 83.*

To connect a person to a writing access area:

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

   ☛ *See "Accessing the User Management Pages", page 69.*
2. Select the **Persons by writing 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*** *.*

5. (Optional) In the query wizard, in the second field enter the characters to find.
6. Click **Find** .
   The persons queried are listed.
7. In the result list, select the person you want to connect.

   ☛ *You can select more than one person.*

8. Click **Connect**.
   The persons selected are 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", page 83.*

To connect a person to a reading access area:

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

   ☛ *See "Accessing the User Management Pages", page 69.*

2. Select the **Persons by writing 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*** *.*

5. (Optional) In the query wizard, in the second field enter the characters to find.
6. Click **Find** .
   The persons queried are listed.
7. In the result list, select the person you want to connect.

   ☛ *You can select more than one person.*

8. Click **Connect**.
   The persons selected are 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 render a user inactive:

1. In the login properties pages in question, display **Characteristics**.

   ☛ *See "Viewing Login Characteristics", page 79.*

2. In the **Status (Login)** field, select "Inactive".
   The user can no longer be able to 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", page 89.**

To delete a user:

1. Access the user management page.

   ☛ *See "Accessing the User Management Pages", page 69.*

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

   ☛ *You can select more than one.*

   The **Delete Objects** dialog box opens.

3. (If necessary) In the **Delete** column, modify the deletion selection of a person and her/his login.
4. Click **Delete** to confirm deletion.
   The person and login 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 "Actions to be Performed to Define a User", page 16.

The following points are covered here:

- configuration:
  - "Creating a Person Group", page 91
  - "Defining a Person Group", page 92
  - "Defining a default connection group", page 95
  - "Connecting a Person Group with Access to a Writing Area", page 95
  - "Connecting a person group with access to a reading area", page 96
  - "Defining the Login of a Person Group", page 97
- management:
  - "Preventing User Group Connection", page 98
  - "Deleting a Person Group", page 99

Creating a Person Group

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

For detailed information on:

- connecting persons belonging to a group, see "Managing Person Groups Rather than Persons", page 41:
- the types of person groups, see "Person group types", page 44.
- the characteristics of a person group, see "Person Group Properties", page 42.
- the characteristics of the login of a person group, see "Properties of a Person Group Login", page 45.

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", page 69.*

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** dialog box 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", page 92.

Defining a Person Group

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

☛ *See "Managing Person Groups Rather than Persons", page 41.*

☛ *For detailed information on:*

- the characteristics of a person, see "Person Properties", page 35.

- the characteristics of a person group, see "Person Group Properties", page 42.

- the characteristics of a login, see "Properties of a Person Group Login", page 45.

- the types of person groups, see "Person group types", page 44.

A person group can be created:

- static

  ☛ *See "Connecting one or more persons to a person group", page 93.*

- dynamically

  ☛ *See "Defining a dynamic person group with LDAP", page 94.*

  ☛ *see "Defining a dynamic person group with a Macro", page 94.*

You can:

- define a default connection group.

  ☛ *See "Defining a default connection group", page 95.*

- connect the person group with access to a reading area

  ☛ *See "Connecting a person group with access to a reading area", page 96.*

- connect the person group with access to a writing area

  ☛ *See "Connecting a Person Group with Access to a Writing Area", page 95.*

- define the data language of the person group

  ☛ *"Specifying the Data Language", page 116.*

- modify the properties of the person group

  ☛ *See "Modifying User Group Properties", page 98.*

To configure a person group, you must:

- assign a profile to the person group

  ☛ *See "Assigning a profile to a person group", page 58.*

- define its login

  ☛ *See "Defining the Login of a Person Group", page 97.*

Connecting one or more persons to a person group

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 Person Group Characteristics", page 78.*

2. Select **Characteristics**.
3. In the **Persons** pane, click **Connect** 🔗.

   ☛ *To add a person not yet created, click **New** ⊕.*

4. (Optional) In the query wizard, in the second field enter the characters to find.
5. Click **Find** 🔍.

   The persons queried are listed.
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.
8. Click **OK**.

Defining a dynamic person group with LDAP

🕮 *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.*

☛ *For information on person group types, see "Person group types", page 44.*

The **LDAP Group** attribute enables definition of LDAP groups belonging to this person group. Persons belonging to LDAP groups use the configuration defined on the person group.

Prerequisite: the LDAP group is already created.

☛ *See "LDAP Authentication", page 104.*

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

1. Access the properties pages of the person group.

   ☛ *See "Viewing Person Group Characteristics", page 78.*

2. Select **Characteristics**.
3. In the **LDAP Group** field, click the arrow and connect the required LDAP group.
4. Click **OK**.
   The dynamic person group is configured with LDAP.

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.*

☛ *For information on person group types, see "Person group types", page 44.*

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:

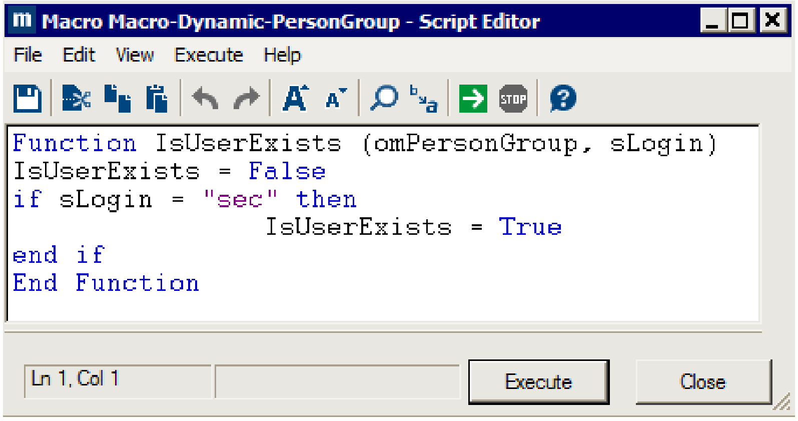
1. Access the properties pages of the person group.

   ☛ *See "Viewing Person Group Characteristics", page 78.*

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", page 44.*

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.

To define a default connection group:

1. Access the properties pages of the person group.

   ☛ *See "Viewing Person Group Characteristics", page 78.*

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

Connecting a Person Group with Access to a Writing 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", page 69.*

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*** ⊕.
5. (Optional) In the query wizard, in the second field enter the characters to find.
6. Click **Find** 🔍.

   The person groups queried are listed.
7. In the result list, select the person group you want to connect.

   ☛ *You can select more than one person group.*
8. Click **Connect**.
   The person groups selected are connected to the writing access area selected.

Connecting a person group with access to a reading area

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

To connect a person group with a reading access area:

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

   ☛ *See "Accessing the User Management Pages", page 69.*
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*** ⊕.
5. (Optional) In the query wizard, in the second field enter the characters to find.
6. Click **Find** 🔍.

   The person groups queried are listed.
7. In the result list, select the person group you want to connect.

   ☛ *You can select more than one person group.*
8. Click **Connect**.
   The person groups selected are connected to the reading access area selected.

Defining the Login of a Person Group

From the Login properties window, you can:

> ☛ *See "Properties of a Person Group Login", page 45.*

- define the login name, the user code associated with the login and the login holder
- modify the status of the person group (inactive)
- restrict access of the person group to certain products

To define the login of a person group:

1. Access the properties pages of the login.

   > ☛ *See "Viewing Login Characteristics", page 79.*

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 serves as a basis for naming user private workspaces.*

   - The **Login Holder** represents the person group associated with this login.
3. (optional) The value of the **Status (Login)** field defines if the user is active or not.
4. (Optional) In the **Command Line** field, define the products available to which the user has access.
   To restrict 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 **MEGA Process, HOPEX IT Architecture and other HOPEX products.** To authorize only the **MEGA Process** and **HOPEX IT Architecture** modules to a user, enter: /RW'PRO;ARC'
5. Click **Apply**.

Modifying User Group Properties

You can modify 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 default connection group
  - group type (LDAP group, computed person group or persons directly connected to group)
  - persons owned in the group

    ☛ *See "Person Group Properties", page 42.*

    ☛ *See "Viewing Person Group Characteristics", page 78.*

    ☛ *See "Defining a Person Group", page 92.*

    ☛ *See "Defining a dynamic person group with LDAP", page 94.*

    ☛ *See "Defining a dynamic person group with a Macro", page 94.*
- login:
  - name
  - user code
  - status
  - accessible products (Command Line)
  - authentication mode

    ☛ *See "Properties of a Person Group Login", page 45.*

    ☛ *See "Viewing Login Characteristics", page 79.*

    ☛ *See "Defining the Login of a Person Group", page 97.*

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 Login Characteristics", page 79.*
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", page 69.*

2. In **Person Groups**, select the person group to be deleted and click **Delete** ⊗.

   ☛ *You can select more than one.*

   The **Delete Objects** dialog box 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 "Accessing Options", page 172).

Configuring Metamodel Access

With the **Metamodel Access** option (**Options > Repository** menu) , you can restrict the view of **HOPEX** objects or functions according to user skill level.

This option can be defined at environment, profile or user level according to the requirement.

Metamodel access levels are:

- **Beginner**
  For introduction to **HOPEX**. Only basic objects are visible. This level allows very simple modeling.
- **Intermediate** (default value)
  For standard use of **HOPEX**. Almost all object types, links and non-technical attributes are visible.
- **Advanced**
  For advanced use of **HOPEX**. All objects, links and non-technical attributes are visible, including those that require advanced skills for their use. Only object types and attributes which are present only for compatibility with previous versions are filtered. Certain technical object types are visible. The user can carry out simple customizations of the **HOPEX** platform.

  This level is used for example to access **Repository Activity** (see "Displaying Updates Made in the Repository", page 138).
- **Expert**
  This level displays all object types, links, and attributes, as well as the abstract metamodel. All HOPEX platform customizations are available.

  Specify this access level only for a highly expert user or a particular profile (e.g.: HOPEX Customizer).

Authorizing Deletion of a Published 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** 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.

Authorizing HOPEX Data Modification

💣 **This option should only be selected in certain highly specific cases, at debugging operations or at HOPEX request, and for a temporary period.**

This option authorizes modification of the **HOPEX** metamodel or any other **HOPEX** technical object. Modifying a **HOPEX** object can generate errors at **HOPEX** upgrades, import of correctives, etc.

💣 **Specify this access level only for a highly expert user or highly advanced profile.**

AUTHENTICATION IN HOPEX

Authentication is a process consisting of verifying that a person corresponds to his or her declared identity. In IT networks, authentication normally depends on a connection name and password.

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 lightens administrator workload relating to password management.

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

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

For more details on single sign-on, see:

- document "Single Sign-On in Windows 2000 networks" at the following Web address:
  http://technet.microsoft.com/fr-fr/library/bb742456.aspx
- technical article ***Unified Login Security Management EN***.

HOPEX proposes the following authentication modes:

- **MEGA** authentication
- **Windows** authentication, which corresponds to Single Sign On.
- **LDAP** authentication
- **Custom** authentication, specific to Web applications connection only

☛ *See the technical article **Web connection overloading and configuration EN***

Defining Default Authentication Mode

Authentication can be:

- managed within the **HOPEX** platform (by default)
- delegated to a third party service

To select your authentication mode, **MEGA** recommends that you use authentication systems resistant to security attack:

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

  ☛ *See the **Web connection overloading and configuration EN** technical article.*

- If your enterprise has an LDAP authentication system, it is preferable to manage your authentication using an LDAP directory.

  ☛ *See "Defining default authentication mode to LDAP", page 103.*

- If you have no standard authentication system in your enterprise, you can use the authentication system managed in HOPEX, less resistant to security attack.
  This is the authentication mode defined by default at installation, its value is "Standard".

  ☛ *See "Viewing default authentication mode", page 103.*

Viewing default authentication mode

In the environment options, you can consult and modify the default **Defined Authentication Mode**.

To view default authentication mode:

1. Access environment options.

   ☛ *See "Modifying options at environment level", page 172.*

2. In the options tree, expand the **Installation** folder and select **User Management**.
3. In the right pane, consult the value of the **Authentication Mode** option. By default at installation, "Standard" is the HOPEX authentication mode.

Defining default authentication mode to LDAP

Users are managed in an LDAP directory and authentication is managed by the LDAP directory.

☛ *Authentication mode of users already created is not impacted. Only users created after the default authentication mode change are concerned.*

To define default LDAP authentication mode:

1. Access environment options.

   ☛ *See "Modifying options at environment level", page 172.*

2. In the options tree, expand the **Installation** folder and select **User Management**.
3. In the right pane, specify "LDAP" for the **Authentication Mode** option.

Defining user authentication mode

User authentication mode is defined on the login by the **Authentication Mode** parameter. The value of this parameter is inherited at user creation from the value of the **Authentication Mode** option defined in the environment options (see "Viewing default authentication mode", page 103).

To define user authentication mode, see "Defining the Login of a Person", page 86.

Windows Authentication

Synchronization with a company directory

Active Directory is a directory service designed principally for Windows environments.

Active Directory is a directory referencing persons (name, first name, telephone number, etc) and objects such as servers, printers, applications, databases, etc.

Active Directory enables inventory of all information concerning the network (users, machines and applications). Active Directory is at the heart of all network architecture and its purpose is to enable users to find and access any resource identified by the service.

Active Directory is based on standards DNS, LDAP, Kerberos, etc.

Associating a Windows user with a HOPEX user manually

You can connect a single **HOPEX** user to a Windows user.

To indicate the Windows identifier of a **HOPEX** user:

1. Access the Login properties pages of the user.

   ☛ *See "Viewing Login Characteristics", page 79.*
2. Select **Characteristics**.
3. In the **Authentication Mode** field drop-down list, select "Windows". The **Windows Login** field appears.
4. In the **Windows Login** field, enter the user reference in the Active Directory in the following format: Domain name\User login:

   `Example: Domain01\TAD`
5. Click **Save**. The domain name disappears from the field and only the user login is displayed (in lower caps).

   `Example: tad`

Single sign-on precautions

A system repository in which all users have been changed to Single Sign On connection mode (Windows) can no longer be opened outside the company in which the repository was created.

If you want the repository to be opened outside your company (by the **HOPEX** technical support team for example), ensure that at least one user remains in **HOPEX** authentication mode.

LDAP Authentication

☛ *LDAP authentication is available only if you have technical module **HOPEX Power Supervisor**.*

An LDAP directory enables storage of user data of the enterprise.

HOPEX Administration allows you to create users authenticated at LDAP server level.

> ☛ *Only users (example: Administrator) with a **HOPEX Administrator** or **User Management Web Administrator** profile can enter LDAP data, see "The Administration profiles provided", page 26.*

Accessing LDAP server management

> ☛ *The **LDAP Servers** folder is available only if you are connected with a user with the HOPEX Administrator profile (example: **Administrator**), see "The Administration profiles provided", page 26 and that LDAP authentication is the user default authentication mode, see "Defining default authentication mode to LDAP", page 103.*

To access LDAP server management:

- From the **Administration** desktop, select the **LDAP Servers** sub-folder.

> ☛ *See "Accessing the User Management Pages", page 69.*

Configuring LDAP authentication

To configure LDAP authentication:

1. Create an LDAP server in **HOPEX Administration**.

   > ☛ *See "Creating an LDAP server", page 105.*

2. Specify parameters of your LDAP server.

   > ☛ *See "Configuring the LDAP server", page 106.*

3. (Optional) You can:
   - configure LDAP parameters

     > ☛ *See "Configuring an LDAP parameter", page 107.*

   - modify LDAP import parameters

     > ☛ *See "Modifying LDAP directory import content", page 108.*

4. Check the configuration of the LDAP server.

   > ☛ *See "Checking the configuration of an LDAP server", page 109.*

When LDAP authentication has been configured:

- you can import persons from the LDAP directory.

  > ☛ *See "Importing persons from an LDAP server", page 109.*

- or you can manually map a **HOPEX** user group with a user group declared in your LDAP server.

  > ☛ *See "Associating a HOPEX user group with an LDAP user group", page 110.*

  > ☛ *When connecting to **HOPEX**, the authentication service uses the **HOPEX** Login and password of the user to authenticate the user with the list of available LDAP servers.*

Creating an LDAP server

The LDAP server is the server on which the LDAP directory is installed.

The LDAP directory can be an Active Directory directory.

To create an LDAP server:

1. Access LDAP server management.

   > ☛ *See "Accessing LDAP server management", page 105.*

2. In the LDAP server menu bar, click **New** ⊕.
3. In the creation of LDAP server dialog box, enter the **Name** of the LDAP server and click **OK**.
   The new LDAP server appears in the list of LDAP servers.
   You must configure the LDAP server, see "Configuring the LDAP server", page 106.

Configuring the LDAP server

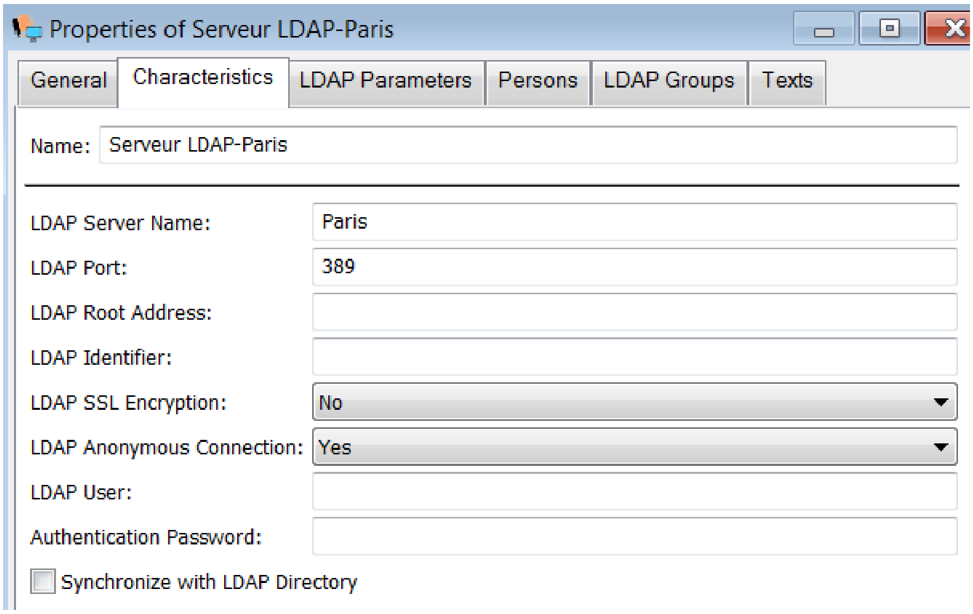
LDAP server configuration is restricted to users with a HOPEX Administrator or User management Administrator profile.

To configure an LDAP server:

Prerequisite: the LDAP server is already created.

☛ *See "Creating an LDAP server", page 105.*

1. Access the LDAP server management pages.
   ☛ *See "Accessing LDAP server management", page 105.*
2. Select the new LDAP server and click **Properties**.



Properties of Serveur LDAP-Paris

Name:	Serveur LDAP-Paris
LDAP Server Name:	Paris
LDAP Port:	389
LDAP Root Address:	
LDAP Identifier:	
LDAP SSL Encryption:	No
LDAP Anonymous Connection:	Yes
LDAP User:	
Authentication Password:	

☐ Synchronize with LDAP Directory

3. In **Characteristics**, complete the following fields:
   - **LDAP Server Name**: name of the server hosting the LDAP directory.
   - **LDAP Port**: LDAP communication bridge

     `Example: 389`
   - **LDAP Root Address:** root address of LDAP server. This is an important attribute to limit query for a user in the LDAP directory or to address a particular forest.
   - **LDAP Identifier**: this is the LDAP attribute enabling unique identification of a user

     `Example: SAMAccountName, UID`
   - **LDAP SSL Encryption**: select "Yes" if you want LDAP directory connection to be SSL protocol encoded
   - **LDAP Anonymous Connection**: if you select "No", you must specify the user via which LDAP directory connection will be made, as well as the user password

     ☛ *Only an administrator user can connect anonymously to an LDAP server.*
   - **LDAP User**: enter the identifier of the LDAP user used for LDAP directory connection. If connection is anonymous, this field should not be completed.

     ☛ *This user must have reading rights on data that **HOPEX** needs to access (example: LDAP person group, membership of a group in LDAP, e-mail in LDAP, etc.).*
   - **Authentication Password**: enter the password of the LDAP user used for LDAP directory connection. If connection is anonymous, this field should not be completed.
   -
4. Click **Save**.
   The LDAP server is configured.

   You can also:
   - configure an LDAP parameter, see "Configuring an LDAP parameter", page 107.
   - modify content of LDAP directory import, see "Modifying LDAP directory import content", page 108.

Configuring an LDAP parameter

An LDAP parameter is a parameter that exists in the LDAP directory and is associated uniquely with a **HOPEX** attribute.

Configuring an LDAP parameter is useful when importing persons from an LDAP directory. This configuration enables initialization of attributes (of the person or login created in **HOPEX**) corresponding to parameters with values stored in the LDAP directory.

```
Example: the "E-mail address" MetaAttribute of the person
is initialized with the "mail" LDAP parameter of the person
in the "Active Directory" LDAP directory (if mapping has
been carried out).
```

To configure an LDAP parameter:

1. Access the LDAP server management pages.

   ☛ *See "Accessing LDAP server management", page 105.*
2. Select the LDAP server for which you want to configure an LDAP parameter and click **Properties** .
3. In **LDAP Parameters**, click **New** .

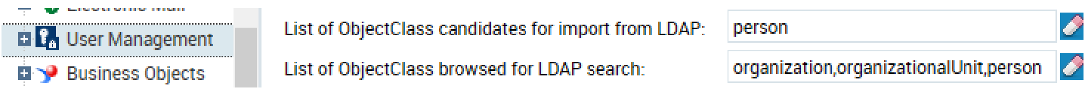
   ☛ *The LDAP parameter enables pre-completion of characteristics of a person corresponding to the LDAP parameters.*
4. Enter the **Name** of the LDAP parameter (example: Mail), then click **Properties** .
5. (Optionally, access the "expert" metamodel) Select **Index on Persons**, so that the parameter value enables unique identification of a person. If a person in **HOPEX** has the same e-mail as a person defined in the LDAP directory, this person is reused (instead of creating a new person and risk duplicating the same person).
6. (Optionally, access the "expert" metamodel) Select **Is available for search** so that an e-mail address can be entered in the import entry area.

   ```
   Example: if you enter ctodd@mega.com, you should find Clara
   TODD.
   ```
7. In the **MetaAttribute** field, click the arrow and select **Connect MetaAttribute**.
8. Execute a query on the MetaAttribute (example: E-mail).
   When importing persons from the LDAP directory, the LDAP parameter (example: mail) will initialize the MetaAttribute (example: E-mail address).

Modifying LDAP directory import content

You can modify LDAP directory import content:

- export candidate objects:
  This option enables definition of the type of objects to be imported from the LDAP directory.
  Default value: person.
- the list of objects browsed for LDAP query
  This option enables addition to the import of a particular person and/or persons of a team ("organization").
  Default value: organization,organizationalUnit,person



List of ObjectClass candidates for import from LDAP: person

List of ObjectClass browsed for LDAP search: organization,organizationalUnit,person

To define content of LDAP directory import:

1. Access environment options.

   ☛ *See "Modifying options at environment level", page 172.*
2. In the options tree, expand the **Installation** folder and select **User Management**.

3. (Optional) In the right pane, modify the **List of ObjectClass candidates for import from LDAP** option.
   To import objects other than persons (default value), for example resources or org-units, specify this in this field. Objects should be separated by commas.
   Everything that is imported creates occurrences of persons with login.
4. (Optional) In the right pane, modify the **List of ObjectClass browsed for LDAP query** option.
   To add a person or organization to the import, enter the name of the person or organization (example: Quality) in the field.
   The result is the list of ObjectClass candidates for import from LDAP, that is, persons by default.

Checking the configuration of an LDAP server

To check the configuration of an LDAP server:

1. Access LDAP server management.

   ☛ *See "Accessing LDAP server management", page 105.*
2. In the edit area, select the LDAP server and click **LDAP Check**.

Importing persons from an LDAP server

The import of persons from an LDAP directory enables initialization of attributes (of the person or login created in **HOPEX**) corresponding to parameters with values stored in the LDAP directory.

☛ *See "Configuring an LDAP parameter", page 107.*

Example: the "E-mail address" MetaAttribute of the person is initialized with the "mail" *LDAP parameter* of the person in the LDAP file (if mapping has been carried out).

📖 *An LDAP parameter is a parameter that exists in the LDAP directory and is associated uniquely with a HOPEX attribute. For example, "mail" is a parameter of the "Active Directory" LDAP directory and can be associated with the e-mail of the person.*

To import persons from an LDAP directory:

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

   ☛ *See "Accessing the User Management Pages", page 69.*
2. In **Persons**, click **Import From LDAP**.
3. The **LDAP Import Wizard** appears.
4. In the **LDAP Server** field, click the drop-down menu and select the server from which you want to import persons.

   ☛ *The LDAP server must be created, see"Creating an LDAP server", page 105.*
5. In the **Queried Element** field, enter the queried character string.

   Example: Support service.
6. Names resulting from the query are listed.
7. Select the persons you want to import.
8. Click **OK**.

Associating a HOPEX user group with an LDAP user group

> 📖 *An LDAP group defines a group or organization in the LDAP directory or Active Directory. It contains a list of users that can potentially connect to the application.*

Having configured the LDAP server (see "Configuring the LDAP server", page 106), you must specify a user group authenticated with the LDAP directory.

> ☛ *If a default person group is defined (example "Guests") and no LDAP group is specified, a person authenticated in LDAP (with the **Belongs to a person group** option selected, see "Person Properties", page 35) automatically belongs to the group defined by default (example: "Guests").*

To specify a user group authenticated with the LDAP directory:

1. Access the LDAP server management pages.

   > ☛ *See "Accessing LDAP server management", page 105.*

2. Select the LDAP server you want to configure and click **Properties** .
3. In the LDAP server properties pages, select **LDAP Groups**.
4. Click **Connect** to connect the existing LDAP user group.
   The LDAP Group query wizard appears.
5. (Optional) In the query field, enter the character string to be queried.
6. Click **Find** .

   > ☛ *To execute an advanced query, click **Open Query Tool** .*

   Query results are displayed.
7. Select the LDAP user group and click **Connect**.

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

   The LDAP user group appears in the list.
8. Connect the HOPEX user group to the LDAP user group.

   > ☛ *See "Defining a dynamic person group with LDAP", page 94.*

Authentication and a user created on the fly

When a user has been created on the fly, the LDAP parameters can be used as indexing identifier (**Index on Person** attribute, see "Configuring an LDAP parameter", page 107) to check that a person with an attribute with the same value as the LDAP directory already exists in **HOPEX**.

Example of use:

Anne, responsible for sending questionnaires, wants to send a questionnaire. If one of the addressees does not exist:

- Anne can create the person (example: "Thomas KOCH" with e-mail "tkoch@mega.com")
- Anne cannot create the login of Thomas Koch since she is not an administrator.

When Thomas KOCH connects to **HOPEX** (Web Front-End), with tkh:

1. The authentication service authenticates tkh with the LDAP directory: the "mail" parameter exists and is indexing identifier type (**Index on Person** is selected),

2. The authentication service checks if a person already has this e-mail.

   ☛ *Answer: Yes.*

3. The authentication service creates the login associated with the person.

If Thomas KOCH has assignments to complete the questionnaire, he can connect to the application to complete this questionnaire.

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", page 112
- "Modifying the life of the first connection link", page 113
- "Modifying password management configuration", page 113
- "Reinitializing a User Password", page 114

Initializing a user Web account

Prerequisites

Before initializing the Web account of a user:

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

  ☛ *See "Viewing Person Characteristics", page 76.*

- check that the following options relating to Web applications are specified:
  - "Specifying the Web applications access path", page 176
  - "Specifying SMTP configuration", page 176

  ☛ *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", page 69.*

2. Select the **Persons** sub-folder.
3. In the Persons list, select the person concerned.
4. Click **Initialize the 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 life of the first connection link, see "Modifying the life of the first connection link", page 113.*

Modifying the life of the first connection link

To modify the life of the first connection link:

1. Access environment options.

   ☛ *See "Modifying options at environment level", page 172.*

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 management configuration

To modify configuration linked to password management:

1. Access environment options.

   ☛ *See "Modifying options at environment level", page 172.*

2. In the options tree, expand the **Installation** folder and select **User Management**.
3. In the right pane, you can modify default configuration of options:
   - **Number of tries before password invalidation**.

     ☛ *Default value: 3*

   - **Password expiry**

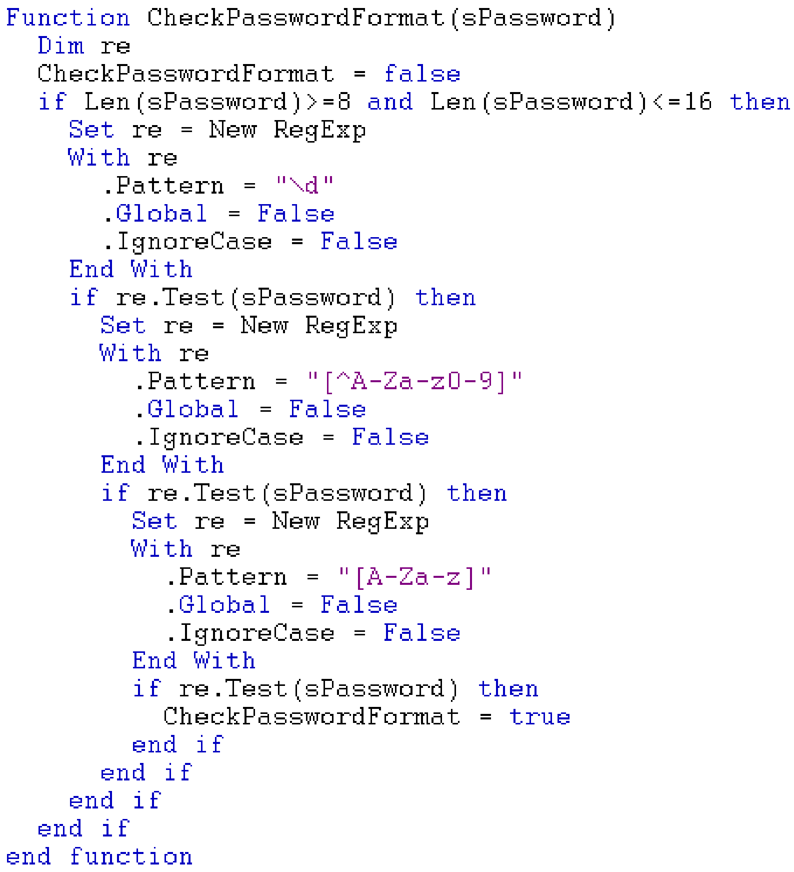
     ☛ *Default value: 40 days*

Modifying password definition rules

To modify password definition rules:

1. Edit the **CheckPasswordFormat** macro.

2. Overload the macro **CheckPasswordFormat** with your definitions. By default this macro imposes that the password should comprise:
   - between 8 and 16 characters
   - at least one letter
   - at least one figure
   - at least one special character



```
Function CheckPasswordFormat(sPassword)
  Dim re
  CheckPasswordFormat = false
  if Len(sPassword)>=8 and Len(sPassword)<=16 then
    Set re = New RegExp
    With re
      .Pattern = "\d"
      .Global = False
      .IgnoreCase = False
    End With
    if re.Test(sPassword) then
      Set re = New RegExp
      With re
        .Pattern = "[^A-Za-z0-9]"
        .Global = False
        .IgnoreCase = False
      End With
      if re.Test(sPassword) then
        Set re = New RegExp
        With re
          .Pattern = "[A-Za-z]"
          .Global = False
          .IgnoreCase = False
        End With
        if re.Test(sPassword) then
          CheckPasswordFormat = true
        end if
      end if
    end if
  end if
end function
```

Reinitializing a User Password

Prerequisite:

Before reinitializing a password, check that the following options relating to Web applications are specified:

- "Specifying the Web applications access path", page 176
- "Specifying SMTP configuration", page 176

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

To reinitialize the password of a user:

1. Access the user management page.

   ☛ *See "Accessing the User Management Pages", page 69.*

2. Select a **Persons** sub-folder.
3. In the edit area, select the person for whom you want to initialize the password.
4. Click **Initialize the 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.

Specifying the Data Language

The data language is the language with which the user connects by default the first time. If the user changes 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 or 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 interface language in Web applications, see "Modifying the interface language in Web applications at environment level", page 178.
- the data language at environment level, see "Modifying the data language in Web applications at environment level", page 179.

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", page 83.*

☛ *See "Viewing Person Group Characteristics", page 78.*

MANAGING WORKSPACES

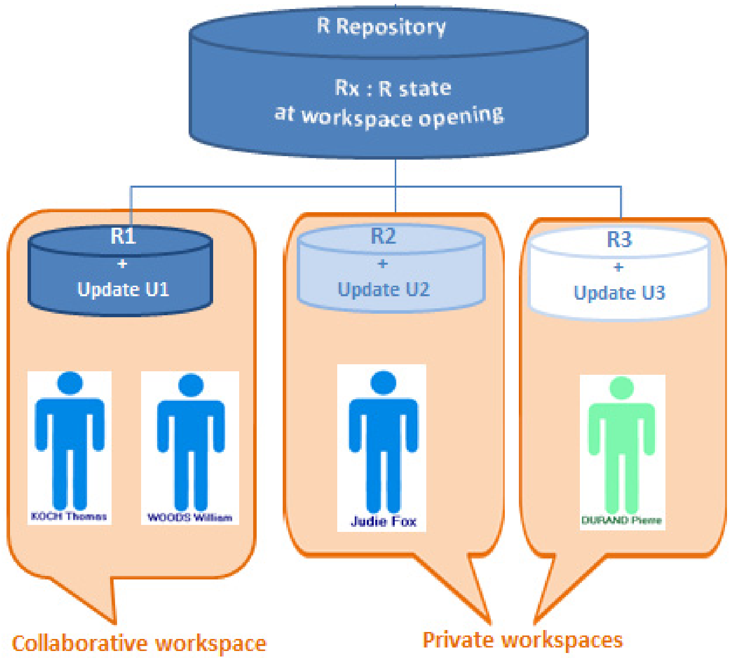
Workspaces are managed by the administrator.

The following points are covered here:

Private Workspace Principle

In a traditional management application, the user cannot control the opening duration of his/her workspace: the end of a data entry corresponds to a definitive save of his/her work.

With **HOPEX** the user controls management of his/her workspace: opening, closing, dispatch, refresh.



Private Workspace

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", page 123.*

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", page 142.*

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", page 126.*

HOPEX allows several users to work at the same time.

Collaborative Workspace

The user can also share his/her private workspace with other users before dispatching his/her modifications and making public his/her work to all other users. To do this, the user creates a **Collaborative Workspace** from his/her private workspace.

☛ *See the **HOPEX Common Features** guide, section "Working in a Collaborative Workspace".*

A user can, in parallel:

- have a private workspace
- be the owner of several collaborative workspaces
- be invited to participate in as many collaborative workspaces as he/she wishes.

USING YOUR 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
- resume work in a collaborative workspace

  ☛ *This option is available with **HOPEX Collaboration Manager** only.*

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. (If you have a password) In the **Password** field, enter your password.

   > ☛ *If you have lost your password, click **Forgot Password**, see "Reinitializing Your Password", page 9.*

4. In the drop-down menu for environments, select your work environment.

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

5. Click **SIGN IN**.
   When you have been authenticated, a new dialog box appears.
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. 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.*

   > ☛ *If you already have a private workspace open, the repository is automatically selected and this field is grayed. To change repository, you must first dispatch or discard your current private workspace.*

8. In the profile drop-down menu, select the profile with which you want to work.
   If you have **HOPEX Collaboration Manager**, go to step 10.
9. Click **LOGIN**.
   A private workspace is created and your desktop opens.
10. If:
    - you do not have a collaborative workspace available, the **Workspace** field is not available. Click **LOGIN**.

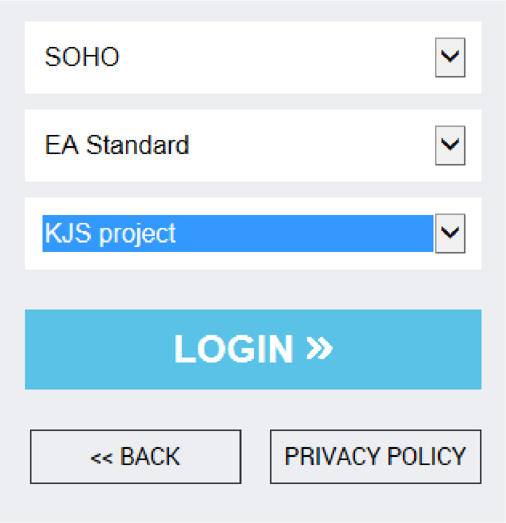
    A private workspace is created and your desktop opens.

    > ☛ *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.*

    - you have at least one collaborative workspace available, in the **Workspace** field, select **Access Private Workspace** or select the collaborative workspace to which you want to connect, or select

Create Private Workspace (if one has not already been created). Click **LOGIN**.

☛ *A user has at most one private workspace in progress in an environment, but can have in parallel several available collaborative workspaces.*



SOHO

EA Standard

KJS project

Your desktop opens and objects in Check Out in the collaborative workspace are available. Authorized participants can update these objects.

A private workspace comprises a set of files located in a sub-folder of the repository:

"<EnvironmentName>\DB\<RepositoryName>\<RepositoryName>.Transactions\xyz.*"

where "xyz" represents the user code.

Note that a private workspace cannot be separated from its repository (these files cannot be used independently).

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 the modifications you have made in your *session* since the last save, see "Edit area", page 13.

☛ *These modifications are not saved in the repository. To save your modifications in the repository, you must dispatch these modifications, see "Dispatching Your Work", page 123.*

HOPEX Repository State Changes

The integrity of the repository is assured by successive changes in its state.

☛ *See example "Private Workspace Life: Example", page 135.*

When repository updates are executed in a private workspace, they are only visible to other users when the user dispatches his/her work.

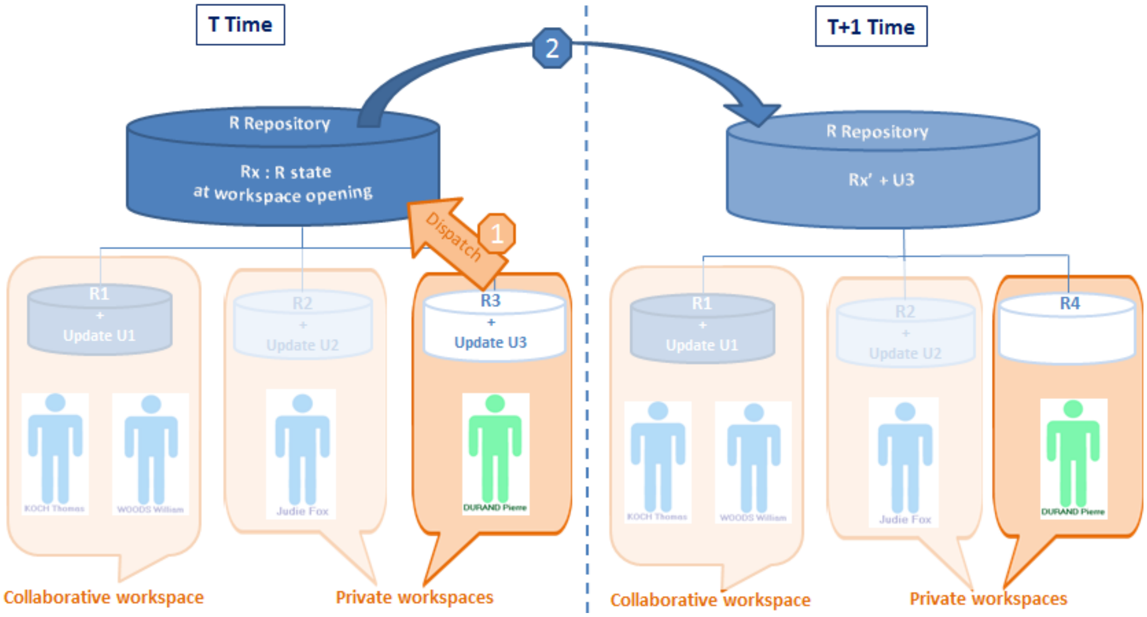
The repository changes from state N to state N+1 with memorization of new data related to the previous situation (state N).

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, or the work of participants in a collaborative workspace.



Dispatch allows:

- a user to make available to other users the modifications he/she has made to the repository.
- users of a collaborative workspace to make available to other users the modifications they have 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.

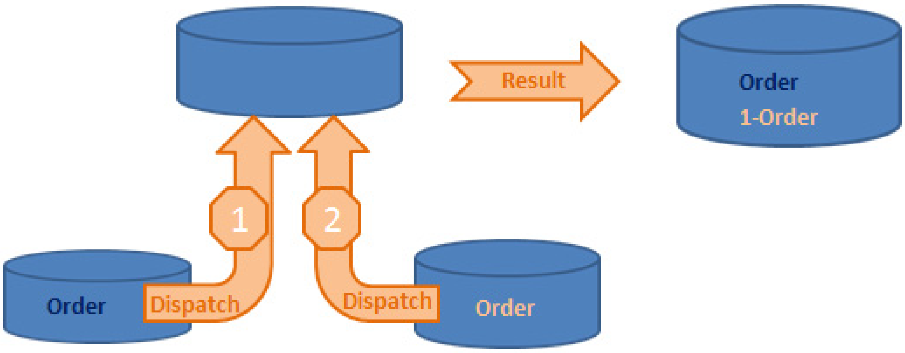
☛ *See "Dispatch Conflicts", page 124.*

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.

Links related to 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.

☛ *For more information on MetaAssociation uniqueness check, see the* ***HOPEX Power Studio*** *- Imposing MetaAssociation Uniqueness.*

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.

A user can refresh his/her data:

- in his/her private workspace
  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.
- in a collaborative workspace.
  The system then creates a new collaborative workspace for all participants in the collaborative workspace, into which is automatically imported the collaborative workspace log containing modifications previously made by participants.

  > ☛ ***HOPEX** recommends that you warn other participants before executing refresh.*

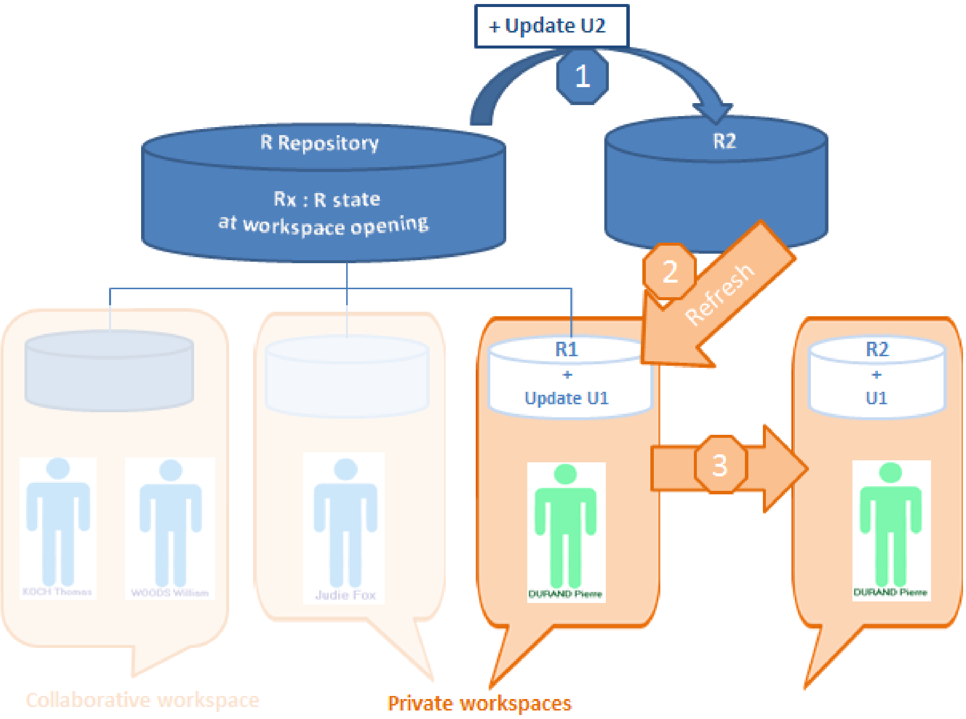
  Refreshing allows a user to incorporate repository and system repository changes made by other users, without dispatching current work.

Refreshing a private (or collaborative) workspace.

- does not update repository or system repository state.
- does not unlock objects modified in the private workspace.

> ☛ *see "Managing locks", page 142.*

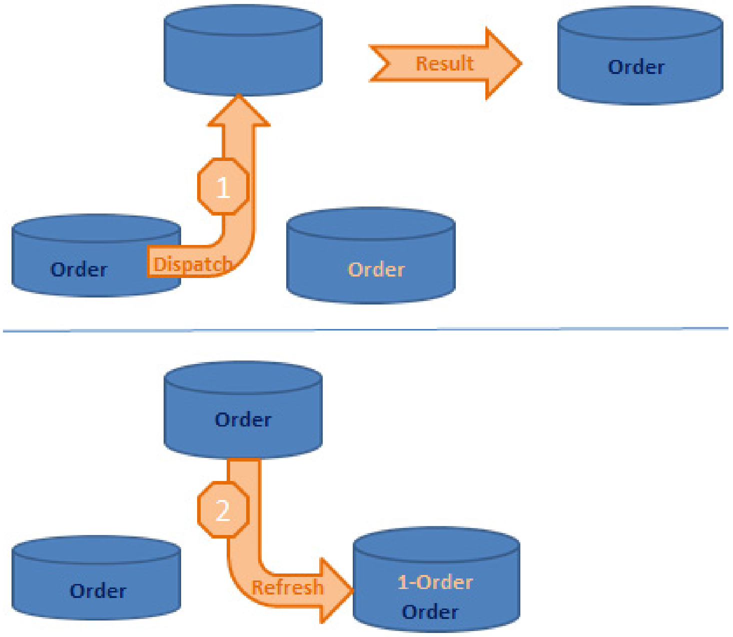
When a user resumes work on his/her private space that has lasted longer than the limit set by the administrator (the default is 6 days), **HOPEX** proposes that the user refreshes or dispatches his/her work.


+ Update U2
1
R Repository
Rx : R state
at workspace opening
R2
2
Refresh
R1
+
Update U1
3
R2
+
U1
KOCH Thomas
WOODS William
Judie Fox
DURAND Pierre
DURAND Pierre
Collaborative workspace
Private workspaces

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", page 124 and "Rejects When Dispatching", page 125.*



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 (from a private or collaborative workspace) cancels all modifications made since the last dispatch. *Discard* of work causes loss of work carried out since opening of the private or collaborative workspace, including modifications to the desktop. A warning message reminds the user of this. Use discard with care.

Discarding work from a private workspace

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 **Repository** tool group, select **Tools > Export**.*

2. In the **Repository** tool group, select **Dispatch > Discard**.

   ☛ *You can also discard your private workspace at disconnection, see "Exiting a Session", page 129 (choose not to dispatch modifications).*

Discarding work performed in a collaborative workspace

Only the collaborative workspace **Owner** can discard the work performed in the collaborative workspace.

☛ *See the **HOPEX Common Features** guide, section "Working in a Collaborative Workspace".*

From your Web desktop, to discard the work performed in the collaborative workspace:

1. (Optional) It is advisable to export the work performed in the collaborative workspace before confirming the discard.

   ☛ *In the **Repository** tool group, select **Tools > Export**.*

2. In the **Repository** tool group, select **Collaborative workspace > Discard**.

   ☛ *You collaborative workspace must be in Closed status to be discarded.*

Exiting a Session

When you exit **HOPEX**, you close your session. From:

- your private workspace 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.
- a collaborative workspace you can:
  - keep modifications you have made

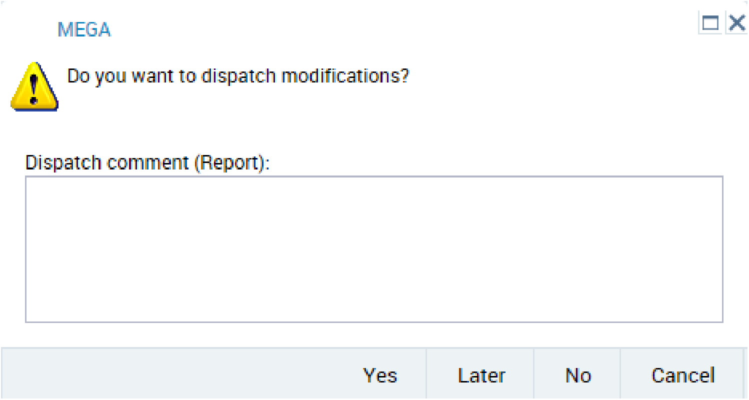
    ☛ *These modifications are saved in the collaborative workspace. These modifications are not saved in the repository until the collaborative workspace is closed.*

  - cancel modifications you have made.

Exiting a session from a private workspace

From your Web desktop, to exit your work *session*:

1. From your **HOPEX** desktop , click **Logout** .
   The **HOPEX** exit dialog box appears.



MEGA

Do you want to dispatch modifications?

Dispatch comment (Report):

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.
   - **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. You can use this option if you want to view data quickly and 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.

     ☛ *Click **Cancel** to not exit your private workspace.*

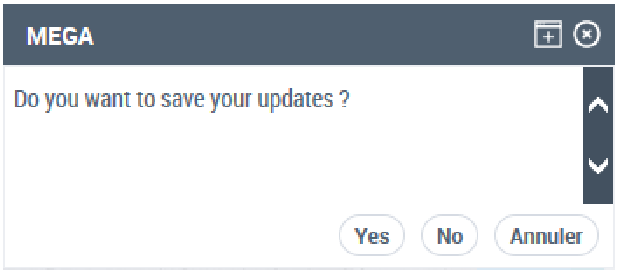
Exiting a session from a collaborative workspace

Exiting **HOPEX** from a collaborative workspace is the same whether you are its owner or not.

For as long as the collaborative workspace is not closed, participants can exit and rejoin the collaborative workspace at any time.

From your Web desktop, to exit your work *session*:

1. From your **HOPEX** desktop , click **Logout** .
   The **HOPEX** exit dialog box appears.



MEGA

Do you want to save your updates ?

2. Click:
   - **Yes** to save your modifications in the collaborative workspace.
     You will be able to continue your modifications in a subsequent work session.

     These modifications are not saved in the repository. Users not participants in the collaborative workspace do not see these modifications.
   - **No** to cancel your modifications in the collaborative workspace.
     Your modifications are not saved in the collaborative workspace, but the latter remains available to carry out other updates.

     ☛ *Click **Cancel** to remain in your collaborative workspace.*

WORKSPACE ADMINISTRATION

You can view the list of current workspaces and their characteristics (owner, delay, status).

See:

- "Accessing the Management Page for Workspaces", page 132
- "Deleting a Workspace", page 134

Accessing the Management Page for Workspaces

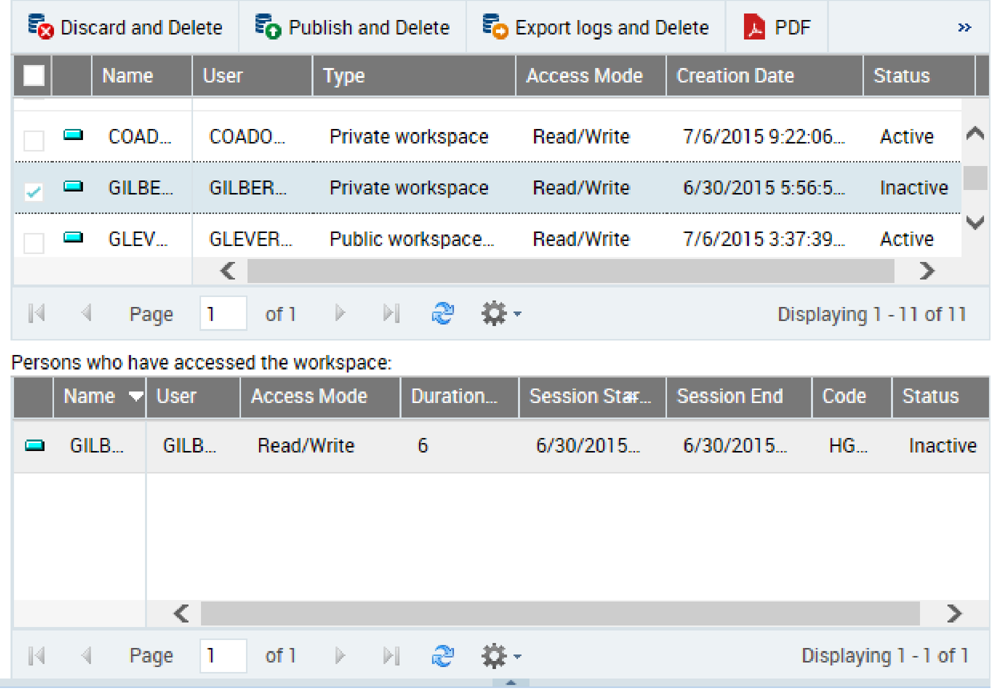
To access the list of current workspaces in an environment:

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

   ☛ *See "Connecting to the Administration Desktop", page 6.*

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.



□		Name	User	Type	Access Mode	Creation Date	Status
□		COAD...	COADO...	Private workspace	Read/Write	7/6/2015 9:22:06...	Active
☑		GILBE...	GILBER...	Private workspace	Read/Write	6/30/2015 5:56:5...	Inactive
□		GLEV...	GLEVER...	Public workspace...	Read/Write	7/6/2015 3:37:39...	Active

Persons who have accessed the workspace:

	Name	User	Access Mode	Duration...	Session Star...	Session End	Code	Status
	GILB...	GILB...	Read/Write	6	6/30/2015...	6/30/2015...	HG...	Inactive

The management page for workspaces currently in progress details the following for each workspace:

☛ *To sort workspaces according to a column, click the header of the corresponding column.*

☺ *You can also arrange columns in the order you want. To do this, click the header of the column to be moved and, holding down the mouse button, move it to the required position.*

- the **User** of the workspace
- the **Type** of workspace:
  - "Private Workspace":

    The user can modify data. His/her updates are kept in his/her private workspace until dispatched.
  - "Public Workspace (micro)":

    The user can modify data. As soon as he/she saves his/her updates, they are visible to other users.

    The user sees immediately the updates of other users.
- 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
  - enabled
  - disabled

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

- for a collaborative workspace, all the users who have accessed the workspace:
  - the **User** who owns 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 **Code**
  - the user **Status**
- for a private workspace:
  - the **User** of the workspace
  - the **Access Mode** of the workspace, for example:
  - its **Duration** in days
  - the start date and time of the last session
  - the end date and time of the last session
  - the user **Status**

Deleting a Workspace

The **HOPEX** administrator can delete a private workspace when this is passive.

To delete a workspace:

1. Access the workspace management page.

   ☛ *See "Accessing the Management Page for Workspaces", page 132.*

2. Select the workspace that 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_YYYY-MM-DD_hh.mm.ss) before discarding it and deleting it.

     ```
     XXX: Code of the user who owns the deleted workspace
     YYYY-MM-DD: dispatch date (year-month-day)
     hh.mm.ss: deletion time (hour.minute.second)
     ```

     ☛ *You, and the owner of the workspace, receive an e-mail with the deleted workspace log.*

     ☛ *The workspace logfile is saved in the sub-folder of the environment workspace directory \Db\NameRepository\NameRepository.Transactions\CCC_YYYY-MM-DD_hh.mm.ss*

     ```
     CCC: Code of the administrator who deleted the workspace
     ```

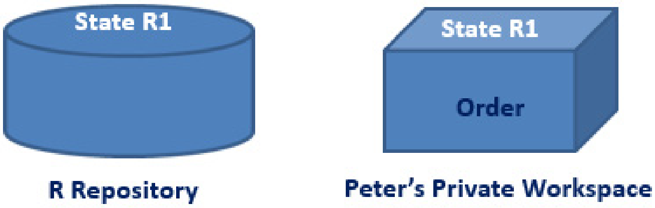
   - **Publish and Delete** if you want to keep the work performed in the workspace.

   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

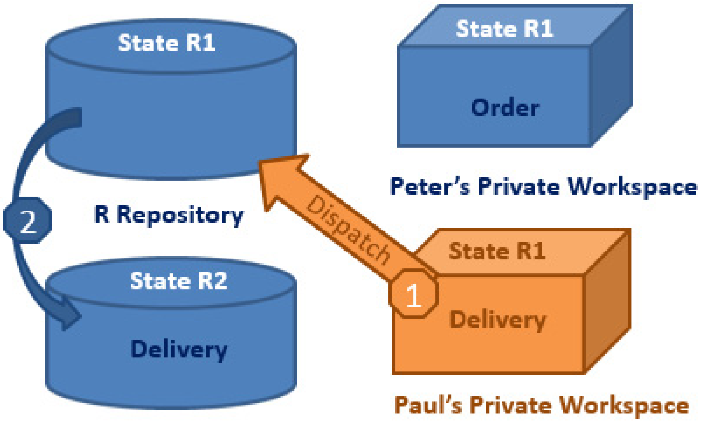
To illustrate how private workspaces work, the following is an example of some steps in the work of several users:

Private Workspace 1



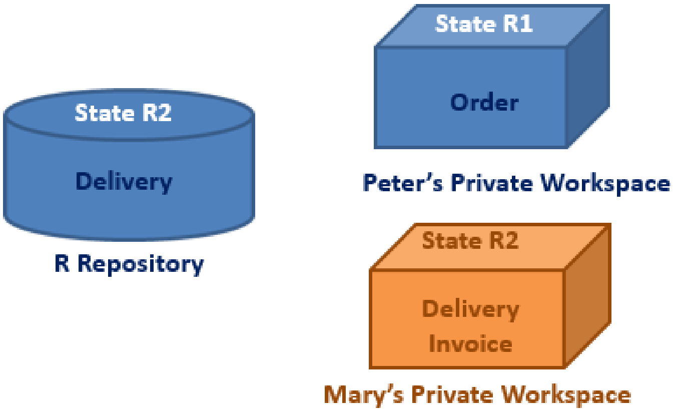
- Peter opens a private workspace, his repository view is state "n" (R1).
- He creates the "Order" message, which he links to the "Customer" org-unit.
- In parallel, Paul dispatches his private workspace...

Private Workspace 2



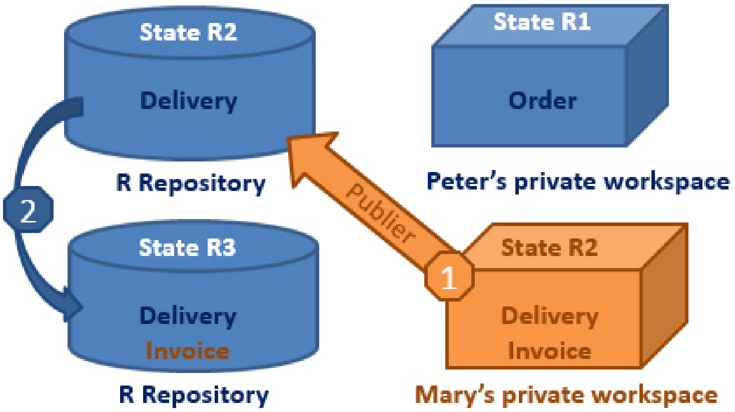
- Paul dispatched his work, which included the creation of the "Delivery" message, linked to the "Customer" org-unit.
- Paul's dispatch changes the repository to state "n+1" (R2).
- This new message is not seen from Peter's private workspace...

Private Workspace 3



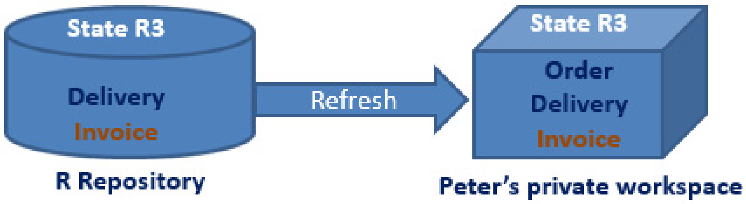
- Mary opens a new private workspace, her repository view is state "n+1" (R2).
- Mary creates the message "Invoice" connected to the "Customer" org-unit...

Private Workspace 4



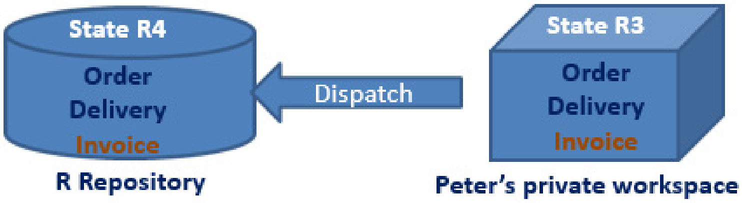
- Mary dispatches her work.
- The repository passes to state "n+2" (R3).
- Peter's view is still in state "n" (R1).
- Peter refreshes his private workspace...

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 work...

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.

Managing Updates

During their modeling work, users make additions to a **HOPEX** repository within their private workspace: they create objects, links between objects, diagrams, etc. Updates corresponding to user actions can be viewed in detail. You can back up all modifications made to a repository from a private workspace in a private workspace log, which can be exported in the form of a command file.

The following points are detailed here:

- "Displaying Updates Made in the Repository", page 138
- "Private Workspaces and Repository Size", page 139
- "Exporting a Private Workspace Log", page 141

Displaying Updates Made in the Repository

To display private workspaces dispatched and the content of their updates:

> ☛ *To access the content of the **Repository Management** pane, you must have **Expert** metamodel access (see "Configuring Metamodel Access", page 100).*

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

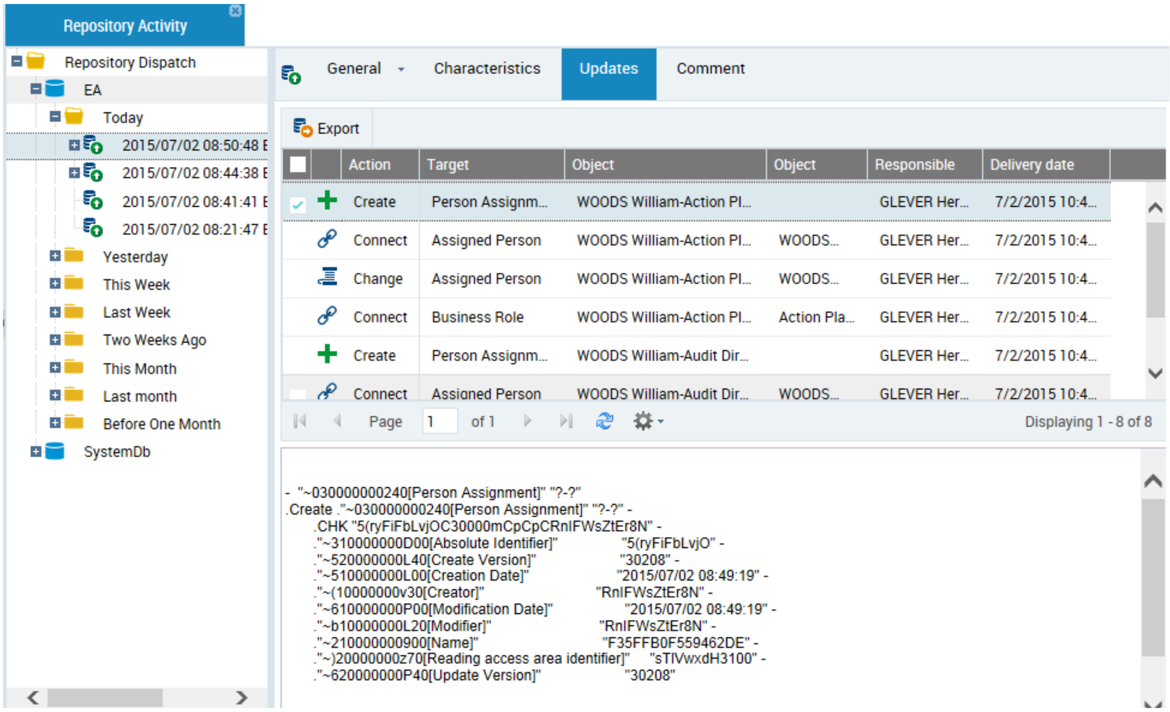
   > ☛ *See "Connecting to the Administration Desktop", page 6.*

2. In the **Repository Management** pane, click the **Repository Activity** sub-folder.
   All dispatches performed on the current repository and the system repository are detailed in the edit area.

   Dispatches are sorted by day, week and month.
3. Click a dispatch.
   The dispatch property pages are displayed in the edit area.
4. Click **Updates**.
   The **Updates** page details the content of the dispatch in the form of a list of actions displayed in chronological order.

5. Select a line to display the details of the action in the lower frame.

   ☛ *See "Exporting a Private Workspace Log", page 141.*



□	Action	Target	Object	Object	Responsible	Delivery date
☑	Create	Person Assignm...	WOODS William-Action Pl...		GLEVER Her...	7/2/2015 10:4...
	Connect	Assigned Person	WOODS William-Action Pl...	WOODS...	GLEVER Her...	7/2/2015 10:4...
	Change	Assigned Person	WOODS William-Action Pl...	WOODS...	GLEVER Her...	7/2/2015 10:4...
	Connect	Business Role	WOODS William-Action Pl...	Action Pla...	GLEVER Her...	7/2/2015 10:4...
	Create	Person Assignm...	WOODS William-Audit Dir...		GLEVER Her...	7/2/2015 10:4...
□	Connect	Assigned Person	WOODS William-Audit Dir...	WOODS...	GLEVER Her...	7/2/2015 10:4...

```
-  "~030000000240[Person Assignment]" "?-?"
.Create ."~030000000240[Person Assignment]" "?-?" -
       .CHK "5(ryFiFbLvjOC30000mCpCpCRnIFWsZtEr8N" -
       ."~310000000D00[Absolute Identifier]"          "5(ryFiFbLvjO" -
       ."~520000000L40[Create Version]"               "30208" -
       ."~510000000L00[Creation Date]"               "2015/07/02 08:49:19" -
       ."~(10000000v30[Creator]"                  "RnIFWsZtEr8N" -
       ."~610000000P00[Modification Date]"            "2015/07/02 08:49:19" -
       ."~b10000000L20[Modifier]"                  "RnIFWsZtEr8N" -
       ."~210000000900[Name]"                      "F35FFB0F559462DE" -
       ."~)20000000z70[Reading access area identifier]"     "sTIVwxdH3100" -
       ."~620000000P40[Update Version]"              "30208"
```

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", page 123 and "Refreshing Data", page 126.*

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", page 126 and "Discarding Work", page 128.*

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", page 123.*

All data accessed by a user is "frozen" for the duration of the private workspace.

Example:

```
For 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.

If a user does not want to dispatch his/her private workspace, refreshing it allows the user to avoid a large increase in the **HOPEX** repository size.

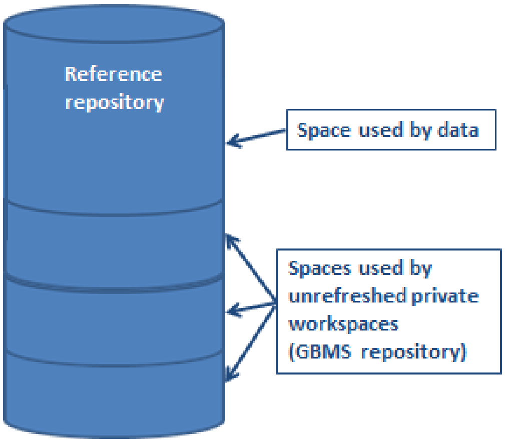
The administrator can set the maximum duration of a private workspace. If your private workspace exceeds the duration defined by your administrator, then each time you establish a connection, a message box appears asking you to dispatch or refresh your private workspace.

You can audit private workspaces with the **HOPEX Administration** application.

💣 **A private workspace that began before significant modifications were made may cause a considerable increase in repository size, since an image of the previous state of the modified elements is kept until the private workspace is refreshed.**

The default option when a user disconnects is indicated in the user configuration. It is defined for the entire environment.

The greater the number of private workspaces and the longer their duration, the more the volume of the temporary space (data) dedicated to private workspace data will increase. This volume can be reduced by repository backup or deletion, new repository creation or logical backup restoration.


Reference repository
Space used by data
Spaces used by unrefreshed private workspaces (GBMS repository)

Exporting a Private Workspace Log

You can create an export file (*private workspace logfile*).

The export file can be exported in format:

- **logfile text** (.mgr).
  Name format of the exported file is "OBJmmdd.mgl", where "mmdd" represents logfile export date month and day.
- **XML MEGA** (.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 repository dispatches.

   ☛ *See "Displaying Updates Made in the Repository", page 138.*

2. In the edit area, select a dispatch.
3. Click **Export** .
4. (Optional) If necessary, modify the data export file name and save folder proposed as default.
5. Select export format.
6. Click **Export**.
   A message prompts you to either open or save the file (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", page 142
- "Managing Locks on Objects", page 143

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 Lock Operating

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 lock (locked or otherwise)

  ☛ *See "Viewing locks on objects", page 144.*
- 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 lock (locked or otherwise)

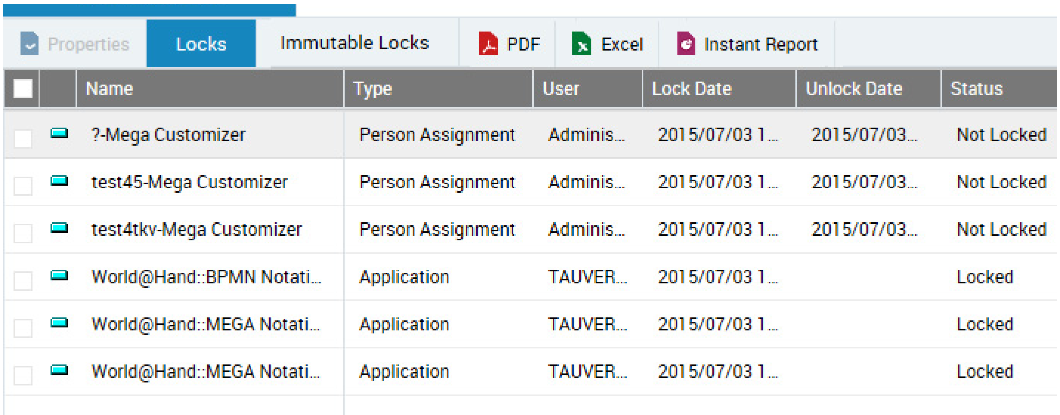
  ☛ *See "Managing immutable locks on objects", page 144.*

For each locked object, you can:

- view its properties

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.



□		Name	Type	User	Lock Date	Unlock Date	Status
□		?-Mega Customizer	Person Assignment	Adminis...	2015/07/03 1...	2015/07/03...	Not Locked
□		test45-Mega Customizer	Person Assignment	Adminis...	2015/07/03 1...	2015/07/03...	Not Locked
□		test4tkv-Mega Customizer	Person Assignment	Adminis...	2015/07/03 1...	2015/07/03...	Not Locked
□		World@Hand::BPMN Notati...	Application	TAUVER...	2015/07/03 1...		Locked
□		World@Hand::MEGA Notati...	Application	TAUVER...	2015/07/03 1...		Locked
□		World@Hand::MEGA Notati...	Application	TAUVER...	2015/07/03 1...		Locked

Viewing locks on objects

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

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

   ☛ *See "Connecting to the Administration Desktop", page 6.*

2. In the **Repository Management** pane, click the **Lock Management** sub-folder.
   The **Lock Management** page appears and lists the locks.
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. Select a lock and click **Properties** to view the details of the lock.
   To consult the history of object modifications, select **General >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", page 6.*

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.

MANAGING OBJECTS

The following points are covered here:

- ✓ "Importing - exporting a command file", page 148
- ✓ "Comparing and Aligning Objects Between Repositories", page 152 (function available with **HOPEX Power Supervisor** or **HOPEX Collaboration Manager**)
- ✓ "Managing UI Access (Permissions)", page 157 (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", page 148.*

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

> ☛ *For more details on .MG* file syntax, see "Command File Syntax", page 307.*

- 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", page 148
- "Exporting Objects", page 150

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", page 6.*

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. Click **Upload**.
6. 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.*

7. Select 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 succes** 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.*

8. In the **Checks** frame, 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 or backup logfile), 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.*

9. In the **Filters** frame, 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", page 124 and "Rejects When Dispatching", page 125.*

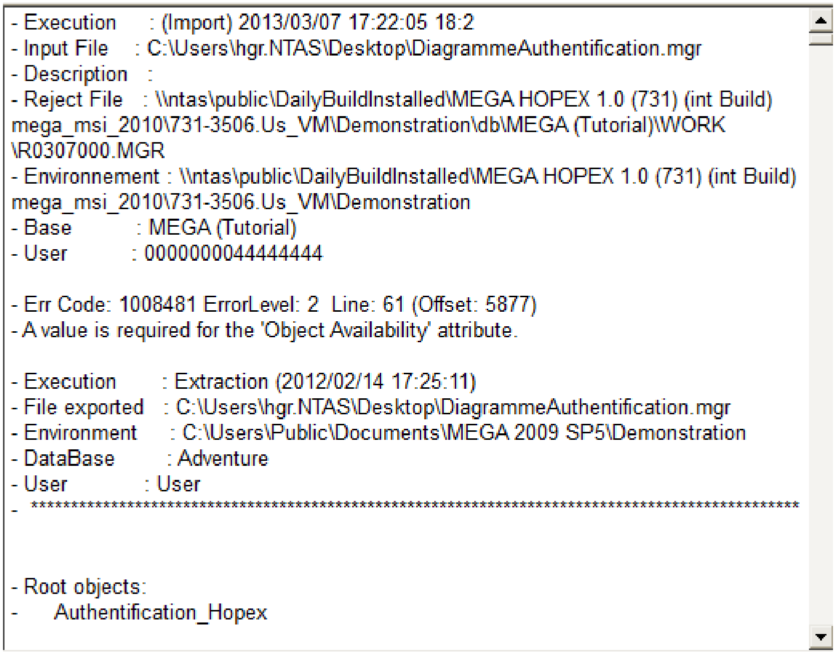
10. Click **Import**.
    The report page appears.

    When the import contains errors, a reject report file is generated.

11. (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 "Managing Options", page 323.*

   Case of a text file import (MGR, MGL): The report file appears and details all the rejects.



```
- Execution     : (Import) 2013/03/07 17:22:05 18:2
- Input File    : C:\Users\hgr.NTAS\Desktop\DiagrammeAuthentification.mgr
- Description   :
- Reject File   : \\ntas\public\DailyBuildInstalled\MEGA HOPEX 1.0 (731) (int Build)
mega_msi_2010\731-3506.Us_VM\Demonstration\db\MEGA (Tutorial)\WORK
\R0307000.MGR
- Environnement : \\ntas\public\DailyBuildInstalled\MEGA HOPEX 1.0 (731) (int Build)
mega_msi_2010\731-3506.Us_VM\Demonstration
- Base          : MEGA (Tutorial)
- User          : 0000000044444444

- Err Code: 1008481 ErrorLevel: 2  Line: 61 (Offset: 5877)
- A value is required for the 'Object Availability' attribute.

- Execution       : Extraction (2012/02/14 17:25:11)
- File exported   : C:\Users\hgr.NTAS\Desktop\DiagrammeAuthentification.mgr
- Environment     : C:\Users\Public\Documents\MEGA 2009 SP5\Demonstration
- DataBase        : Adventure
- User            : User
-  ************************************************************************************************



- Root objects:
-      Authentification_Hopex
```

Example of rejects file at MGR file import

Exporting Objects

You can export **HOPEX** objects from the **Administration** desktop:

You can export objects in the following formats:

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

  ☛ *For more details on .MGR file syntax, see "Command File Syntax", page 307.*

- **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", page 6.*

2. In the **Administration** tab, click the **Tools** pane.
   The management tree for tools appears.
3. In the tree, select the **XMG/MGL/MGR > Export** sub-folder.
   The **Hopex Objects Export - Parameterization** page appears.
4. In the **Export File** field, select the export file format.
5. In the **Options** frame, by default, two export configuration options are proposed:
   - **Include Objects of Merging** exports the technical objects resulting from merging objects (_TransferredObject).
   - **Propagate** exports the objects listed together with their dependent objects.
6. In the **Objects to export**, click **Add objects to list** .
   The query dialog box appears.
7. Start the query and select the appropriate objects in the result window.
8. Click **OK**.
   The objects appear in the list of objects to be exported.

   You can carry out this procedure several times, allowing you for example to export objects of different types.

   > ☛ *In the event of an error, click **Remove objects from list** to delete an object from the list.*
9. When selection is complete, click **Export**.
   The export file is exported.
10. (Optional) If required, in the **Export File** field, click the arrow and select **Open** to read the contents of the export file.
11. Click **OK**.
    A message appears.
12. Click **Save**.
    The exported file can then be imported into another repository.

    > ☛ *See "Importing a command file in HOPEX", page 148.*

Comparing and Aligning Objects Between Repositories

☛ *The object compare and align feature is available with the **HOPEX Power Supervisor** or the **HOPEX Collaboration Manager** technical module.*

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.
- a file and a repository (or repository objects)
- two repository archived states

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

See:

- "Compare and Align Principle", page 152
- "Compare and Align Warnings", page 153
- "Compare and Align", page 153

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.

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 > Data Exchange > Import/Export Synchronization > MEGA**, select the option **Delete files produced at compare/align on completion of processing**.*

Compare and Align

☛ *Before comparing and aligning, see "Compare and Align Warnings", page 153.*

To compare and align:

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

   ☛ *See "Connecting to the Administration Desktop", page 6.*

   ☛ *You can also Compare and Align in a **HOPEX** desktop.*

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
   - a file and a repository

4. Click **Next**.
5. Select:
   - the **Source repository**
   - the **Target repository**, which is the repository to be updated.

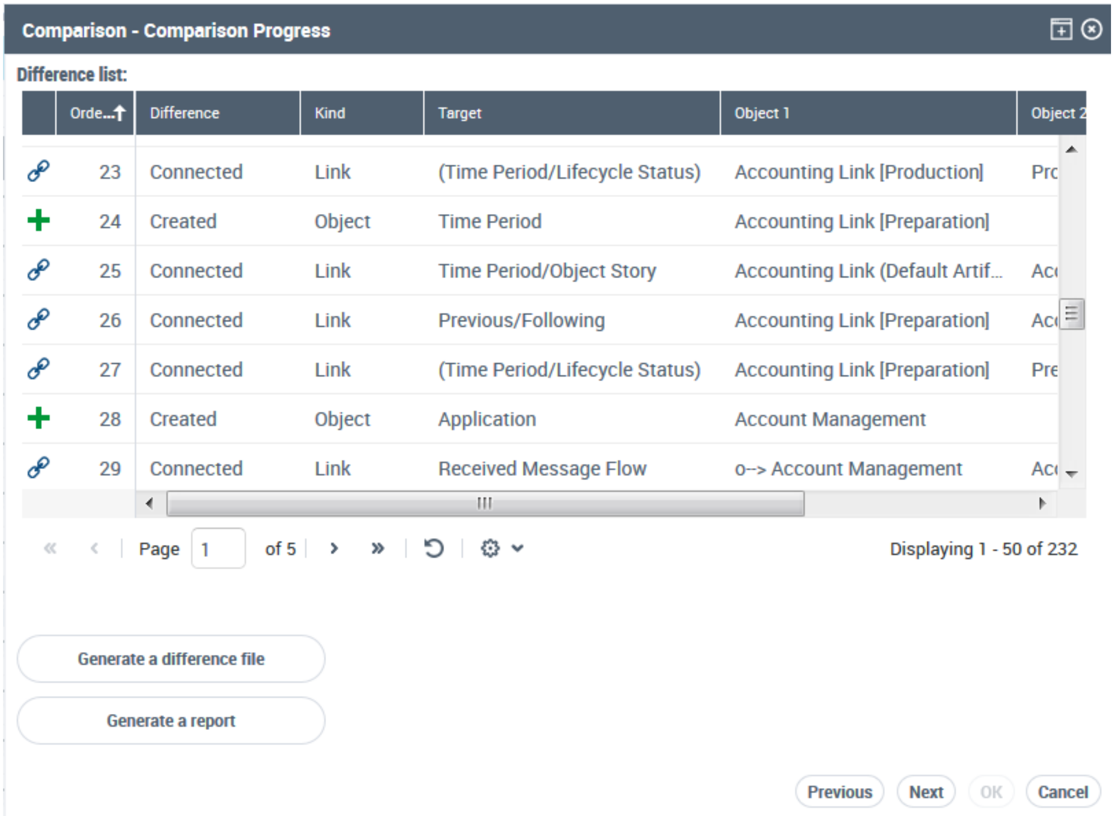
     ☛ *It can be a private workspace of the repository.*
6. (Optional) If required, you can choose to **Compare all repository objects**. Select the option an go to step 10.

   ☛ ***Warning**: processing of this option can be time-consuming.*
7. Click **Next**.
   The dialog box for selection of objects to be compared opens.
8. In the **Perimeter** field, select the perimeter type (by default **Standard for Comparison**)

   ☛ *For detailed information on perimeters, see the **HOPEX Power Studio** - **Perimeters** technical article.*
9. In the **Elements to compare** pane, select:
   - **Add from source** ▶ to add objects from the source repository, or
   - **Add from target** ◀ to add objects from the target repository.

     ☛ *If you have opened the comparison wizard from an object, this object is automatically added in the list of objects to be compared.*

10. Click **Next**.
    The **Comparison Progress** window opens. It presents the differences between compared objects and their modifications.



Comparison - Comparison Progress

Difference list:

	Orde...↑	Difference	Kind	Target	Object 1	Object 2
🔗	23	Connected	Link	(Time Period/Lifecycle Status)	Accounting Link [Production]	Prc
✚	24	Created	Object	Time Period	Accounting Link [Preparation]	
🔗	25	Connected	Link	Time Period/Object Story	Accounting Link (Default Artif...	Acc
🔗	26	Connected	Link	Previous/Following	Accounting Link [Preparation]	Acc
🔗	27	Connected	Link	(Time Period/Lifecycle Status)	Accounting Link [Preparation]	Pre
✚	28	Created	Object	Application	Account Management	
🔗	29	Connected	Link	Received Message Flow	o--> Account Management	Acc

Page 1 of 5

Displaying 1 - 50 of 232

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 > 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.

12. (Optional) Click **Generate a report** to generate the comparison report (.pdf format) which contains:
    - the list of differences detected
    - statistics
13. 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.
14. Click **OK**.

Managing UI Access (Permissions)

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

💣 **To modify profile UI access, you must have modification authorization rights on this profile.**

💣 **To modify a profile for which you do not have modification rights, you can create a new profile from this profile, see** ***"Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50*****.**

UI access is managed at profile level.

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 accesses to user interface workflows, see the* ***HOPEX Collaboration Manager - Workflows*** *guide.*

- *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.*

Accessing the UI Access Management Pages (Permission)

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

💣 **To modify UI access of a profile, you must have modification authorization rights on this profile.**

💣 **To modify a profile supplied by HOPEX, you must create a new profile, see "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50.**

- **Object UIs**, which details for the selected profile its access to UI of objects and its access to tools specific to these objects.

  ☛ *See "Object UI Access Values", page 158.*

  ☛ *See "Managing UI Access", page 159.*

- **General UIs**, which details for the selected profile its access to general UIs.

  ☛ *See "Object UI Access Values", page 158.*

  ☛ *See "Managing General UI Access", page 166.*

To access the UI access management pages:

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

   ☛ *See "Connecting to the Administration Desktop", page 6.*

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

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

- **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

💣 **To modify UI access on an object for a given profile, you must have modification authorization rights on this profile.**

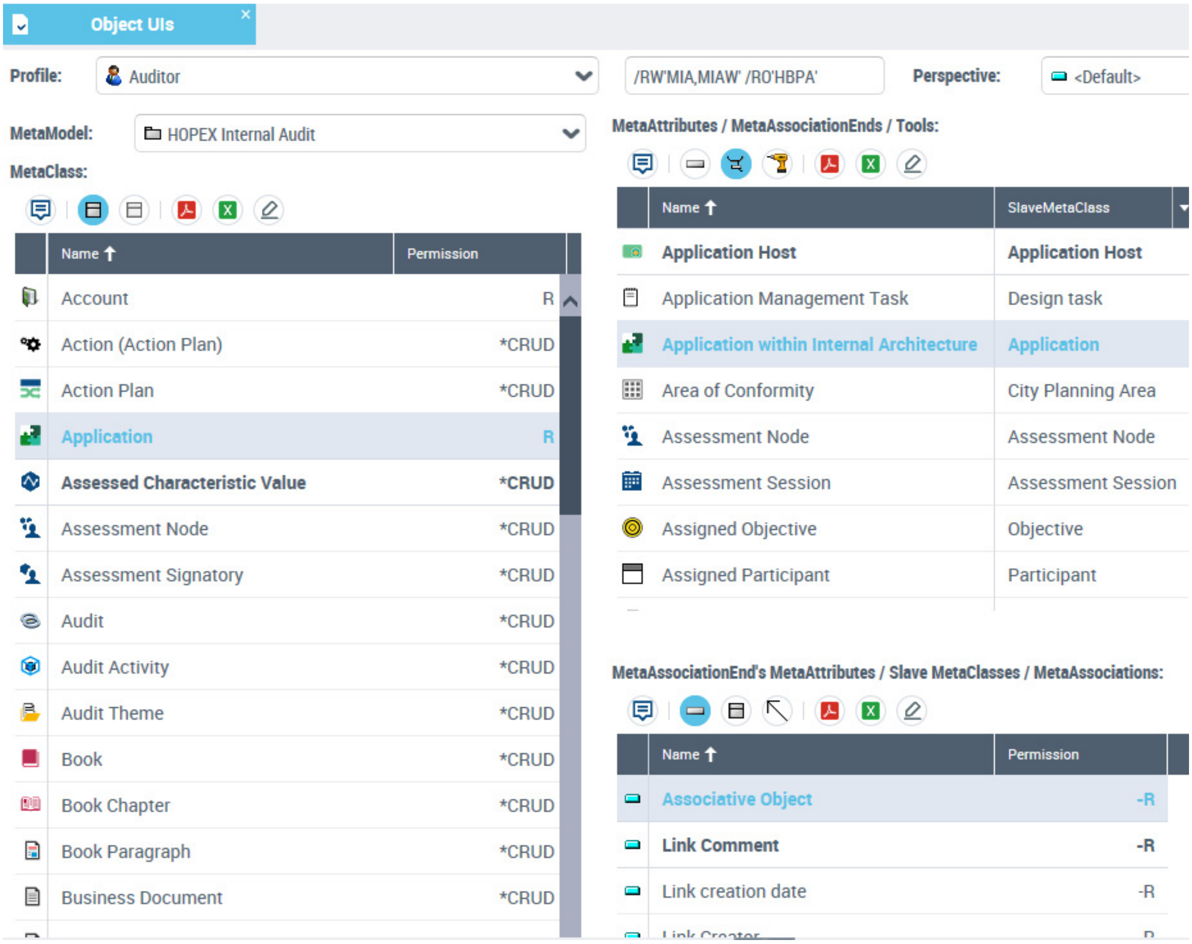
☛ *For information on management of accesses to user interface workflows, see the **HOPEX Collaboration Manager - Workflows** guide.*

For a new profile, access permissions on an object of this profile are by default:

- inherited from the Default profile, if the profile is not an aggregation of profiles (in profile parameters, the profile does not contain sub-profiles, see "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50).
- inherited from permissions defined on owned profiles, if the profile is an aggregation of profiles (in profile parameters, the profile contains one or

several profiles, see "Customizing an Existing Profile / Creating a Profile from an Existing Profile", page 50).

☛ *See "Rules on permissions at profile aggregation", page 166.*



Object UIs

Profile: Auditor /RW'MIA,MIAW' /RO'HBPA' Perspective: <Default>

MetaModel: HOPEX Internal Audit

MetaClass:

Name	Permission
Account	R
Action (Action Plan)	*CRUD
Action Plan	*CRUD
Application	R
Assessed Characteristic Value	***CRUD**
Assessment Node	*CRUD
Assessment Signatory	*CRUD
Audit	*CRUD
Audit Activity	*CRUD
Audit Theme	*CRUD
Book	*CRUD
Book Chapter	*CRUD
Book Paragraph	*CRUD
Business Document	*CRUD

MetaAttributes / MetaAssociationEnds / Tools:

Name	SlaveMetaClass
Application Host	**Application Host**
Application Management Task	Design task
Application within Internal Architecture	Application
Area of Conformity	City Planning Area
Assessment Node	Assessment Node
Assessment Session	Assessment Session
Assigned Objective	Objective
Assigned Participant	Participant

MetaAssociationEnd's MetaAttributes / Slave MetaClasses / MetaAssociations:

Name	Permission
Associative Object	-R
Link Comment	**-R**
Link creation date	-R
Link Creator	R

In the **Object UIs** tab:

- the **Profile** field enables definition of the profile for which you want to define access 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 for a profile", page 161.
- "Modifying access permissions of MetaAttributes of a MetaClass for a profile", page 163.
- "Modifying access permissions to tools of a MetaClass for a profile", page 164.
- "Modifying access permissions of a link around a MetaClass for a profile", page 164.
- "Modifying access permissions on links around a MetaClass for a profile", page 165.

Modifying access permissions on occurrences of a MetaClass for a profile

To modify access permissions on occurrences of a MetaClass for a profile:

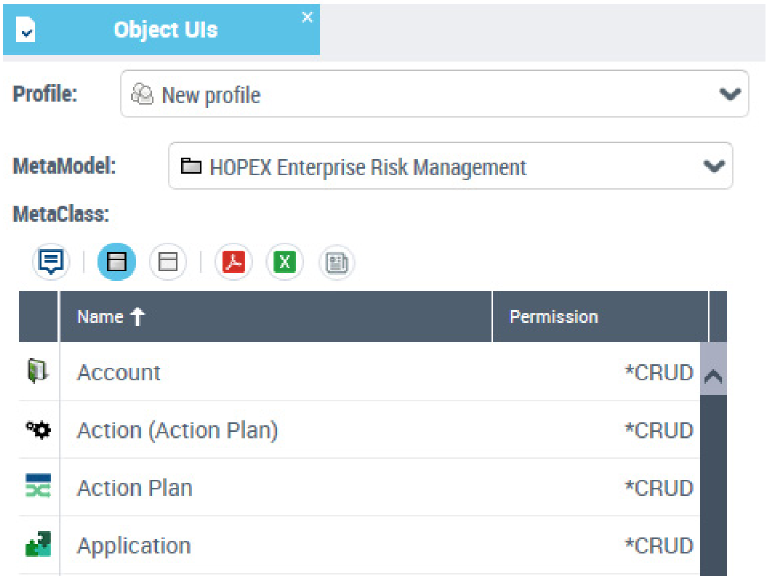
1. Access the UI access management pages and select the **Object UI Access**.

   ☛ *See "Accessing the UI Access Management Pages (Permission)", page 157.*

2. In the **Profile** field, select the profile using the drop-down menu.

   ☛ *The <Default> profile 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.



Profile: New profile

MetaModel: HOPEX Enterprise Risk Management

MetaClass:

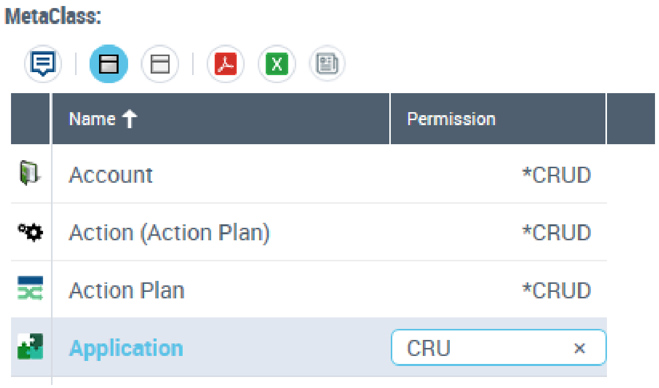
Name	Permission
Account	*CRUD
Action (Action Plan)	*CRUD
Action Plan	*CRUD
Application	*CRUD

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 the <Default> profile.*

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

   ☛ *See "MetaClass occurrence access permissions", page 158.*

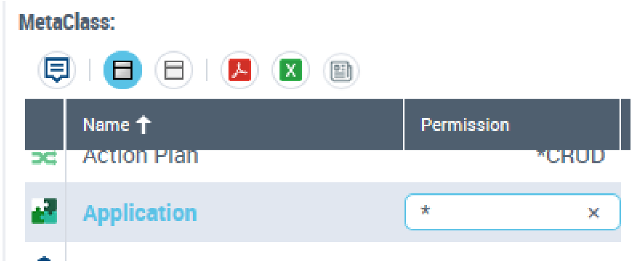


MetaClass:

	Name ↑	Permission
	Account	*CRUD
	Action (Action Plan)	*CRUD
	Action Plan	*CRUD
	Application	CRU ×

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.

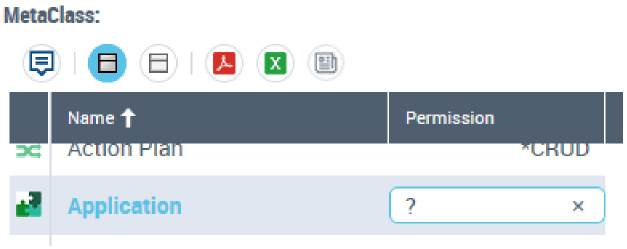
   ☛ *To return to the default value of the permission on the MetaClass, enter the character *.*



MetaClass:

	Name ↑	Permission
	Action Plan	*CRUD
	Application	* ×

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



MetaClass:

	Name ↑	Permission
	Action Plan	*CRUD
	Application	? ×

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

- "Modifying access permissions of MetaAttributes of a MetaClass for a profile", page 163.
- "Modifying access permissions to tools of a MetaClass for a profile", page 164.
- "Modifying access permissions of a link around a MetaClass for a profile", page 164.
- "Modifying access permissions on links around a MetaClass for a profile", page 165.

Modifying access permissions of MetaAttributes of a MetaClass for a profile

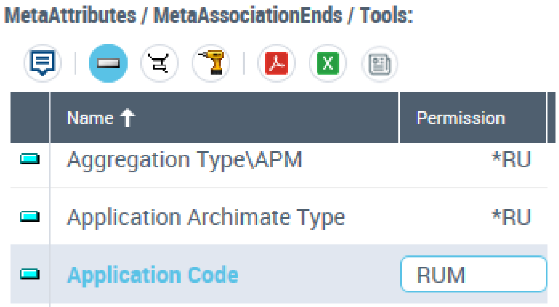
To modify access permissions of MetaAttributes of a MetaClass for a profile:

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

   ☛ *See "Accessing the UI Access Management Pages (Permission)", page 157.*
2. In the **Profile** field, select the profile using the drop-down menu.

   ☛ *The <Default> profile 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.
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", page 159.*



MetaAttributes / MetaAssociationEnds / Tools:

Name ↑	Permission
Aggregation Type\APM	*RU
Application Archimate Type	*RU
Application Code	RUM

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 to tools of a MetaClass for a profile

A tool can be available or not.

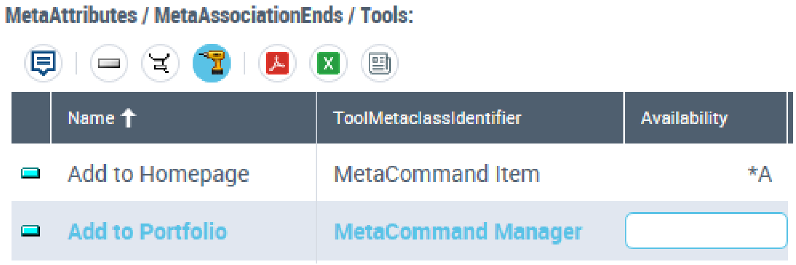
To modify access permissions to tools of a MetaClass for a profile:

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

   ☛ *See "Accessing the UI Access Management Pages (Permission)", page 157.*
2. In the **Profile** field, select the profile using the drop-down menu.

   ☛ *The <Default> profile defines default 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", page 159.*



MetaAttributes / MetaAssociationEnds / Tools:

	Name ↑	ToolMetaclassIdentifier	Availability
	Add to Homepage	MetaCommand Item	*A
	Add to Portfolio	MetaCommand Manager	

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 for a profile

To modify access permissions of a link around a MetaClass for a profile:

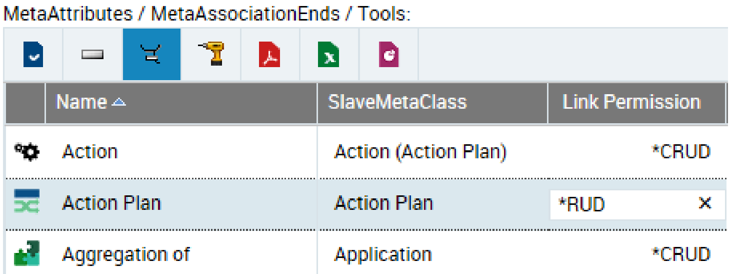
1. Access the UI access management pages and select **Access Object UIs**.

   ☛ *See "Accessing the UI Access Management Pages (Permission)", page 157.*
2. In the **Profile** field, select the profile using the drop-down menu.

   ☛ *The <Default> profile defines default 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", page 158.*



MetaAttributes / MetaAssociationEnds / Tools:

	Name	SlaveMetaClass	Link Permission
	Action	Action (Action Plan)	*CRUD
	Action Plan	Action Plan	*RUD
	Aggregation of	Application	*CRUD

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 for a profile", page 165.

Modifying access permissions on links around a MetaClass for a profile

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 for a profile:

1. Select the MetaAssociationEnd.

☛ *See "Modifying access permissions of a link around a MetaClass for a profile", page 164, 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", page 159.*

☛ *See "MetaClass occurrence access permissions", page 158.*

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 at profile aggregation

When a profile aggregates several sub-profiles, its permissions are defined by the addition of permissions defined on its sub-profiles.

```
Example:

Profile 1 is the aggregation of sub-profiles 1.1 and 1.2.

If the permission on an object A of sub-profile 1.1 has
value CR, and that of sub-profile 1.2 has value RUD, then
the value of this permission on object A for profile 1 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:

Profile 1 is the aggregation of sub-profiles 1.1 and 1.2.

If the permission on an object A of sub-profile 1.1 has
value *CRUD, and that of sub-profile 1.2 has value R, then
the value of this permission on object A for profile 1 is R.
```

Managing General UI Access

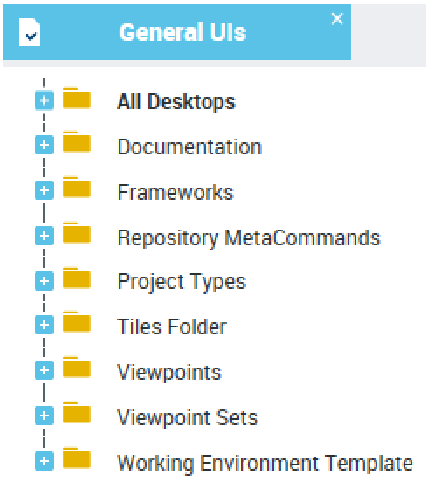
You can manage general UI access for a profile. General UIs are classified by category:

- desktop
- command category
- command group
- general command
- properties page
- tree

To manage general UI access:

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

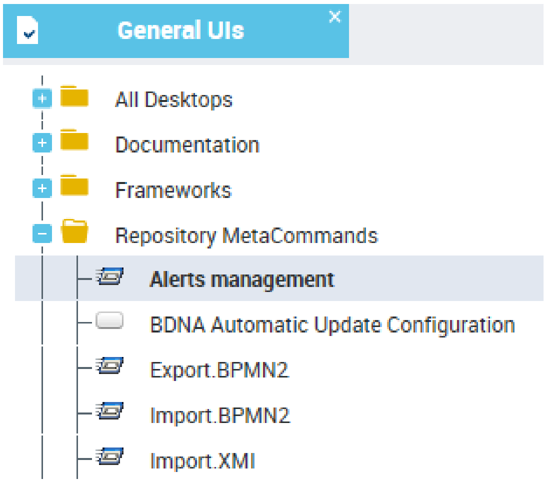
   ☛ *See "Accessing the UI Access Management Pages (Permission)", page 157.*



General UIs

- All Desktops
- Documentation
- Frameworks
- Repository MetaCommands
- Project Types
- Tiles Folder
- Viewpoints
- Viewpoint Sets
- Working Environment Template

2. Expand the folder of the category concerned.
3. In the list, select the tool concerned.

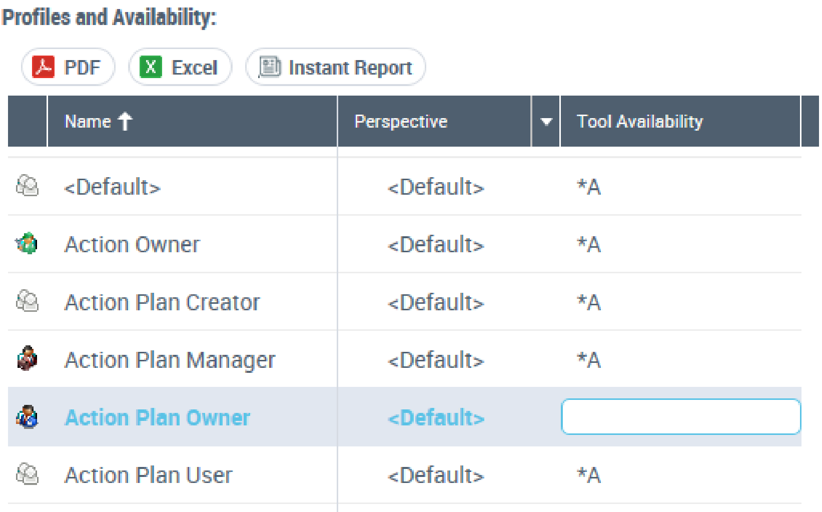


General UIs

- All Desktops
- Documentation
- Frameworks
- Repository MetaCommands
  - Alerts management
  - BDNA Automatic Update Configuration
  - Export.BPMN2
  - Import.BPMN2
  - Import.XMI

4. In the **Profiles and Availability** frame, select the profile for which you want to modify access on the tool.

5. In the **Tool Availability** field, enter the availability value.



Profiles and Availability:

Name	Perspective	Tool Availability
<Default>	<Default>	*A
Action Owner	<Default>	*A
Action Plan Creator	<Default>	*A
Action Plan Manager	<Default>	*A
Action Plan Owner	<Default>	
Action Plan User	<Default>	*A

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 ?.*

MANAGING OPTIONS

This chapter presents the various tools and options used to configure and customize **HOPEX**.

The points covered here are:

OPTIONS OVERVIEW

In the **Administration** desktop, **HOPEX** options can be configured at the following levels:

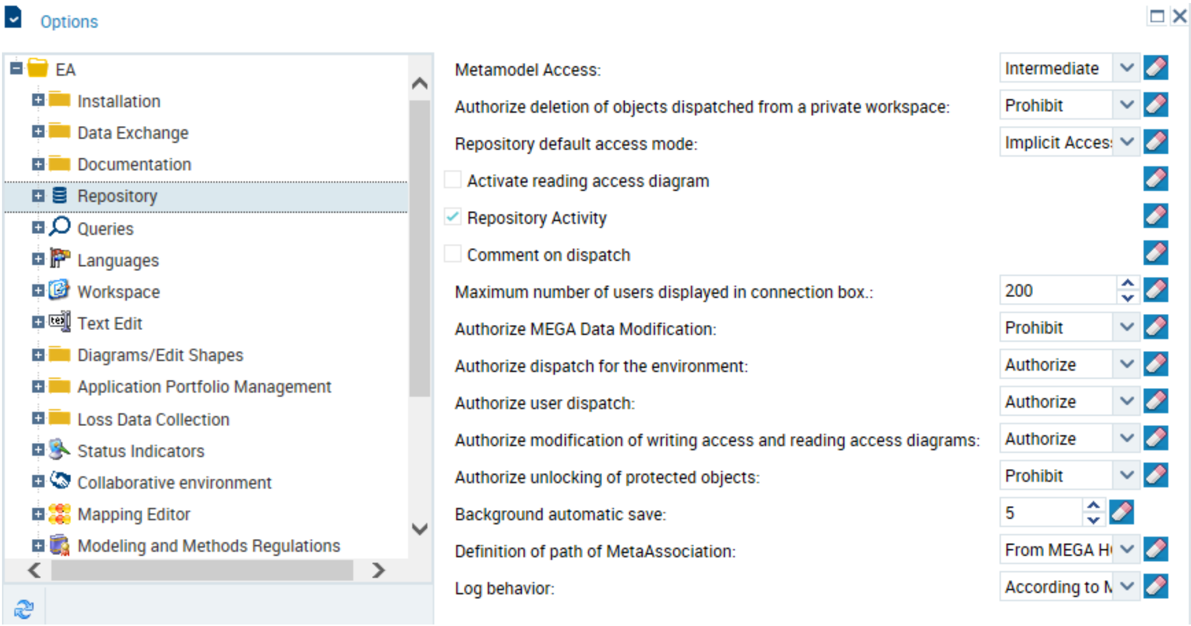
- environment
- profile (which groups a configuration common to several users)
- user

By default, the option levels are governed by an inheritance mechanism:

- the profile inherits the option values defined at environment level.
- the user inherits the option values defined at connection profile 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.

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.



Metamodel Access: Intermediate

Authorize deletion of objects dispatched from a private workspace: Prohibit

Repository default access mode: Implicit Acces

□ Activate reading access diagram

☑ Repository Activity

□ Comment on dispatch

Maximum number of users displayed in connection box.: 200

Authorize MEGA Data Modification: Prohibit

Authorize dispatch for the environment: Authorize

Authorize user dispatch: Authorize

Authorize modification of writing access and reading access diagrams: Authorize

Authorize unlocking of protected objects: Prohibit

Background automatic save: 5

Definition of path of MetaAssociation: From MEGA H

Log behavior: According to N

The left pane contains the option tree classified by group.

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:

- Roll the mouse over the option to display context-sensitive help.

  ☛ *When the user has a private workspace in progress, you cannot modify its options from **HOPEX Administration**.*

ACCESSING OPTIONS

Options Level

You can modify the options at the following levels:

- environment

  ☛ *See "Modifying options at environment level", page 172*

- profile

  ☛ *See "Modifying options at profile level", page 172*

- user

  ☛ *See "Modifying options at user level", page 172*

Modifying options at environment level

To modify options at environment level from the **Administration** desktop:

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

   ☛ *See "Connecting to the Administration Desktop", page 6.*

2. In the edit area, click **Environment Options**.
   The environment options window opens.

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", page 69.*

2. In the edit area, select the profile concerned.
3. Click **Options**.
   The profile options window opens.

Modifying options at user level

☛ *A user can modify some of his/her options from the toolbar on his/her desktop "Toolbar", page 10.*

To modify the options of a user from the **Administration** desktop:

1. Access the user management page.

   ☛ *See "Connecting to the Administration Desktop", page 6.*

2. Select a **Persons** sub-folder.
3. In the edit area, select the person concerned.
4. Click **Options**.
   The person's options window opens.

Option Inheritance

An option inherits a value defined at a higher level:

- A user inherits options defined at the connection profile level.
- A profile inherits options defined at the environment level.
- An environment inherits options defined at the site level.

The icon located opposite the option indicates the inheritance, or not, from the higher level:

- **Default value** indicates the inheritance from the higher level.
- **Modified value** indicates that the inherited option value has been modified. The value is no longer inherited from the higher level.

To specify that an option does not inherit the value defined at higher level:

1. Open the options page.

   ☛ *See "Options Level", page 172.*

2. Click **Default value** .
   The icon changes in **Modified value** .

Checking Option Modifications

You can prohibit modification of any option at a level lower than your current level.

> Example: if you open options of the environment, you can prohibit modification of all options at user level.

Prohibiting modification of a lower level option

To prohibit modification of a lower level option:

1. Access the options.

   ☛ *See "Options Level", page 172.*

2. Click 🔓 icon located opposite the option concerned.

   The padlock closes 🔒: option modification by a user is now prohibited from **HOPEX**.

Unlocking the modification of a lower level option

To unlock modification of a lower level option:

1. Access the options.

   ☛ *See "Options Level", page 172.*

2. Click the closed padlock icon.
   The padlock opens: modification of the option is again possible.

Reinitializing the value of an option

To reinitialize the value of an option:

1. Access the options.

   ☛ *See "Options Level", page 172.*

2. Click **Default value** .
   The value of the option is reinitialized.

AVAILABLE OPTION GROUPS (USER LEVEL)

☛ *Repository and modeling options contain important information for the functional administrator.*

- **Installation**
  Options linked to installation: licenses, information on the company, cache management, user management, Web user desktop (application Web), etc.
- **Data Exchange**
  Options linked to import/export, exchanges with third party tools.
- **Documentation**
  Options linked to documentation generated by **HOPEX** (reports (MS Word), reports (Open Office), Web sites, Description, reports, performance indicators)
- **Repository**
  Options authorizing or prohibiting access to certain repository functions.
- **Queries**
  Options linked to the query tool
- **Languages**
  Activated data languages
- **Text Editing**
  Options concerning RTF format comment entry
- **Diagrams/Edit Shapes**
  Options of drawing tool configuration (diagrams and shapes editor)
- **Status indicators**
  Options concerning display of indicators available in workspace and diagrams
- **Collaborative Environment**
  Options available with **HOPEX Collaboration Manager** product
- **Mapping Editor**
  Options linked to the mapping editor, a tool enabling alignment of data models (essentially with **HOPEX Database Builder**)
- **Modeling and Methods Regulations**
  Options linked to modeling regulations and rules
- **Business Process and Architecture Modeling**
  Options linked to processes and architecture enabling display of certain functions
- **Simulation**
  Options enabling definition of **HOPEX Process Simulation** use level
- **Compatibility**
  Compatibility options regarding diagrams and obsolete functionalities
- **Technical Support**
  Options concerning Technical Support access
- **Monitoring**
  Option concerning data access supervision

Web Application-Linked Options

Installation Options

For detailed information on the installation options linked to Web applications, see the **HOPEX Web Front-End Installation Guide**.

> ☛ *To manage languages in Web applications, see "Managing Languages in Web Applications", page 178.*

Specifying the Web applications access path

To specify the Web applications access path:

1. Access environment options.

   > ☛ *See "Modifying options at environment level", page 172.*

2. In the options tree, expand the **Installation** folder and select **Web Application**.
3. In the right pane, specify the **Web Application Path** option.

   ```
   Example: http://<Server Name>/HOPEX
   ```

Specifying SMTP configuration

To specify SMTP configuration:

1. Access environment options.

   > ☛ *See "Modifying options at environment level", page 172.*

2. In the options tree, expand the **Installation** folder and select **Electronic Mail**.
3. The following options should be specified in the right pane:
   - **Default address of sender via SMTP**

     ```
     Example: server@company.com, AdministratorName@company.com
     ```

   - **SMTP Server**

     ```
     Example: exa.fr.company.com
     ```

System Information Access Option (Web user)

By default the Web user can download the system information report (html format) regarding the current session and the installed version:

- HOPEX System Information (available components and versions, trace logs)
- MWAS System Information ("Generation Context" XML file)
- IIS System Information (inetinfo.exe)
- Client System Information

Downloading the system information report

To download the system information report from HOPEX (Web Front-End):

1. In your HOPEX desktop tool group, click **My account**.

   ☛ *See "Toolbar", page 10.*

2. Select **HOPEX System Web Report**.
   The **Collecting Client-Side data** page is displayed.
3. Click the **Click here to skip client-side data collection** link.
   The report is displayed in html format.

Removing access to system information

By default the Web user can download the system information report (html format) regarding the current session and the installed version. For security reasons, for example, you can remove access to this information.

To remove access to system information from a Web desktop:

1. Access environment options.

   ☛ *See "Modifying options at environment level", page 172.*

2. In the options tree, expand the **Installation** folder and select **Web Application**.
3. In the right pane, clear **Availabitlity of the system information report from the Web**.
   The **My account > HOPEX System Web Report** menu is no longer available.

MANAGING LANGUAGES IN WEB APPLICATIONS

You can modify:

- the interface language in Web applications, see:
  - "Modifying the interface language in Web applications at environment level", page 178.
  - "Modifying the interface language in Web applications at user level", page 178
- the data language in Web applications, see "Modifying the data language in Web applications at environment level", page 179.

Modifying the interface language in Web applications at environment level

The interface language defines the default language in which the Web application interface is displayed.

> ☛ *The Web user can modify the interface language from his/her desktop, see "Modifying the interface language in Web applications at user level", page 178.*

To define the interface language in Web applications:

1. Access the environment options management window.

   > ☛ *See "Modifying options at environment level", page 172.*

2. In the options tree, expand the **Installation** folder and select **Web Application**.
3. In the right pane, modify the value of the **GUI language** via the drop-down menu.

Modifying the interface language in Web applications at user level

From his/her **HOPEX** desktop, the user can change his/her interface language.

To modify the interface language in Web applications at user level:

1. From your **HOPEX** desktop, in the **Miscellaneous** toolbar, select **My Account > Options**.
2. Expand the **Installation** folder and select **Web Application**.
3. In the right pane, modify the value of the **GUI language** via the drop-down menu.

   > ☛ *You must disconnect for this modification to be taken into account.*

Modifying the data language in Web applications at environment level

The data language is the language with which the user connects by default the first time. If the user changes 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 "Specifying the Data Language", page 116.*

💣 **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", page 172.*

2. In the options tree, expand the **Installation** folder and select **Web Application**.
3. In the right pane, modify the value of the **Data language** via the drop-down menu.

6

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.

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 A physical backup (GBMS only) consists of copying the files of a repository from their original location to another.

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)

group

Descriptors, which are available with the **HOPEX Power Studio** technical module, comprise a tree of several successive groups. Each group concerns one object, and defines the query or link used to access this object from the preceding object. You can connect texts and other groups to a group. Users can define the order in which groups and texts are processed.

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.

LDAP parameter

An LDAP parameter is a parameter that exists in the LDAP directory and is associated uniquely with a **HOPEX** attribute. For example, "mail" is a parameter of the "Active Directory" LDAP directory and can be associated with the e-mail of the person.

LDAP server

The LDAP server is the server on which the LDAP directory is installed. The LDAP directory can be an Active Directory directory.

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. Isolated objects are found by checking that each object is used in another object. For example, a Diagram containing Org-units and Messages is itself used by a Process, an Org-unit, a Project, etc. This functionality is available with the **HOPEX Power Supervisor** technical module.

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.

The list of persons can for example come from an LDAP server.

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 (GBMS, SQL Server, or Oracle). 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 > 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 session 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.

A user is authorized to access certain functions of the product and certain repositories. Each user has a specific desktop in each database, and can connect to this desktop from any workstation in a given environment.

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 persons (Login: System) and Mega (Login: Mega) 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.